NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PRIVACY IN PLAIN SIGHT: FOURTH AMENDMENT CONSIDERATIONS FOR THE COLLECTION, RETENTION, AND USE OF DATA BY LAW ENFORCEMENT IN PUBLIC PLACES

by

Kristen Ziman

December 2018

Co-Advisors: Kathleen L. Kiernan (contractor)
Carolyn C. Halladay

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE PRIVACY IN PLAIN SIGHT: FOURTH AMENDMENT CONSIDERATIONS FOR THE COLLECTION, RETENTION, AND USE OF DATA BY LAW ENFORCEMENT IN PUBLIC PLACES	**5. FUNDING NUMBERS**
6. AUTHOR(S) Kristen Ziman	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Cities around the globe are implementing technology that provides an interactive experience for their citizens in open spaces. Transportation, infrastructure, parking, and lighting are all part of a "smart city." Cameras, drones, facial recognition, kiosks, and geofencing are built into the platform as well; however, the latter brings up privacy concerns as they pertain to government surveillance. This thesis examines how data collected using the open-source methods of smart city technology can be used by law enforcement under the Fourth Amendment, which protects citizens from government intrusion. The Fourth Amendment has been the litmus test for what constitutes a search and seizure, and with a properly executed warrant or a subpoena, information can be used by law enforcement. This thesis explores whether the Fourth Amendment can withstand the test of technology, whereby data collected by a city can be used by law enforcement to solve crimes that occur in plain sight. This thesis follows the historical path of Fourth Amendment case law since the inception of technology and recognizes that legislation and policy should be enacted to identify the owner of the data collected and determine how long it should be maintained. Rather than easily accessing data, law enforcement may be required to show reasonable suspicion and obtain a warrant.

14. SUBJECT TERMS Fourth Amendment, smart city, law enforcement, privacy	**15. NUMBER OF PAGES** 69
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

PRIVACY IN PLAIN SIGHT: FOURTH AMENDMENT CONSIDERATIONS FOR THE COLLECTION, RETENTION, AND USE OF DATA BY LAW ENFORCEMENT IN PUBLIC PLACES

Kristen Ziman
Police Chief, Aurora (IL) Police Department
MA, Boston University, 2008

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2018**

Approved by: Kathleen L. Kiernan
Co-Advisor

Carolyn C. Halladay
Co-Advisor

Erik J. Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Cities around the globe are implementing technology that provides an interactive experience for their citizens in open spaces. Transportation, infrastructure, parking, and lighting are all part of a "smart city." Cameras, drones, facial recognition, kiosks, and geofencing are built into the platform as well; however, the latter brings up privacy concerns as they pertain to government surveillance. This thesis examines how data collected using the open-source methods of smart city technology can be used by law enforcement under the Fourth Amendment, which protects citizens from government intrusion. The Fourth Amendment has been the litmus test for what constitutes a search and seizure, and with a properly executed warrant or a subpoena, information can be used by law enforcement. This thesis explores whether the Fourth Amendment can withstand the test of technology, whereby data collected by a city can be used by law enforcement to solve crimes that occur in plain sight. This thesis follows the historical path of Fourth Amendment case law since the inception of technology and recognizes that legislation and policy should be enacted to identify the owner of the data collected and determine how long it should be maintained. Rather than easily accessing data, law enforcement may be required to show reasonable suspicion and obtain a warrant.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

As cities have become more wirelessly connected, issues have intensified around data collection and the ways in which a person's privacy and civil liberties are affected when opting in for an interactive experience in a public place. In choosing connectivity to enrich an experience, a citizen might not be aware of the mounds of data collected that could reveal one's identity or location among other information. How might smart cities strike a balance between data collection and a person's right to privacy as it pertains to government actors? This thesis follows the journey of one city as it becomes "smart," exploring this question and its implications.

The mayor of Aurora—the second largest city in Illinois—intends to use the 100-square-mile network of underground fiber optics already installed to serve as the foundation for the construction of a tech corridor. Part of the plan is to develop "smart parking," so citizens and visitors can easily find parking using an app that directs them to vacant spaces. Also planned is the installation of kiosks throughout the downtown area. Citizens can use the digital interface at the kiosk to obtain information on restaurants, entertainment, or scheduled events in the area. The goal, according to the mayor, is not only to recoup costs through advertising but also to engage citizens, so they feel a part of the community.[1]

In an effort to make the tech corridor user-friendly and provide connectivity to citizens, the mayor intends to use a GPS satellite network as well as radio frequencies to create virtual boundaries around designated areas. The concept, called "geofencing," relies on the GPS functionality of smartphones, which most people carry.[2] If visitors who have the GPS capability cross the virtual boundary around the downtown corridor and RiverEdge Park, they can receive information on their smartphones.[3]

---

1 "Episode 32: Aurora Lights Up Smart Cities," YouTube video, 57:35, posted by Constructech TV, August 6, 2018, https://www.youtube.com/embed/7K9PZKrikKg.

2 Jason Fitzpatrick, "What Is 'Geofencing'?," How-to Geek, September 21, 2016, https://www.howtogeek.com/221077/htg-explains-what-geofencing-is-and-why-you-should-be-using-it/.

3 Fitzpatrick.

Future phases of Aurora's smart city concept include plans to install cameras inside the park, so security personnel can monitor events. This surveillance will help alleviate workforce and coverage limitations by police officers. Other considerations for future phases include tethered drones to capture a birds-eye view of the park, facial-recognition software, parking sensors, and smart lighting.[4] Tethered drones have become an observation tool for law enforcement because they improve situational awareness across a venue and contribute to resource deployment.

As cities like Aurora have become smarter and the world has become more connected, privacy and legal implications regarding data collection and dissemination have intensified. A delicate balance must be struck that affords the consumer the convenience of connectivity while prohibiting personal data from being shared with government actors who attempt to utilize that data. The intersection of law and technology is converging, and the regulatory efforts require further exploration of how citizens can expect privacy in plain sight.

The Fourth Amendment to the U.S. Constitution provides the legal framework for privacy issues. It reads, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[5] The complexity of the standard has evolved in the digital age along with advancements in communications and digital technology. For example, it is unclear whether facial recognition software that captures the identity of a person constitutes an illegal search. Similarly, is there an expectation of privacy when a consumer voluntarily opts into a Wi-Fi geofence? The Fourth Amendment application is not as clear-cut regarding these technological advancements.

This thesis follows the historical path of Fourth Amendment case law since the inception of technology and recognizes that legislation and policy should be enacted that identify the owner of the data collected and the length of time data should be maintained.

---

[4] Richard C. Irvin, "Prioritization of Information Technology Initiatives" (lecture, Alarm Detection Services, Aurora, IL, July 11, 2018).

[5] U.S. Const. amend. IV.

To determine whether digital data collected in public spaces, such as downtown Aurora or RiverEdge Park, can be used by law enforcement within the parameters of the Fourth Amendment, this thesis explores what *might* happen. Smart city technology is applied within these spaces, and hypothetical crimes are overlaid to create potential scenarios. This thesis ultimately predicts there will be a tipping point in the form of backlash when all the innovations that comprise a smart city begin to identify people and compromise privacy.

Rather than waiting for the Supreme Court to rule on pending cases or carve out exceptions, this thesis recommends that legislation be introduced to determine who owns data and to regulate the balance between privacy and public safety. The courts can only rule on cases that come before them, but members of Congress have the capacity to weigh the arguments and reactions from their constituents and determine the best way forward to address policies. Being proactive is better than allowing the courts to decide the fate of the third-party doctrine and the protection of metadata and stored communications. In addition, agencies who implement smart city technology should establish a policy that outlines how the data will be used and how long they will be retained. Cities and vendors should be transparent about the information collected, so citizens are protected from their content being shared with other companies or the government.

Law enforcement must continue to adhere to the parameters of the Fourth Amendment when seeking data on suspects, witnesses, and victims of crime. Law enforcement must embrace the revelation that data require controls, which are developed by changing policy and driving new legislation to provide citizens transparency about how their digital footprint is being used. Furthermore, there is strong evidence that the Fourth Amendment remains the gatekeeper of unreasonable searches, even in the digital age. The case law presented in this thesis is crucial because it follows the development of the citizen's privacy right vis-à-vis the government's need for information to solve a crime, beginning with a physical search through the emergence of technology and surveillance. The notion of privacy in plain sight is an oxymoron—there is no such thing as privacy when technology is watching.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Before I started this program, I considered myself a writer. I was knocked down on day one at CHDS when Chris Bellavita responded to one of my declarations by asking, "Who are you, and why should I believe you?" At that moment, all my molecules scrambled, and I began to develop an understanding and respect for research. Before then, I had enjoyed the comfort of opinion without the discomfort of thought. Thus, the journey of research for this thesis began.

In comparative mythology, the hero's journey is a tale of a man who goes on an adventure but must undergo obstacles along the way. Mentors emerge throughout the journey and guide him through crisis until the hero ultimately prevails and comes home transformed.

I was convinced that Carolyn Halladay was the obstacle whose role was to thwart my journey. Her feedback and revision requests often paralyzed me because I didn't know how to move forward. In the ultimate plot twist, I discovered that Halladay created the conflict to enlighten me and reveal the true path. I'm better because of her. A second mentor emerged along the way in the form of Kathleen Kiernan, who talked me off a few ledges and inspired me to keep moving. I knew I couldn't let her down.

Mayor Richard Irvin told me it was a "no-brainer" that I pursue this degree, but what neither of us realized at the time was my thesis was born of his vision for a smart city. He is moving Aurora forward, and in doing so, he has validated my belief in leadership and taking risks.

Chris remained my true north along this journey, as she has with all my adventures. Bailey, Jake, Megan, and Jim gave me purpose—I want them to know that major achievements in life are almost always preceded by difficult roads. The command staff of the Aurora Police Department manned the ship and stayed the steady course while I was away. To say I am grateful for their leadership and support is an understatement.

Each of us in Cohort 1703-04 traveled our own journey, but we were on the same path. We helped each other along the way through encouragement, memes, and bonding at a two-star hotel.

It is my honor to stand shoulder to shoulder with those who compose the homeland security enterprise and work tirelessly to make our respective corners of the world safer. My classmates and the instructors at CHDS are the real heroes of this journey, and because of all of you, I am transformed.

I. SMART CITY TECHNOLOGY: DATA COLLECTION AND USE BY LAW ENFORCEMENT

With the inception of "smart cities" technology, digital data are being collected from open-source access points from sensors and devices in residential homes and cities. There is no strict definition of a smart city. However, cities are eager to assume the title because, broadly speaking, a smart city is one that uses technology to deliver better services to residents and to solve problems pertaining to transportation and quality-of-life issues. One such city is Aurora, Illinois, which starting with RiverEdge Park, has planned a smart venue meant to form the cornerstone of a greater smart-city project. Entertainment and civic engagement are also important for residents because they add to their quality of life. A smart city initiative might enhance the experience of a person attending a concert through technology that offers an interactive experience while at the venue. While the concert patrons enjoy the benefits of being "connected," are they giving up privacy in exchange?

The mining and use of data have the potential to endanger the privacy of citizens.[1] The Fourth Amendment bounds data collection as it pertains to searches and seizures. That is, the Constitution governs the collection of personal data in circumstances where law enforcement presents evidence of probable cause to a judge, who then determines whether cause exists to issue a warrant for the collection of data. The Fourth Amendment determines whether data can be lawfully collected.

On the other hand, no comprehensive body of law concerns the retention of data collected in cities that are "smart." Cameras that capture faces, license plates, and interactions collect an immense amount of data. As the sensors become smarter, so do the data. Yet there is no constitutional guidance for how long data can be retained or what specifically can be done with them after they have been lawfully collected. This thesis explores law enforcement and Fourth Amendment considerations for the collection, retention, and use of data in smart cities.

---

[1] Antoni Martinez-Balleste, Pablo Perez-Martinez, and Agusti Solanas, "The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible," *IEEE Communications Magazine* 51, no. 6 (June 2013), https://doi.org/10.1109/MCOM.2013.6525606.

A. RESEARCH QUESTION

This thesis explores the implications of data collection and its effect on individual civil liberties in the case of opting in for an interactive experience in a public place. In agreeing to connect, individuals provide data on their locations and perhaps their identities. This work seeks to determine how that information can be used by law enforcement. Specifically, using RiverEdge Park and downtown Aurora as an example, this thesis asks the following: Does a person give up the right to privacy in public where there is digital technology, and can law enforcement utilize that technology to solve crimes within the parameters of the Fourth Amendment?

B. LITERATURE REVIEW

This review explores the literature as it pertains to data collection and technology and the ways law enforcement uses the data within the parameters of the Fourth Amendment. It seeks to determine whether patrons who opt into an interactive experience at a public venue make their identity susceptible to use by law enforcement.

1. Defining a Smart City

Before an implementation plan can be developed, there must be a clear picture of what constitutes a smart city. Jack Gold defines a smart city this way: "One of those all-encompassing terms that everyone defines however they want."[2] This broad and poorly detailed overview leaves more questions than answers. Sam Musa defines the concept as follows:

> A city that engages its citizens and connects its infrastructure electronically. A smart city has the ability to integrate multiple technological solutions, in a secure fashion, to manage the city's assets. The city's assets include, but [are] not limited to, local departments' information systems, schools, libraries, transportation systems, hospitals, power plants, law enforcement, and other community services.[3]

---

[2] Matt Hamblen, "Just What Is a Smart City?" *Computerworld*, October 1, 2015, https://www.computerworld.com/article/2986403/internet-of-things/just-what-is-a-smart-city.html.

[3] Sam Musa, "Smart City Roadmap," Academia, January 2016, 1–9, https://www.academia.edu/21181336/Smart_City_Roadmap.

Although Musa locates "technological solutions" at the core of a smart city, he provides no examples to describe what exactly he means. In his research on sensors and the internet of things, Stefan Poslad offers that "technology is driving the way city officials interact with the community and the city's infrastructure. Through the use of real-time control systems and sensors, data are collected from citizens and sensors and then processed in real-time."[4]

Boyd Cohen has discovered distinct phases in the adoption of the implementation of a smart city. The initial phase is driven by tech companies that want to sell their products. The next phase is a city government looking to adopt a product to improve the delivery of services and processes. The final phase is citizen-driven, whereby consumers adopt the product.[5] Taewoo Nam and Theresa A. Pardo present a "multidimensional framework of smart city innovation, [which places] equal importance on technology, organization, policy, and context dimensions."[6] These phases illustrate that the implementation of smart-city technology is layered and complex, and each dimension must be present to ensure success.

Dan Doctoroff ponders on what a city would look like if it were built from the internet up:

> Looking at history, one can make the argument that the greatest periods of economic growth and productivity have occurred when we have integrated innovation into the physical environment, especially in cities. The steam engine, electricity grid, and automobile all fundamentally transformed urban life, but we haven't really seen much change in our cities since before World War II. If you compare pictures of cities from 1870 to 1940, it's like night and day. If you make the same comparison from 1940 to today, hardly anything has changed. Thus, it's not surprising that, despite the rise of computers and the internet, growth has slowed and productivity increases

---

4 Stefan Poslad et al., "Using a Smart City IoT to Incentivise and Target Shifts in Mobility Behaviour—Is It a Piece of Pie?" *Sensors* 15, no. 6 (June 4, 2015): 13069–96, https://doi.org/10.3390/s150613069.

5 Boyd Cohen, "The 3 Generations of Smart Cities," Fast Company, August 10, 2015, https://www.fastcompany.com/3047795/the-3-generations-of-smart-cities.

6 Taewoo Nam and Theresa Pardo, "Smart City as Urban Innovation: Focusing on Management, Policy, and Context" (policy paper, Center for Technology in Government, University of Albany, New York, 2011), https://doi.org/10.1145/2072069.2072100.

> are so low. . . . So our mission is to accelerate the process of urban innovation.[7]

By incorporating technology into a city's infrastructure using sensors and the internet of things, Doctoroff's theory of acceleration might be realized.

2. Court Decisions and the Fourth Amendment

If innovation within a city is the goal, it makes sense to determine how public safety fits within that paradigm. Scholars hold various views on whether smart cities are easier or harder to police. On the one hand, the data being funneled in might be beneficial to identify criminal offenders more easily. On the other hand, more questions arise about how such information can be used by the government and what the role of law enforcement should be in a smart city. Several court decisions have guided law enforcement regarding technology and privacy. *United States v. Jones* set a precedent for the use of global positioning system (GPS) trackers in criminal investigations. A GPS tracker had been attached to a suspected drug dealer's vehicle by the Federal Bureau of Investigation. The suspect's vehicle was monitored and tracked for a month, but that fact was not the documented cause for concern by the courts. Rather, the court held that the action by the FBI of physically placing the tracker on the vehicle constituted trespassing and, thus, an illegal search.[8]

In a similar case, a federal court in Kentucky upheld that placing a GPS tracker on a suspect's vehicle did not violate the Fourth Amendment because law enforcement was not tracking the vehicle in real time—it was used only to monitor a "moment in time."[9] In other words, constant monitoring of a vehicle constitutes a violation of privacy whereas going back to determine whether a vehicle was in the area of a crime does not. In both cases, law enforcement attempted to monitor the location of the vehicle and used GPS as

---

[7] Daniel L. Doctoroff, "Reimagining Cities from the Internet Up," *Sidewalk Talk* (blog), November 30, 2016, https://medium.com/sidewalk-talk/reimagining-cities-from-the-internet-up-5923d6be63ba#.ubj2h5kdb.

[8] Rachel Levinson-Waldman, "Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public," *Emory Law Journal* 66 (March 2017): 527.

[9] United States v. Williams, No. 15-5432 (6th Cir. filed April 29, 2015).

the method to gather the information, but the rulings were vastly different. In *United States v. Jones*, the decision hinged on the FBI trespassing to place the tracker on the vehicle rather than the surveillance itself. These divergent rulings leave unanswered questions pertaining to surveillance in public places.

3. Law Enforcement's Use of Information

Collecting data is the easy part of policing in a smart city. Finding ways to make it useful to enforce laws and thwart criminal acts is the real challenge. Because collecting data is a vital component of developing a smart city, privacy issues arise. Thus, it is critical that policies are in place to address these issues.

In her thesis titled "Lawful Hacking: Toward a Middle-Ground Solution to the Going Dark Problem," Hoaithi Y. T. Nguyen tackles the debate of end-to-end encryption—embedded by private-sector technology companies—which prevents the government from gaining access to the information, even with a lawful warrant.[10] She concludes that a middle ground solution is one in which the homeland security enterprise performs its job within constitutional parameters and without sacrificing individual liberty.[11]

That middle ground has yet to be determined despite 50 years having passed since the landmark case *Katz v. United States*, which reviewed the FBI's wired surveillance outside a phone booth where a suspected criminal was conducting business. In this case, Justice Stewart ruled that "the Fourth Amendment protects people, not places."[12] He went on to say that a person inside a phone booth has a reasonable expectation of privacy and should have the assurance that one's conversation is not broadcast for anyone to hear.[13]

---

10 Hoaithi Y. T. Nguyen, "Lawful Hacking: Toward a Middle-Ground Solution to the Going Dark Problem" (master's thesis, Naval Postgraduate School, 2017).

11 Nguyen.

12 Katz v. United States, 389 S. Ct. 347, 351 (1967).

13 Richard S. Julie, "High-Tech Surveillance Tools and the Fourth Amendment: Reasonable Expectations of Privacy in the Technological Age," *American Criminal Law Review* 37, no. 127 (January 2000).

The case, which centered on the Fourth Amendment, has set the guiding principle for law enforcement pertaining to privacy.

To further illustrate the spectrum of police accountability, body-worn cameras have been implemented in roughly 18 percent of police agencies in the United States.[14] Questionable behavior by police has led to body-worn cameras and, with their implementation, a paradox surrounding the privacy of the individuals whom the police encounter. In the article "The Rise and Risk of Police Body-Worn Cameras in Canada," Thomas Bud questions whether the demand for police accountability outweighs a person's right to privacy when being recorded. He contends that it is unrealistic for an officer to seek and gain consent prior to the interaction.[15] The question remains whether a person has a right to privacy in a public place.

C. RESEARCH DESIGN

This research focused on the implications of data collection and whether it can be used to solve crimes without affecting a person's civil liberties—particularly in a venue where patrons opt into open-source technology. The Fourth Amendment protects citizens from unlawful searches and seizures, but it is silent on the definition of "search" as it pertains to open-source data. There is a growing need to ensure that collected data from private citizens are used within the parameters of department policy and do not infringe on individual rights.

1. Limits

Limited case law provided clear guidance on what information law enforcement can use to build a case against a person whose information is obtained in public spaces. A clear answer to the questions posed was unlikely without judicial guidance. Specifically, this research focused on downtown Aurora and RiverEdge Park—an open-air concert

---

14 Mike Maciag, "Survey: Almost All Police Departments Plan to Use Body Cameras," *Governing*, January 26, 2016, http://www.governing.com/topics/public-justice-safety/gov-police-body-camera-survey.html.

15 Thomas K. Bud, "The Rise and Risks of Police Body-Worn Cameras in Canada," *Surveillance and Society* 14, no. 1 (2016): 6.

venue where patrons opt into an interactive experience by connecting to Wi-Fi. By voluntarily opting in, what are the fine-print caveats to personal information that can be accessed by law enforcement?

2. Data Sources

This thesis used the implementation of smart city technology in RiverEdge Park and the downtown Aurora area as its main data sources to determine whether the Fourth Amendment can withstand the digital information collected in public places and how law enforcement can use that information.

- The Fourth Amendment to the U.S. Constitution served as the foundation for analysis and from which the cases were collected.
- Case law and court documents that correlate with the Fourth Amendment and the use of data by the government were explored.
- Reports and literature by the American Civil Liberties Union (ACLU) and other entities that challenge privacy protections for the digital age of widespread government surveillance were gathered.
- Possible scenarios of hypothetical incidents were explored to further determine the limitations (or exclusions) by law enforcement in evidence collection.
- Policy and literature that outline current policies and government practices pertaining to data collection were analyzed.

3. Type of Analysis

This thesis used thematic analysis, which examines themes and patterns within the data specific to the research question.[16] This method was applied to the following categories:

16 Virginia Braun and Victoria Clarke, "Using Thematic Analysis in Psychology," *Qualitative Research in Psychology* 3, no. 2 (January 2006): 77–101, https://doi.org/10.1191/1478088706qp063oa.

1. Background on the smart city initiative at RiverEdge Park

2. Timeline of the Fourth Amendment and case studies on the collection and retention of data

3. Intelligence-led policing

The analysis led to the following conclusions:

- Law enforcement agencies need a process or policy to collect and retain data from open sources.
- Intelligence-led policing is the catalyst for data collection, and data are being used to solve crimes.
- There is no such thing as privacy in a smart city, but citizens are not giving up privacy rights in exchange for crime reduction as long as law enforcement is not extending beyond the scope of the Fourth Amendment.

D. CHAPTER OUTLINE

Chapter II presents the smart city initiative for RiverEdge Park and an overview of what a patron can expect in a smart venue experience. Chapter III explores case law relating to the Fourth Amendment as the foundation for analysis. Then, the chapter analyzes court decisions involving privacy in a public space and introduces the Third-Party Doctrine as a method for law enforcement to collect data without a warrant. In Chapter IV, case law is applied to hypothetical crimes in public spaces, challenging Fourth Amendment tenets by presenting crime scenarios against the backdrop of emerging technologies. Chapter V concludes with recommended legislation to regulate the ownership of data collected in a smart city and the balance between privacy and public safety.

II. RIVEREDGE PARK: A SMART CITY VENUE FOR CONCERTS

As cities become more wirelessly connected, issues intensify around data collection and the ways in which a person's privacy and civil liberties are affected when opting in for an interactive experience in a public place. By choosing connectivity to enrich an experience, a citizen might not be aware of the mounds of data collected that might reveal one's identity and location among other information. When and how might smart cities strike a balance between data collection and a person's right to privacy as it pertains to government actors? These questions and their implications are explored in following one smart city's transformation.

A. BACKGROUND

Aurora, Illinois, evolved from a blue-collar railroad city to a cultural hub for arts and entertainment. As the second largest city in Illinois, Aurora has become a destination for those seeking art walks, open-air concerts, and award-winning theater.[17] As home to the Paramount Theater and RiverEdge Park, an open-air concert venue, the city attracts crowds who travel from Chicago and beyond the Illinois border to attend. The Paramount Arts Center attracts more than 36,000 subscribers every year to its professional productions.[18] The summer of 2017 attracted more than 100,000 people to RiverEdge Park.[19]

Because of these venues, Aurora has become known as a cultural hub for the arts. In 2018, the city received a $15 million tax credit from the Illinois Housing Authority for development of the Aurora Arts Center. The $35 million project will house a high-end

17 Marie Wilson, "RiverEdge Park Completes Longtime Aurora Vision," *Daily Herald*, June 10, 2013, http://www.dailyherald.com/article/20130610/news/706109913/.

18 "Mission & History," Paramount Theatre, accessed November 20, 2018, https://paramountaurora.com/about/.

19 "Be a Sponsor," RiverEdge Park, accessed November 20, 2018, https://riveredgeaurora.com/sponsor/.

restaurant and the Paramount School for the Performing Arts in the hopes of attracting more artists to Aurora.[20]

By the same token, Aurora has made vast improvements to its downtown area including the construction of an open-air concert venue, RiverEdge Park, to attract visitors. The $18.5 million venue was completed in 2013 and seats 8,500 people. Since opening, it has featured nationally known artists representing every music genre from classic rock to country. The venue brags a concrete area near the stage as well as lawn seats for those who prefer a more laid-back experience. The park houses separate buildings for the concessions, ticket sales, and food vendors, and because it sits along the Fox River, every seat includes a water view.[21]

1. The Vision for a Smart City

The success of these venues prompted Aurora mayor Richard C. Irvin to call for collaboration among department heads on a project that would bring an interactive experience to the patrons of the downtown corridor. His vision was to develop a smart city that chief information officer Michael Pegues describes as "a municipality that delivers first-class services to its citizens." Pegues believes that products and services should be delivered to employees and citizens in a way that streamlines bill payments, garbage collection, and educational opportunities.[22] Mayor Irvin's vision—to provide accessibility and connectivity to visitors and citizens of the second-largest city in the state—begins with the infrastructure already in place. The 100-square-mile network of underground fiber optic cables will supply the foundation of the tech corridor. Mayor Irvin envisions a more pedestrian-friendly downtown where services are delivered, and citizens are engaged. Part of the plan is to develop "smart parking," so citizens and visitors can easily find parking

---

20 Steve Lord, "Work Begins on $35 Million Downtown Aurora Arts Center," *Aurora Beacon-News*, October 11, 2017, http://www.chicagotribune.com/suburbs/aurora-beacon-news/news/ct-abn-aurora-artscenter-st-1012-20171011-story.html.

21 Wilson, "RiverEdge Park Completes Longtime Aurora Vision."

22 "Episode 32: Aurora Lights Up Smart Cities," YouTube video, 57:35, posted by Constructech TV, August 6, 2018, https://www.youtube.com/embed/7K9PZKrikKg.

by using an app that directs them to vacant spaces. This solution will alleviate the congestion caused by cars circling the downtown area looking for parking.[23]

The implementation of the smart city strategic plan is expected to be completed within three to five years. Public–private partnerships will defer costs for shared services. Private industry can help deploy services where there is a mutual interest. For example, kiosks throughout the downtown area will offer citizens an interactive platform for information on restaurants, entertainment, and scheduled events in the area. The goal, according to the mayor, is not only to recoup costs through advertising but also to engage the citizens, so they feel a part of the community.[24]

In an effort to make the tech corridor user-friendly and provide connectivity to citizens, the mayor intends to use a GPS satellite network as well as radio frequencies to create virtual boundaries around designated areas. The concept, called "geofencing," relies on the GPS functionality of smartphones, which most people carry.[25] If visitors who have the GPS capability cross the virtual boundary around the downtown corridor and RiverEdge Park, they can receive information on their smartphones.[26]

Whether patrons attend a sporting event or a concert, they have come to expect connectivity. In large measure, this expectation is a result of individuals documenting and sharing their experiences instantly with friends and families on social media. In some cases, this means sharing with others at the same event. Event organizers want spectators to stay at the venue rather than leave to find internet connectivity. The top priority for any venue is to ensure that patrons are staying put. That translates into more food and beverage sales inside the stadium.[27] Technological changes, in this case, have a direct and measurable return on investment for the provision of services at the venue.

---

23 Constructech TV.

24 Constructech TV.

25 Jason Fitzpatrick, "What Is 'Geofencing'?," How-to Geek, September 21, 2016, https://www.howtogeek.com/221077/htg-explains-what-geofencing-is-and-why-you-should-be-using-it/.

26 Fitzpatrick.

27 Trips Reddy, "10 Ways Stadiums & Venues Are Using Technology to Delight Fans & Keep Them Coming Back," Umbel, September 29, 2015, https://www.umbel.com/blog/publishers/10-ways-stadiums-are-using-technology-to-delight-fans/?cn-reloaded=1.

With end-to-end connectivity at the venue, methods to improve a patron's experience are becoming more commonplace. Among them are a robust wireless network solution, mobile applications, and digital kiosks—all of which are initiatives the Aurora mayor plans to move forward.[28] The availability of free Wi-Fi and access to mobile applications, with opportunities to try new apps, complete surveys for discounts, and document experiences, encourage others to attend future events.

2. RiverEdge Park as a Smart Venue

A robust wireless network is already built into the infrastructure of Aurora through a fiber optic network that runs underground and provides more than 19 gigabytes of Ethernet fiber across the city.[29] The connectivity extends to the River Edge Park concert venue as part of its 82-mile fiber ring (see Figure 1).[30]

Figure 1. Fiber Optic Network at RiverEdge Park

Powerful connectivity in the park is the foundation upon which other forms of technology will be implemented. According to Michael Pegues, "A smart park influence will drive

---

28 Reddy.

29 "Transforming City of Lights to City of Light Speed," OnLight Aurora, November 20, 2018, http://www.onlightaurora.com/.

30 Steve Lord, "Aurora Looks to Expand Fiber Optic Network Downtown," *Aurora Beacon-News*, February 26, 2018, http://www.chicagotribune.com/suburbs/aurora-beacon-news/news/ct-abn-aurora-fiber-st-0227-20180226-story.html.

economic development, enable local business, develop innovative revenue streams and enhance Aurora's identity—all of which will enrich citizen experience."[31] Aurora plans to use both mobile applications and kiosks to leverage information-sharing among citizens and visitors. These platforms will allow Aurora to push out public safety information, weather advisories, and even coupons to nearby restaurants.[32]

Phase one of the smart park initiative in Aurora is well underway with projected completion in 2019.[33] Future phases include plans to install cameras inside the park, so security personnel can monitor events. This surveillance will help alleviate the workforce and coverage limitations of police officers. Other considerations for future phases include tethered drones to capture a birds-eye view of the park, facial-recognition software, parking sensors, and smart lighting.[34] Tethered drones have become an observation tool for law enforcement because they improve situational awareness across a venue and contribute to resource deployment. For example, medical evacuation decisions can be made more quickly with information from above. The facial recognition component has great utility for the ordinary lost car or lost tickets and specific utility for lost children who may have been molested or kidnapped. Law enforcement can also use the capability to monitor the origin of aggression, fraud, or diversion or to track a malevolent actor.

The consumer has the option to join, or "opt in," the Wi-Fi geofence to benefit from the services that the venue intends to market to its customers. The most important part of any geofence strategy is getting people to opt in voluntarily, participate actively in the goods and services offered at the venue and, on an individual level, use the capability as a safety net. The consumer instantly receives a notice of hazards and warnings, instructions for response and evacuations, and means to report suspicious activity. Without participation from consumers, efforts to push information are futile.[35] The companies that

---

31 Michael Pegues, "COA River Edge Smart Park" (presentation, Smart Park, Aurora, IL, 2017).

32 Richard C. Irvin, "Prioritization of Information Technology Initiatives" (lecture, Alarm Detection Services, Aurora, IL, July 11, 2018).

33 Irvin.

34 Irvin.

35 "The Top 4 Things You Should Know about Geo-Fencing," *Survey Sampling International* (blog), May 27, 2013, https://www.surveysampling.com/blog/top-4-things-know-geofencing/.

set up geofencing for marketing purposes stress that the data collected from those who opt in are as necessary as the information delivered to them. These companies suggest that a city collects data on users' demographics, historical data, and movements.[36] These data are typically stored by vendors on computer servers. The data may exist in cloud-based storage or in a location where the storage provider maintains servers. Data that are stored inside the United States are normally protected, and the government must follow procedures to gain legal authority to gain access. However, data stored in other countries do not involve the same regulations and legal parameters.[37] The information used for marketing and commerce is accessible to those who are not government actors; however, the legal authority for the government to intercept information depends on the extent of oversight in the country in which the data is stored. Most consumers do not think about who can access their data until they are intercepted by the government and subject to an unreasonable search and seizure.

While the end user benefits from coupons and information that are relevant to their experience at a shopping center—in Aurora's case, River Edge Park and the downtown district—the greater benefactor is the city itself. By determining users' demographics and movements, data can predict where they are likely to shop and dine and entice those actions with incentives. When a business or city can detect human patterns, it can predict future behavior.[38]

3. Before Smart Venues

Attending an event before the inception of smart technology fell into the "you don't know what you don't know" category. Ticket sales required going to the box office or calling a phone number. The tickets arrived in the mail or awaited the patron at will call, which required standing in line. After driving around several city blocks multiple times to find parking and waiting in line to retrieve his tickets, he joined another line to enter the

---

36 "The Top 4 Things You Should Know."

37 Mike Talon, "Cloud 101: Geofencing," *Stratoscale* (blog), https://www.stratoscale.com/blog/cloud/cloud-101-geo-fencing/.

38 Michael Boland, "Mobile & Local Join the Big Data Movement," Search Engine Watch, August 17, 12, https://searchenginewatch.com/sew/opinion/2199396/mobile-local-join-the-big-data-movement.

venue. One could expect more lines for concessions and restrooms inside the venue and no connectivity with Wi-Fi.

Now that connectivity is commonplace within and around venues, patrons expect an interactive experience, and Aurora is on the verge of delivering by increasing the amount and variety of choices in real time. Connectivity includes access to tickets, requests to change seats, memorabilia purchases in advance, and food ordering—with the option at some venues to explore nutritional information depending on one's dietary requirements or food allergies. The capability keeps lines moving and encourages crowdsourcing solutions whereby patrons answer questions and share information, which can save time and lower frustration levels. For law enforcement, the moving lines increase a sense of order and customer satisfaction, which reduces potential conflict.

4. The Smart Venue Experience

The technological application becomes more realistic to the end user when it chronicles the journey of a concert-goer through her own lens. It begins with the purchase of the ticket. Since 2010, most venues have eliminated paper tickets, resulting in the reduction of long lines of entry, a solution to stolen or lost tickets, and a decrease in counterfeiting and scalping.[39] Computer and mobile applications now provide a platform for purchasing a ticket, eliminating the paper, and replacing it with a bar code. With the mobile ticket accessible on a patron's smartphone, attending the concert unfolds through a series of events.

Finding parking on the day of the event can be a cumbersome experience for the concert-goer, but using the parking sensor application that Aurora intends to implement, the patron simply clicks on a smartphone app and determines the parking places available a short distance from the entrance of the venue. Unlike driving city blocks to search for parking, sensors installed in the parking places alert users to vacancies, and drivers are able to reserve spots. Payment information is obtained upon downloading the app, so paying for

---

[39] Paul Farhi, "'Paperless Ticketing' Aims to Thwart Scalping at Concerts, Sports Events," *Washington Post*, July 5, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/07/04/AR2010070404180.html.

parking is as simple as a click on the smartphone. The GPS locator guides the driver to the parking place and eliminates the time and frustration of locating parking. It also helps the patron locate one's vehicle after the event. This is particularly helpful if families or colleagues get separated because they can converge by agreement on the location of the vehicle.

The walk from the parking spot is only a few blocks from the venue, and upon exiting the vehicle, the patron enters a pre-programmed geofence that outlines the perimeter of downtown Aurora. An alert appears on the patrons' mobile phone welcoming them to downtown Aurora and offering an opt-in to the Wi-Fi geofence. If the patron accepts, her location is logged. As the patron walks to the venue, an alert appears on her smartphone offering a coupon for appetizers and cocktails at a restaurant in proximity.

Once the concert-goer has an opportunity—should she choose to visit the downtown establishment—she travels to the venue to attend the concert. The mobile app is designed to collect GPS data on the movements of the patron via her smartphone, and once the app determines she has been standing in line for more than a few minutes, it pushes an alert to her mobile device that reads "You have been standing in line for 8 minutes. Enjoy 50% off at the concession stand once you enter the park." A discount on food and beverage is designed to recognize and reward the patron for her patience.

The line moves quickly, and at the entrance, the patron presents the mobile app from which the barcode is scanned quickly and efficiently. Once inside, the patron finds a location inside the park with views of the stage as well as several jumbo-screens that allow viewing of the concert from all angles.

The patron is alerted to a push-notification that advises there is a 20 percent chance of rain during the open-air concert. The advisory promises to keep the patron informed of any precipitation changes or announcements pertaining to the weather.

Once settled in the park, the patron enjoys a beverage, and the lights in the venue dim, signaling the start of the concert. Another alert pushed to the mobile device advises that the restrooms at the south end of the lot have the shortest line in the event nature calls. In addition, a map of the park appears on the smartphone diagraming the food vendors

located throughout the venue. The patron is also advised where to find the first aid tent and security.

The concert is well underway, and the crowd is enjoying themselves and singing along with the band. The patron is completely unaware of the presence of a tethered drone 400 feet in the air that serves as a bird's-eye monitor of the park. The patron is also unaware of the surveillance cameras positioned throughout the park that allow security and law enforcement officers an unobstructed view from end to end.

A locked room that sits above the main floor houses members of law enforcement who monitor the cameras to ensure the safety and security of all attendees. They watch for activity that might indicate a suspicious person or package that threatens the peace and well-being of the patrons. Should the cameras detect a threat of any kind, the monitors communicate with law enforcement in real time on the ground to investigate.

The patron is unaware of the monitoring, and after the encore performance, she packs up and exits the park. Once again, an alert on her smartphone invites her for a nightcap at the pub nestled along the path to the patron's vehicle. The parking app has already sent a reminder that her space expires in 45 minutes, so there is no hurry to get to the vehicle. As the patron walks in the downtown area, motion sensors illuminate the streetlights. The patron stops at a kiosk located nearby and touches a tab that provides information about upcoming events in downtown Aurora. The patron walks to the parking place, enters her car, and drives home—while mentally planning her next trip to an Aurora event.

While the connectivity was useful to the customer, ongoing push notifications and alerts are also potential distractions to a person who is walking or driving. The debate is whether being constantly connected is value-added or value-subtracted.

5. Policing a Smart Venue

The patron has opted to share information as specific as her physical location, and by voluntarily acknowledging via a privacy policy that the data collected will be used by the city, the patron freely permits the use. A privacy policy is a statement that declares to

the user how her information is collected, stored, and released. It informs the user of how the city intends to use the information collected, and with whom that information can be shared.[40] If the user accepts the privacy policy, she accepts the terms associated with the use of her personal data. This permission dictates precisely how the city of Aurora uses the data collected by visitors who opt in—to market the city and entice citizens to spend money in the downtown area.

B. CONCLUSION

As cities like Aurora have become smarter and the world has become more connected, the privacy and legal implications pertaining to data collection and dissemination have intensified. A delicate balance must be struck that affords the consumer the convenience of connectivity while prohibiting personal data from being shared with government actors that might attempt to use that data. Law and technology are intersecting, and the regulatory efforts require further exploration of how citizens can expect privacy in plain sight.

40 Business Dictionary, s.v. "privacy policy," accessed August 7, 2018, http://www.businessdictionary.com/definition/privacy-policy.html.

III. PRIVACY IN PUBLIC SPACE CASE LAW

The Fourth Amendment in the Constitution of the United States is the source of most of the legal framework on privacy issues. It reads, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[41]

The following questions must be asked in administering the Fourth Amendment:

- Was there a search?
- Was there a seizure?
- Was any search or seizure of "persons, houses, papers, [or] effects"?
- Was any such search or seizure reasonable?[42]

If a search or a seizure of a person or things is unreasonable, it violates the Fourth Amendment. This applied standard seems relatively simple; however, there has been much dissent over domain in the interpretation of this standard because "people have different expectations of privacy in different circumstances, relationships and time periods."[43] The complexity of the standard has evolved in the digital age along with advancements in communications and digital technology. For example, it is unclear whether facial recognition software that captures the identity of a person constitutes an illegal search. Similarly, is there an expectation of privacy when a consumer voluntarily opts into a Wi-Fi geofence? The Fourth Amendment application is not as clear-cut regarding these technological advancements.

---

41 U.S. Const. amend. IV.

42 Jim Harper, "Administering the Fourth Amendment in the Digital Age," National Constitution Center, accessed July 13, 2018, https://constitutioncenter.org/digital-privacy/The-Fourth-Amendment-in-the-Digital-Age.

43 Griffin, "What Does It Mean to Be Secure in One's Person, Papers, and Effects?," *RedState* (blog), September 23, 2013, https://www.redstate.com/diary/griffinelection/2013/09/23/what-does-it-mean-to-be-secure-in-ones-person-papers-and-effects/.

A. THE DEVELOPMENT OF THE CASE LAW

The following court decisions reveal a journey through the information age. Technology has become a useful tool for law enforcement in investigating crimes, but the complexity of the law's application has increased with advancements in technology.

1. *Olmstead v. United States*: Wiretapping Does Not Constitute a Search

When electronic surveillance emerged as a technology, the 1928 decision in *Olmstead v. United States* determined that wiretapping a home of a suspect did not constitute a violation of the Fourth Amendment because law enforcement did not actually enter the suspect's home. Furthermore, the court ruled that conversations captured via wiretapping did not fall into the categories of "papers and effects." [44] *Olmstead* remained the presiding case for many years until the Fourth Amendment standards were tested as innovation evolved.

2. *Katz v. United States*: A Departure from Protecting Places

In 1967, *Katz v. United States* reversed *Olmstead* by a majority ruling that focused on exposure. Mr. Katz had entered a public phone booth to make illegal gambling bets. Unbeknownst to him, the FBI was recording his conversations through a listening device that they had attached to the phone booth. Katz was arrested and convicted as a result of the recordings. Justice Potter Stewart opined that Katz had physical protection when he entered a phone booth, and thus, his conversations inside were not privy to the public:

> The Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. However, what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[45]

---

[44] Olmstead v. United States, 277 S. Ct. 438 (1928).

[45] *Katz*, 389 S. Ct. 347.

3. *Kyllo v. United States*: The Difference between the Eye and the Ear

The state argued that when Katz entered a glass phone booth, he was not attempting to conceal himself from the public, and thus, he had no expectation of privacy. However, the court wrote, "What he sought to exclude when he entered the both was not the intruding eye—it was the uninvited ear." [46]

Following the theme of technological advancement, a 1992 case involving a similar methodology of surveilling a home was heard by the Supreme Court in *Kyllo v. United States.* The U.S. Department of the Interior had applied a thermal imaging device outside a defendant's home. The imaging did not capture conversations, nor did it have the capability to determine the activities of the people inside. However, agents were able to detect heat emitting from the house, which caused them to discern there was a significant amount of light inside the home. Acting on reasonable suspicion from facts previously gathered, the agents deducted that the light was sufficient probable cause to seek a warrant for the defendant illegally running a marijuana grow house. Federal agents sought and secured a warrant and seized 100 marijuana plants in the home. The defendant was arrested and convicted, but once the defense appealed to the Supreme Court, his conviction was overturned on the grounds that thermal-imaging devices constituted a search under the Fourth Amendment.[47]

The *Kyllo* opinion set a precedent on devices aiding the government in a search of a person's home by overturning the applied standard. Orin S. Kerr points out that these decisions offer clarity regarding homes but leave law enforcement in the dark regarding government surveillance in public places:

> On the one hand, the Fourth Amendment extends constitutional protections to a person's "houses, papers and effects" from unwarranted government interference. . . . On the other hand, the Fourth Amendment offers no protection from government surveillance in public.
>
> Just as a person voluntarily exposes himself to observation by traveling in public to deliver communication, so does a person voluntarily expose

46 *Katz*, 389 S. Ct. 347.

47 Kyllo v. United States, 533 S. Ct. 27 (2001).

> himself to observation by hiring an agent to deliver his communications remotely.[48]

The aspect of the phone booth in the Katz case seems to contradict Kerr's opinion that there is no protection from the government in a public place. The court ruled that a person in a public phone booth *does* have a reasonable expectation of privacy, but it did not define privacy in public where there is no physical concealment.

The aforementioned cases have solidified the Fourth Amendment as the legal standard even as technology has emerged that would aid the government in conducting searches of persons, homes, or effects. Even in cases where a person's right to privacy is open to interpretation, the courts have provided a strong opinion on government interference. However, how does the Fourth Amendment apply to the government using a third party as a means to gather evidence for a conviction?

In 1976 in *United States v. Miller*, the Supreme Court held that the government could legally obtain the bank records without a warrant of a man who possessed an illegal whiskey still and was carrying out the business of a distillery without paying taxes.[49] The court found that a person who voluntarily turns over information to a third party has no expectation of privacy: "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[50]

Smith v. Maryland (1989) adds another element to an already complex process of determining grounds for reasonableness in a search. In this case, a female was the victim of a robbery. She was able to discern that a Monte Carlo vehicle at the scene likely belonged to the robber. Shortly after the robbery, the self-identified offender began calling the victim and threatening her. On one occasion, he advised her to step outside her home; when she did, she observed the same Monte Carlo. The victim provided this information to the police, who noted a Monte Carlo matching the description was driving in the area of the victim's home. They were able to ascertain the registered owner—Smith—from the license plate.

---

48 Ariane de Vogue, "Supreme Court Takes on Major Fourth Amendment Case," CNN, November 29, 2017, https://www.cnn.com/2017/11/29/politics/supreme-court-fourth-amendment-case/index.html.

49 United States v. Miller, 425 S. Ct. 435 (1976).

50 *Miller*, 425 S. Ct. at 751–752.

Because the suspect had been calling the victim via telephone, law enforcement contacted the phone company, which at the behest of police, installed an electronic device on the suspect's telephone. The device allowed the police to capture the telephone numbers the suspect dialed from his phone. The police did not obtain a warrant before requesting that the phone company install the device.[51] The recorded digits revealed that Smith called the victim's home again. Based on this evidence, the police obtained a search warrant and found a phone book opened to the page containing the victim's name. Smith was arrested and eventually indicted for robbery.[52]

Smith sought to suppress the evidence retrieved from the pen register based on a violation of the Fourth Amendment. The state argued that the police had not retrieved the information from the pen register—the phone company had. Therefore, it was not a government intrusion. The state further argued that Smith had a reasonable expectation of privacy in communication over a telephone, but the numbers dialed did not. The judges did not agree and applied the same standard as was applied in *Katz v. United States*. Just as it was determined that Katz had a reasonable expectation of privacy inside a phone booth, so did Smith inside his home.[53] Nevertheless, the state successfully argued that while Smith had a reasonable expectation of privacy from the government, the phone company—a third party that not only installed the pen register but also kept records of phone calls—was immune from the Fourth Amendment.[54]

B. THIRD-PARTY DOCTRINE

These cases established the theory of what would become known as the "third-party doctrine." The third-party doctrine is a controversial legal theory maintaining that when information is voluntarily provided to a third party, it loses its Fourth Amendment protection. For example, if a drug dealer tells an informant of his plans to break the law or

51 Smith v. Maryland, 442 S. Ct. 735 (1979).

52 *Smith*, 442 S. Ct. 735.

53 *Smith*, 442 S. Ct. 735.

54 *Smith*, 442 S. Ct. 735.

a white-collar criminal discloses his misconduct to an accountant, the government may collect evidence from these ancillary individuals.[55]

The third-party doctrine is simple: a person who discloses criminal acts to a third party gives up his Fourth Amendment rights pertaining to the information. The Supreme Court ruled on this matter in *United States v. Miller*:

> The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[56]

1. *United States v. Jones*: Implications of the Third-Party Doctrine

In a more recently decided case in 2012, *United States v. Jones*, the police installed a GPS tracking device directly onto the suspect's vehicle without using a third party to collect the data. The Supreme Court ruled in favor of Jones, and the justices voted unanimously that it was a Fourth Amendment intrusion to install a tracking device on a vehicle without a warrant. However, they were split five to four on the reasons behind the ruling. The majority held that the police committed a trespass against Jones's personal effects by installing the GPS.[57] Justice Sotomayor specifically highlighted her uneasiness with the tenet of third-party doctrine:

> Fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[58]

---

55 Orin S. Kerr, "The Case for the Third-Party Doctrine," *Michigan Law Review* 107, no. 561 (February 2009): 42.

56 *Miller*, 425 S. Ct. 435.

57 United States v. Jones, 132 S. Ct. 945 (2011).

58 *Jones*, 132 S. Ct. 945.

Justice Sotomayor's strict interpretation of the third-party doctrine triggered a debate between Greg Nojeim, senior counsel at the Center for Democracy and Technology, and George Washington law professor Orin Kerr. Nojeim argued that in the digital age, the third-party doctrine no longer serves customers and leads to absurdity given that the majority of information is communicated through an intermediary. Kerr disagreed, arguing that the doctrine should apply when information is provided to a third party and not merely when information moves through that third party. For example, if a criminal leaves tangible evidence of his crime on his friend's desk, to whom does it belong? Can the police file a court order to obtain the records, or are they still the property of the criminal?[59]

2. Metadata

This question shifted dramatically when it was discovered in June 2013 that the Nation Security Administration had been collecting the metadata of millions of phone customers. The thought prior to this discovery was that third-party data were only applicable to a small number of people who were suspected of committing crimes. Once everyone's data were collected, the question of constitutionality arose. Although conversations were not being recorded, the phone numbers and duration of calls were.[60]

It is appropriate to consider whether the Fourth Amendment holds up in the age of modern technology in the same way it did when *Smith v. Maryland* was decided. Michelle Richardson, an attorney at the ACLU, argues that *Smith* was decided at a time when people were using only landlines to communicate, and the data collected were not as sophisticated and voluminous as the data being collected today:

> It's incredibly rich data, which is why they want it so bad. Because everyone was using landlines when Smith v. Maryland was decided, getting metadata did not mean getting information about whenever a cellphone connected to which tower or transmitted GPS coordinates to a provider. So back then,

---

59 John Villasenor, "What You Need to Know about the Third-Party Doctrine," *Atlantic*, December 30, 2013, https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/.

60 Villasenor.

> location tracking was a much more onerous affair, requiring so many resources it was only used for the most serious investigations.[61]

Richardson believes *Smith v. Maryland* is "way out of date. . . . It was before cell phones, before the Internet, before services that collect intensely personal information."[62]

C. *CARPENTER V. UNITED STATES*: LANDMARK CASE

United States v. Jones was decided by the Supreme Court based on the government physically trespassing to place the GPS tracker, but the justices, in a concurrent opinion, questioned whether the *Smith v. Maryland* case would have held in the age of modern technology.[63] The lingering question centered—and centers—on the fact that Americans carry a cell phone with them at all times. The cell phone is continually communicating with cell towers to provide GPS positioning, so a person's location is known. The question is whether the government can access that information without a warrant.

A 2018 Supreme Court decision answered the question in *Carpenter v. United States.* The dispute began back in 2011 when four men were arrested for robbing a number of cell phone stores over the course of a year. The defendant, Timothy Carpenter, was not among those arrested. However, one of the offenders confessed to the robberies and turned over his cell phone to the FBI.[64] The agents requested a subpoena to access information from different wireless phone companies, so they could determine with whom the offender was communicating during the time of the robberies. The FBI was required only to seek information or evidence that was pertinent to its investigation.[65] From the data collected, the FBI learned that Carpenter had been in proximity of four of the armed robberies and

---

61 Andrea Peterson, "The NSA Says It 'Obviously' Can Track Locations without a Warrant. That's Not so Obvious," *Washington Post*, December 4, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/12/04/the-nsa-says-it-obviously-can-track-locations-without-a-warrant-thats-not-so-obvious/.

62 Peterson.

63 Peterson.

64 Carpenter v. United States, No. 16-204 (S. Ct. June 22, 2018).

65 Nina Totenberg, "Justices May Impose New Limits on Government Access to Cellphone Data," NPR, November 29, 2017, https://www.npr.org/2017/11/29/567348000/justices-may-impose-new-limits-on-government-access-to-cellphone-data.

arrested him on several counts of aiding and abetting. He was sentenced to 1,359 months in federal prison.[66]

Carpenter's defense argued that the government's accessing of his location through the geo-location of his cell phone constituted an illegal search. The defense further argued that the third-party doctrine did not apply because those who use cellular devices do not share such information of their own volition. In what seems like an implausible defense, Carpenter's team claimed that his location should not be privy to the government because he carries his cell phone with him at all times and his location is continually updated—even at home where there is an expectation of privacy.[67] The government argued that the third-party doctrine was applicable because the cell phone companies, not Carpenter, owned the records. The losing argument was that when people agree to hand over their information to a third party, it no longer belongs to them.

Prior to Carpenter, the courts had ruled that in cases involving cell phones, locations were privy to the government as part of an investigation. This landmark case has proven that the Fourth Amendment protects data that are turned over to a third party. Investigators now must obtain a warrant, which requires a higher standard of probable cause than suspicion. This was a significant victory for those who have been fighting for more privacy and less government intrusion.

It is important to note that *Carpenter* did not overturn the aforementioned cases. Nor did the court expound on other cell phone issues that have been raised—not relating to this case—such as information from real-time cell site locations or geofencing. Thus, there are still lingering questions pertaining to privacy in public.

---

66 United States v. Carpenter, 819 F.3d 880 (6th Cir. 2015).

67 Stephen A. Miller and Rachel Collins Clarke, "Supreme Court Tackles Fourth Amendment Case Involving Cellphone Privacy," Legal Intelligencer, February 7, 2018, https://www.law.com/thelegalintelligencer/sites/thelegalintelligencer/2018/02/07/supreme-court-tackles-fourth-amendment-case-involving-cellphone-privacy/.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. HYPOTHETICAL CRIMES IN PUBLIC SPACES

He loses his power when we know his face.

—Michelle McNamara, *I'll Be Gone in the Dark*

The smart city concept offers a unique testing ground for balancing individual privacy and public safety. This chapter explores how digital data might be used by law enforcement within the parameters of the Fourth Amendment to investigate crimes in a smart city. Furthermore, it applies smart city technologies to hypothetical crimes as a way of exploring the boundaries of constitutional law.

A. GIVE ME YOUR PURSE!

The Aurora downtown is considered safe according to data collected on violent crimes in the city. The patrons who live, work, and attend events in the downtown area do so without overwhelming fear of being victims of crime. However, even in the areas with a low crime index, there is still a risk. Patrons are not immune from becoming victims of crime, whether it be from a person with criminal intent or an opportunist looking to monopolize on a moment. The ideal smart venue experience described in Chapter II describes the patron of downtown Aurora attending an evening event without incident. An alternate ending in which nefarious, criminal activity occurs explores the use of data collection under the Fourth Amendment.

Just as the patron walks away from the kiosk and toward her vehicle, she is confronted by a man who blocks her path and demands she hand over her purse. Before she can think or act, the man forcefully rips the purse from her shoulder and scurries away. The victim is left standing on the sidewalk and paralyzed with fear. Thankfully, she remembers that her phone is in her pocket and quickly retrieves it to call 9-1-1. When the police arrive, she is still shaken but able to provide a description of the offender through her hazy recollection. She knew he was a white male with scruffy facial hair wearing a

black t-shirt with a logo on the chest. She believes she saw a tattoo on his forearm as he reached to grab her purse, but as with the logo, she cannot provide specifics.

The police officers set up a perimeter around the downtown area in the hopes they can contain the offender while they conduct a grid search. They radio the description to the other units and begin canvassing for witnesses. Because Aurora utilizes smart city technology, the officers contact the city to determine what data can be extracted from the servers to capture a digital footprint of the offender.

1. Geofence

The city's geofence around downtown is a boundary, but it does not necessarily expose an end user's location. The user must voluntarily reveal his or her location by enabling GPS services on one's phone to be contacted by the geofence.[68] Location-based services allow users to receive information about points of interest in proximity. These services can provide users with information on restaurants or bars in the area.[69] The primary function of the geofence is for marketing the city; however, GPS on cell phones exposes users by providing their locations, which may be beneficial to law enforcement but problematic for those wishing anonymity.[70] In this scenario, the robber's location services might have been activated, thus leaving law enforcement a clue in determining his identity.

2. Kiosk

The downtown area is equipped with kiosks that provide residents and visitors a place to explore upcoming events and nearby shopping or establishments. Some kiosks require that visitors enter an email address to receive coupons and special offers. By

---

68 Bryan Bonack, "Geofences: What They Are, What They Aren't, and Why They're Effective," *Geospatial World* (blog), July 9, 2018, https://www.geospatialworld.net/blogs/geofences-what-they-are-what-they-arent-and-why-theyre-effective/.

69 Ben Niu et al., "Enhancing Privacy through Caching in Location-Based Services," *IEEE Conference on Computer Communications* (2015): 1025, https://doi.org/10.1109/INFOCOM.2015.7218474.

70 George Avalos, "Location-Based 'Geo-Fencing' Apps Raise Privacy Concerns," Science X Network, January 5, 2012, https://phys.org/news/2012-01-location-based-geo-fencing-apps-privacy.html.

collecting email, the city may create a mailing list for marketing purposes. Naturally, the end user can unsubscribe; however, most consumers are interested in learning about upcoming events at the locations they frequent.

New customer-facing kiosks do more than collect emails. A new wave of technology utilizes cameras in kiosks to collect physical data on consumers. For example, the camera can collect physical data points that recognize age, gender, and even clothing. By determining the patron's age and gender, the kiosk can be programmed to tailor marking to that demographic. A consumer estimated to be in his or her twenties might receive information on nightclubs in the area while an older patron might appreciate information on fine dining. The kiosk can also push options for cheeseburgers rather than salads for a person who is heavier in the computer's estimation.[71]

It is plausible that the perpetrator's identity might have been captured by the kiosk camera. This would depend on whether the offender is a nefarious actor who would be cautious enough not to leave a digital trace or, conversely, a careless criminal who lacks the prowess to cover his tracks. Kiosk companies assure the public that the cameras are not "spying on people," the data are merely collected on those walking by the sign for the purpose of marketing, and no information is saved.[72] However, law enforcement is banking on accessing images on the servers to use as evidence in a crime.

Under the Fourth Amendment cases outlined in Chapter III, the *Katz* privacy test delineated that citizens are afforded a "reasonable expectation of privacy." This threshold has established reasonable police action under the Fourth Amendment, and the digital age is testing this doctrine. Recalling *Katz*, the courts ruled that installing a GPS tracker on a vehicle was considered an intrusion. The two-prong test in *Katz* first determines whether

---

71 Patrick Thibodeau, "Kiosks Are Looking at You, Too," InformationWeek, October 25, 2017, https://www.informationweek.com/big-data/ai-machine-learning/kiosks-are-looking-at-you-too-/d/d-id/1330207.

72 Thibodeau.

there is an expectation of privacy. Second, it requires society—a subjective body—to determine whether there is a reasonable privacy expectation.[73]

Given this summation, the geofence falls outside the scope of privacy given that a person sharing one's GPS location makes a choice. If one turns off location services, the geofence does not trigger a user's location. Furthermore, a kiosk capturing an email voluntarily is subject to a government search. Cameras inside a kiosk collecting images as people walk by seem to fall outside the scope of *Katz*.

In *United States v. Jones*, the Supreme Court ruled that law enforcement violated the Fourth Amendment when it placed a GPS tracker on a vehicle without a warrant.[74] Officers tracked Jones's vehicle for 28 days, and the court determined Jones had a reasonable expectation of privacy pertaining to his movement. Applying this case to geofencing is not suitable because Jones's movements were traced without his knowledge. By contrast, a person who crosses a geofence is alerted on one's smartphone. In the Jones case, Justice Alito acknowledged that new technology would bring new questions regarding a person's diminished privacy in exchange for convenience.[75] The "convenience" piece is not easily interpreted as one person's perception of "convenience" might differ from another's. Geofencing and kiosks might be perceived as welcoming to one person who appreciates the perks and notifications while intrusive to someone else.

B. CATCHING A CRIMINAL

The concert at River Edge Park is in full swing on a sweltering Saturday night in August. The band is belting out its set, and the crowd is on its feet, singing along. The concession lines for beer have been steady all evening, and most of the attendees are enjoying libations and the atmosphere without incident. However, in one corner of the park, an overserved patron is growing belligerent and stumbling into people. Another male patron has grown impatient with the other man's aggression and asks the inebriated man

---

73 Margaret Hu, "Cybersurveillance Intrusions and an Evolving Katz Privacy Test," *American Criminal Law Review*, 55, no. 127 (2018).

74 *Jones*, 132 S. Ct. 945.

75 Hu, "Cybersurveillance Intrusions."

to leave the area. The request only angers the drunk man, and he barrels toward the stranger and gives him a shove that knocks him over. A group of bystanders quickly rush to subdue the drunkard, and mayhem ensues. One man rises from the pile and declares that he has been stabbed and is bleeding profusely from his stomach.

Law enforcement officers scanning from the security perch above the park notice what appears to be a fight in the crowd, so they summon ground security to the location. Officers arrive, and they locate a man lying in a pool of blood. They quickly attempt to ascertain what occurred and determine the man was stabbed but are unsure by whom. The drunken, belligerent man whom witnesses say started the fight is not in the immediate area. He seems to have vanished, and no one knows whether he was alone or with someone else. The officers summon medics, get a description of the alleged offender, and radio the security office. A drone is launched over the crowd, and the officers begin conducting a grid search to locate the offender. The drone is equipped with facial recognition software, which scans the crowd for wanted subjects and known individuals registered in the database.

Police officers on foot are attempting to locate the alleged offender in the venue. After receiving a report from those at the park exits that no one matching the man's description has left, they check the restrooms and other areas in the park where he might have concealed himself. Meanwhile, the officers are in contact with Aurora's technology department to gather a list of those who opted into the concert venue's geofence via smartphone. In addition, the ticket office extracts a compilation of those who purchased tickets via credit card to gather the identities of those inside the park. The remaining security staff begins to review the footage of the fixed cameras in the park to identify the offender in the stabbing and push out a still photo for identification purposes.

1. Drones

Drones are a new tool for law enforcement, and legislation outlines the parameters in which police can use them. As of May 2018, the Center for the Study of the Drone at Bard College estimated that at least 910 emergency service agencies in the United States

are operating drones. The center estimates that drone acquisition by law enforcement agencies has increased by 82 percent over a one-year period.[76]

With the growing rate of drones used in policing efforts, legislation has been enacted that provides guidelines for law enforcement. The Illinois Compiled Statutes specifically prohibit law enforcement from collecting data except when it "possesses reasonable suspicion that, under particular circumstances, swift action is needed to prevent imminent hard to life, or to forestall the imminent escape of a suspect or the destruction of evidence."[77]

The ACLU takes a strong stance against the use of drones. The ACLU's director of police practices argues, "If there are drones hovering above First Amendment activities, people will stay home."[78] That may be true, but the legislation enacted in Illinois makes it lawful to send the flying machine over the crowd in search of a violent offender. In this case, the knife-wielding man might still be a threat or, at the very least, attempting to escape and get rid of the evidence.

2. Facial Recognition

Facial recognition is a biometric software program that measures points on a person's face by analyzing and comparing contours that are unique to each individual. The technique captures data and uses algorithms to identify and verify people quickly.[79] For the purpose of these hypothetical crimes, it is appropriate to determine what legal ramifications are on the horizon. Supporters of facial recognition software see the technology as an aid to police when searching for missing persons or catching dangerous criminals. However, civil rights groups fear that it infringes on a person's right to privacy

---

76 "Public Safety Drones: An Update," Center for the Study of the Drone, May 28, 2018, https://dronecenter.bard.edu/public-safety-drones-update/.

77 Freedom from Drone Surveillance Act, 725 Ill. Comp. Stat. 167 (2014), http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3520&ChapterID=54.

78 "Police Drones and Privacy," *Chicago Tribune*, May 9, 2018, http://www.chicagotribune.com/news/opinion/editorials/ct-edit-drones-police-illinois-20180504-story.html.

79 "What Is Facial Recognition?," Techopedia, accessed October 7, 2018, https://www.techopedia.com/definition/32071/facial-recognition.

and will be misused by law enforcement—specifically to deport undocumented immigrants.[80]

In addition, the technology works well, but it is not perfect. The police in South Wales began using facial recognition software in June 2017, and their trial touts over 2,000 positive identifications that led to the arrests of over 450 people. However, of the nearly 2,470 faces identified during a football game, 92 percent were found to be false positives.[81] Technology companies, such as Microsoft, which are on the cutting edge of perfecting the software, have called on Congress to regulate the use of facial recognition technology.[82] Facial recognition has surfaced in airports, sports stadiums, and police stations. However, there are no set rules to govern how the technology is used. Should those who are exercising their First Amendment rights be subject to surveillance?

As reviewed in *Illinois v. Lidster*, the police had set up a checkpoint to stop motorists and inquire about a hit-and-run accident that had recently occurred.[83] Approaching the checkpoint, Robert Lidster nearly struck one of the officers. The officers directed Lidster to a side street and administered sobriety tests after smelling alcohol on him. Lidster challenged his arrest, arguing that the checkpoint violated his Fourth Amendment rights. The case made it to the Supreme Court after the lower courts could not agree. Judge Posner opined,

> Lidster is important because it divorces searching from suspicion. It allows surveillance that invades liberty and privacy to be conducted because of the importance of the information sought, even if it is not sought for use in a

---

80 Victoria Cavaliere, "Microsoft Wants Regulation of Facial Recognition Technology to Limit 'Abuse,'" CNN, July 14, 2018, https://money.cnn.com/2018/07/14/technology/microsoft-facial-recognition-letter-government/index.html.

81 Press Association, "Welsh Police Wrongly Identify Thousands as Potential Criminals," *Guardian*, May 5, 2018, https://www.theguardian.com/uk-news/2018/may/05/welsh-police-wrongly-identify-thousands-as-potential-criminals.

82 Russell Brandom, "How Should We Regulate Facial Recognition?," Verge, August 29, 2018, https://www.theverge.com/2018/8/29/17792976/facial-recognition-regulation-rules.

83 Illinois v. Lidster, 540 S. Ct. 419 (2004).

> potential criminal proceeding against the people actually under surveillance.[84]

In short, it is more important to catch a person who is a threat to the safety of others than to protect the privacy of those under surveillance. The same concept can be applied to camera surveillance in a place where there is no expectation of privacy.

The United States has come a long way since the cases of *Olmstead* and *Kyllo*, from which the emergence of technology paved a long and winding path for the Fourth Amendment's parameters. The parameters are being tested, and it is too soon to tell whether they will withstand the pressure.

C. A PERPETRATOR PAYS FOR PARKING

A woman enters downtown Aurora to attend a popular farmers' market that she discovered on her social media news feed. Parking is scarce, so she opens an application on her phone that guides her to a parking space only a block away from her destination. She uses the app to pay for and secure the parking place, effortlessly parks her vehicle, and walks to the market.

Upon entering her license plate in the parking app, the police department dispatch receives an alert that the registered owner is wanted on several warrants for forgery and retail theft from another jurisdiction. The call is dispatched to officers who respond and find the car parked and unoccupied. The officers determine that the driver has paid for the space for one hour and decide to come back as the expiration nears. Once they do, they see the woman who matches the description of the registered owner walking toward the vehicle. The officers stop the woman before she reaches her car, and they ask for identification, which reveals she is the wanted person. She is taken into custody without incident thanks to the parking technology.

Most companies that provide parking sensors are contracted by the city in which they operate, so privacy policies are necessary. In the hypothetical, the license plate

---

[84] Richard A. Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency* (New York: Oxford University Press, 2006), http://ebookcentral.proquest.com/lib/ebook-nps/detail.action?docID=272395.

information went directly to police dispatch, but currently, that information is collected by a third party. Nevertheless, it seems easy for law enforcement to obtain that information. The third-party doctrine has been the applied standard for requesting data, but the recent decision in *Carpenter v. United States* altered the criteria by determining that law enforcement can obtain third-party information only with a warrant.[85] For many civil libertarians, this is a victory against government intrusion.

The ACLU believes that license plate readers and sensors are tracking citizens. According to the ACLU's website, smart technology "has the potential to create permanent records of virtually everywhere any of us has driven, radically transforming the consequences of leaving home to pursue private life and opening up many opportunities for abuse."[86] Sensors for parking and license plate readers gather information on vehicles, which leads to owner information. Gone are the days in which a quarter in the meter bought a few hours and anonymity. Patrons exchange credit card information for convenience, and cameras automatically track license plates and charge a fee based on how long the car is parked. Most people think little about these choices—unless they are trying to avoid detection.

D. CONCLUSION: WHO OWNS THE DATA?

Most smart cities involve partnerships between the public and private sectors. Cities contract with private companies that provide the platform and process to collect and store data. Governments have traditionally owned data that are applicable to their operations, but as cities have become smarter, they turn to contractors to manage such precious information.[87] Teresa Scassa, the research chair of information law and policy at the University of Ottawa, talks about this change:

---

85 Carpenter v. United States, 137 S. Ct. 2211 (2017).

86 Jefferson Graham, "Coin-Operated Parking Becomes Ancient History as Apps, Sensors Take Over Cities," *USA Today*, October 11, 2017, https://www.usatoday.com/story/tech/talkingtech/2017/10/11/coin-operated-parking-becomes-ancient-history-apps-sensors-take-over-cities/678347001/.

87 Teresa Scassa, "Who Owns All the Data Collected by 'Smart Cities'?," *Toronto Star*, November 23, 2017, https://www.thestar.com/opinion/contributors/2017/11/23/who-owns-all-the-data-collected-by-smart-cities.html.

> A shift from public to private sector ownership of the data collected and generated in smart cities will place restrictions on governments' abilities to use and reuse urban data, and to share it with others. Put another way, governments become data tenants rather than data landlords.[88]

Thus, it will be difficult for law enforcement to obtain the data collected when a crime is committed. Quite simply, if the city does not own the data and the third-party doctrine no longer provides the police access to data upon request, it will be far more cumbersome for law enforcement to such information—even in the course of an investigation.

[88] Scassa.

V. RECOMMENDATIONS AND CONCLUSION

> Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.
>
> —Dissenting opinion in *Olmstead v. United States*, 277 U.S. 438 (1928)

This research began with an attempt to explore the concept of a smart city and how the data associated with it might be used by law enforcement to investigate crimes occurring under the watchful eye of technology. The Fourth Amendment has been the guiding beacon for government intrusion and goals of this thesis were to determine whether that framework holds in the digital age and to explore the delicate balance between security and privacy.

A. SECURITY V. PRIVACY

In his book *Data and Goliath*, author Bruce Schneier takes a firm stand on the preservation of privacy:

> Privacy is not a luxury that we can only afford in times of safety. Instead, it's a value to be preserved. It's essential for liberty, autonomy, and human dignity. We must understand that privacy is not something to be traded away in some fearful attempt to guarantee security, but something to maintain and protect in order to have real security. None of this will happen without a change of attitude. In the end, we'll get the privacy we as a society demand and not a bit more. [89]

The discourse regarding privacy is that a citizen has to relinquish a portion of it in exchange for security. When Edward Snowden gave away government secrets, he was a hero to some and a traitor to others. Regardless of viewpoint, his statement is the crux of the privacy-versus-security argument: "Arguing that you don't care about the right to

89 Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, 1st ed. (New York: Norton, 2016).

privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."[90] The other side of the argument can be summed up in James Madison's words on the dangers of war: "No nation could preserve its freedom in the midst of continual warfare."[91]

Freedom of privacy departed with the emergence of the information age. Before the advancement of technology, it was far easier to be anonymous; however, the digital age of cameras, smartphones, geofences, kiosks, and drones are challenging the prospect of living anonymously while under surveillance. The digital age has a long memory, and data and metadata are being stored in the cloud and recalled when circumstances necessitate. The research of this thesis has concluded there is no such thing as privacy in plain sight. Furthermore, strong evidence suggests that the Fourth Amendment remains the gatekeeper of unreasonable searches even in the digital age. The case law researched for this thesis is crucial because it follows the development of the citizen's privacy right vis-à-vis the government's need to collect data to solve crimes, beginning with a physical search through the emergence of technology and surveillance. No matter what scenario is presented, *Katz v. United States* retains the threshold for reasonableness.

In *Data and Goliath*, Schneier considers the cost savings and increased capabilities of technologies in police surveillance:

> Following someone covertly, either on foot or by car, costs around $175,000 per month—primarily for the salary of the agents doing the following. But if the police can place a tracker in the suspect's car, or use a fake cell tower device to fool the suspect's cell phone into giving up its location information, the cost drops to about $70,000 per month, because it only requires one agent. And if the police can hide a GPS receiver in the suspect's car, suddenly the price drops to about $150 per month—mostly for the surreptitious installation of the device. Getting location information from the suspect's cell provider is even cheaper: Sprint charges law enforcement only $30 per month. The difference is between fixed and marginal costs. If a police department performs surveillance on foot, following two people

---

90 Sophie Kleeman, "In One Quote, Snowden Just Destroyed the Biggest Myth About about Privacy," News, Mic.com, accessed October 9, 2018May 29, 2015, https://mic.com/articles/119602/in-one-quote-edward-snowden-summed-up-why-our-privacy-is-worth-fighting-for#.2e130nE7W.

91 Scott Horton, "Madison on the Dangers of War," *Stream* (blog), July 7, 2007, https://harpers.org/blog/2007/07/madison-on-the-dangers-of-war/.

> costs twice as much as following one person. But with GPS or cell phone surveillance, the cost is primarily for setting up the system. Once it is in place, the additional marginal cost of following one, ten, or a thousand more people is minimal.[92]

Schneier makes the business case for law enforcement to employ surveillance techniques through technological monitoring; however, his point identifies the slippery slope of convenience and cost savings of the government monitoring its citizens.

B. THE FUTURE OF THE THIRD-PARTY DOCTRINE

From a law enforcement perspective, the future of information accessibility is more uncertain given the recent case decision involving the third-party doctrine. In *Carpenter v. United States*, the permissions that allowed the government to obtain data from third-party vendors began to close when Justice Sotomayor wrote to reduce the scope of the doctrine:

> It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.[93]

These "mundane" tasks are ones that were explored in this thesis. The concert attendee who opts into an interactive experience at a venue provides data to a city or a government, and that data can be retrieved to determine the person's identity. The method in which the city gathers the data depends on who owns the information collected. If the city owns the data, they may be turned over to law enforcement because it is an official arm of the city. However, if a third-party vendor owns the data, the third-party doctrine no longer permits the government access to obtain the information without a warrant.

Time will tell whether the Supreme Court justices will lock the gate when it comes to government surveillance in the possession of third parties. Justice Alito has become an outspoken voice on privacy issues and technology. He writes,

---

92 Schneier, *Data and Goliath*, 25.

93 United States v. Jones, No. 10-1259, slip op. at 34 (S. Ct. January 23, 2012).

> New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.[94]

C. RECOMMENDATIONS

Rather than awaiting the Supreme Court to rule on the third-party doctrine or to carve out exceptions, this thesis recommends that legislation be introduced to determine who owns data and to regulate the balance between privacy and public safety. The courts can only rule on cases that come before them while members of Congress have the capacity to weigh arguments and reactions from their constituents as well as determine the best way forward to address policies. Being proactive is better than allowing the courts to decide the fate of the third-party doctrine and protection for metadata and stored communications.

In addition, the agencies that implement smart city technologies should set policies that outline how the data will be used and how long it will be retained. Cities and vendors should be transparent about the information collected, so citizens are protected from their content being shared with other companies or the government. In *Transforming City Governments for Successful Smart Cities*, Nina David, Johnathan Justice, and John G. McNutt advocate for strong governance and transparency in a world where many citizens distrust their government. They posit, "Smart cities should be transparent cities. Information technology should facilitate the open government movement in any municipality, especially in a smart community."[95]

Law enforcement should investigate each incident while adhering to the U.S. Constitution and its amendments. The Fourth Amendment provides the necessary guidelines for searches and seizures, and the scope of surveillance lives within those

---

94 Dahlia Lithwick, "Alito vs. Scalia," Slate, January 23, 2012, http://www.slate.com/articles/news_and_politics/jurisprudence/2012/01/u_s_v_jones_supreme_court_justices_alito_and_scalia_brawl_over_technology_and_privacy_.html.

95 Manuel Pedro Rodríguez Bolívar, ed., *Transforming City Governments for Successful Smart Cities* (Cham, Switzerland: Springer, 2015), 69, http://public.eblib.com/choice/publicfullrecord.aspx?p=3567486.

parameters. Rather than easily accessing data, law enforcement may be required to show reasonable suspicion and obtain a warrant.

D. CONCLUSION

As more people connect to the internet of things, the more convenient it is to navigate the world. The emergence of technology has taken innovation and connectivity to another level, and cities have begun to structure platforms to support smart city technologies. Transportation, infrastructure, parking, and lighting are all part of a smart city. Cameras, drones, facial recognition, kiosks, and geofencing are built into the platform as well; however, the latter technologies raise the privacy concerns of government surveillance. There will likely be a tipping point in the form of backlash when all innovations that comprise a smart city begin to identify people and compromise privacy.

Since the early 1900s, there has been case law specifically governing the use of technology particularly in criminal investigations. The evolution of technology has caused the courts to apply the Fourth Amendment standard of "physical searches" to "virtual searches," and thus far, it has remained the applicable litmus test for all searches and seizures by the government. The third-party doctrine allows law-enforcement to obtain data from vendors that house metadata from cell phones and other forms of technology; however, the Supreme Court is reviewing the doctrine as a threat to privacy. Future court cases involving seizures of information by law enforcement without a warrant will determine whether the doctrine remains intact. With this uncertainty, it would be appropriate for Congress to develop guidelines that strike a balance between privacy and security.

The notion of privacy in plain sight is an oxymoron—there is no such thing as privacy when technology is watching. Law enforcement must continue to adhere to the parameters as dictated by the Fourth Amendment when seeking data on suspects, witnesses, and victims of crime. Law enforcement must embrace the revelation that data require controls, and those are developed by changing policy and driving new legislation to provide transparency to citizens about how their digital footprint is being used. Embracing this revelation will deter a revolution.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Avalos, George. "Location-Based 'Geo-Fencing' Apps Raise Privacy Concerns." Science X Network. January 5, 2012. https://phys.org/news/2012-01-location-based-geo-fencing-apps-privacy.html.

Boland, Michael. "Mobile & Local Join the Big Data Movement." Search Engine Watch. August 17, 2012. https://searchenginewatch.com/sew/opinion/2199396/mobile-local-join-the-big-data-movement.

Bonack, Bryan. "Geofences: What They Are, What They Aren't, and Why They're Effective." *Geospatial World* (blog), July 9, 2018. https://www.geospatialworld.net/blogs/geofences-what-they-are-what-they-arent-and-why-theyre-effective/.

Brandom, Russell. "How Should We Regulate Facial Recognition?" Verge. August 29, 2018. https://www.theverge.com/2018/8/29/17792976/facial-recognition-regulation-rules.

Braun, Virginia, and Victoria Clarke. "Using Thematic Analysis in Psychology." *Qualitative Research in Psychology* 3, no. 2 (January 2006): 77–101. https://doi.org/10.1191/1478088706qp063oa.

Bud, Thomas K. "The Rise and Risks of Police Body-Worn Cameras in Canada." *Surveillance and Society* 14, no. 1 (2016): 118–119.

Cavaliere, Victoria. "Microsoft Wants Regulation of Facial Recognition Technology to Limit 'Abuse.'" CNN. July 14, 2018. https://money.cnn.com/2018/07/14/technology/microsoft-facial-recognition-letter-government/index.html.

Center for the Study of the Drone. "Public Safety Drones: An Update." May 28, 2018. https://dronecenter.bard.edu/public-safety-drones-update/.

Chicago Tribune. "Police Drones and Privacy." May 9, 2018. http://www.chicagotribune.com/news/opinion/editorials/ct-edit-drones-police-illinois-20180504-story.html.

Cohen, Boyd. "The 3 Generations of Smart Cities." Fast Company. August 10, 2015. https://www.fastcompany.com/3047795/the-3-generations-of-smart-cities.

Constructech TV. "Episode 32: Aurora Lights Up Smart Cities." YouTube video, 57:35. August 6, 2018. https://www.youtube.com/embed/7K9PZKrikKg.

De Vogue, Ariane. "Supreme Court Takes on Major Fourth Amendment Case." CNN. November 29, 2017. https://www.cnn.com/2017/11/29/politics/supreme-court-fourth-amendment-case/index.html.

Doctoroff, Daniel L. “Reimagining Cities from the Internet Up.” *Sidewalk Talk* (blog), November 30, 2016. https://medium.com/sidewalk-talk/reimagining-cities-from-the-internet-up-5923d6be63ba#.ubj2h5kdb.

Farhi, Paul. “‘Paperless Ticketing’ Aims to Thwart Scalping at Concerts, Sports Events.” *Washington Post*, July 5, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/07/04/AR2010070404180.html.

Fitzpatrick, Jason. “What Is ‘Geofencing’?” How-to Geek, September 21, 2016. https://www.howtogeek.com/221077/htg-explains-what-geofencing-is-and-why-you-should-be-using-it/.

Graham, Jefferson. “Coin-Operated Parking Becomes Ancient History as Apps, Sensors Take Over Cities.” *USA Today*. October 11, 2017. https://www.usatoday.com/story/tech/talkingtech/2017/10/11/coin-operated-parking-becomes-ancient-history-apps-sensors-take-over-cities/678347001/.

Griffin. “What Does It Mean to Be Secure in One’s Person, Papers and Effects?” *RedState* (blog), September 23, 2013. https://www.redstate.com/diary/griffinelection/2013/09/23/what-does-it-mean-to-be-secure-in-ones-person-papers-and-effects/.

Hamblen, Matt. “Just What Is a Smart City?” *Computerworld*, October 1, 2015. https://www.computerworld.com/article/2986403/internet-of-things/just-what-is-a-smart-city.html.

Harper, Jim. “Administering the Fourth Amendment in the Digital Age.” National Constitution Center. Accessed July 13, 2018. https://constitutioncenter.org/digital-privacy/The-Fourth-Amendment-in-the-Digital-Age.

Horton, Scott. “Madison on the Dangers of War.” *Stream* (blog), July 7, 2007. https://harpers.org/blog/2007/07/madison-on-the-dangers-of-war/.

Hu, Margaret. “Cybersurveillance Intrusions and an Evolving Katz Privacy Test.” *American Criminal Law Review*, 55, no. 127 (2018).

Irvin, Richard C. “Prioritization of Information Technology Initiatives.” Lecture, Alarm Detection Services, Aurora, IL, July 11, 2018.

Julie, Richard S. “High-Tech Surveillance Tools and the Fourth Amendment: Reasonable Expectations of Privacy in the Technological Age.” *American Criminal Law Review* 37, no. 127 (January 2000).

Kerr, Orin S. “The Case for the Third-Party Doctrine.” *Michigan Law Review* 107, no. 561 (February 2009): 562–563.

Kleeman, Sophie. “In One Quote, Snowden Just Destroyed the Biggest Myth about Privacy.” Mic. May 29, 2015. https://mic.com/articles/119602/in-one-quote-edward-snowden-summed-up-why-our-privacy-is-worth-fighting-for#.2e130nE7W.

Levinson-Waldman, Rachel. “Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public.” *Emory Law Journal* 66 (March 2017): 527–28.

Lithwick, Dahlia. “Alito vs. Scalia.” Slate. January 23, 2012. http://www.slate.com/articles/news_and_politics/jurisprudence/2012/01/u_s_v_jones_supreme_court_justices_alito_and_scalia_brawl_over_technology_and_privacy_.html.

Lord, Steve. “Aurora Looks to Expand Fiber Optic Network Downtown.” *Aurora Beacon-News*, February 26, 2018. http://www.chicagotribune.com/suburbs/aurora-beacon-news/news/ct-abn-aurora-fiber-st-0227-20180226-story.html.

———. “Work Begins on $35 Million Downtown Aurora Arts Center.” *Aurora Beacon-News*, October 11, 2017. http://www.chicagotribune.com/suburbs/aurora-beacon-news/news/ct-abn-aurora-artscenter-st-1012-20171011-story.html.

Maciag, Mike. “Survey: Almost All Police Departments Plan to Use Body Cameras.” *Governing*, January 26, 2016. http://www.governing.com/topics/public-justice-safety/gov-police-body-camera-survey.html.

Martinez-Balleste, Antoni, Pablo Perez-Martinez, and Agusti Solanas. “The Pursuit of Citizens’ Privacy: A Privacy-Aware Smart City Is Possible.” *IEEE Communications Magazine* 51, no. 6 (June 2013). https://doi.org/10.1109/MCOM.2013.6525606.

Miller, Stephen A., and Rachel Collins Clarke. “Supreme Court Tackles Fourth Amendment Case Involving Cellphone Privacy.” Legal Intelligencer. February 7, 2018. https://www.law.com/thelegalintelligencer/sites/thelegalintelligencer/2018/02/07/supreme-court-tackles-fourth-amendment-case-involving-cellphone-privacy/.

Musa, Sam. “Smart City Roadmap.” Academia. January 2016. https://www.academia.edu/.

Nam, Taewoo, and Theresa Pardo. “Smart City as Urban Innovation: Focusing on Management, Policy, and Context.” Policy paper, Center for Technology in Government, University of Albany, New York, 2011. https://doi.org/10.1145/2072069.2072100.

Nguyen, Hoaithi Y. T. “Lawful Hacking: Toward a Middle-Ground Solution to the Going Dark Problem.” Master’s thesis, Naval Postgraduate School, 2017.

Niu, Ben, Qinghua Li, Xiaoyan Zhu, Guohong Cao, and Hui Li. "Enhancing Privacy Through Caching in Location-Based Services." *IEEE Conference on Computer Communications* (2015): 1017–1025, https://doi.org/10.1109/INFOCOM.2015.7218474.

OnLight Aurora. "Transforming City of Lights to City of Light Speed." Accessed November 20, 2018. http://www.onlightaurora.com/.

Paramount Theatre. "Mission & History." Accessed November 20, 2018. https://paramountaurora.com/about/.

Pegues, Michael. "COA River Edge Smart Park." Presentation, Smart Park, Aurora, IL, 2017.

Peterson, Andrea. "The NSA Says It 'Obviously' Can Track Locations without a Warrant. That's Not so Obvious." *Washington Post*, December 4, 2013. https://www.washingtonpost.com/news/the-switch/wp/2013/12/04/the-nsa-says-it-obviously-can-track-locations-without-a-warrant-thats-not-so-obvious/.

Poslad, Stefan, Athen Ma, Zhenchen Wang, and Haibo Mei. "Using a Smart City IoT to Incentivise and Target Shifts in Mobility Behaviour—Is It a Piece of Pie?" *Sensors* 15, no. 6 (June 4, 2015): 13069–96. https://doi.org/10.3390/s150613069.

Posner, Richard A. *Not a Suicide Pact: The Constitution in a Time of National Emergency*. New York: Oxford University Press, 2006. http://ebookcentral.proquest.com/lib/ebook-nps/detail.action?docID=272395.

Press Association. "Welsh Police Wrongly Identify Thousands as Potential Criminals." *Guardian*, May 5, 2018. https://www.theguardian.com/uk-news/2018/may/05/welsh-police-wrongly-identify-thousands-as-potential-criminals.

Reddy, Trips. "10 Ways Stadiums & Venues Are Using Technology to Delight Fans & Keep Them Coming Back." Umbel. September 29, 2015. https://www.umbel.com/blog/publishers/10-ways-stadiums-are-using-technology-to-delight-fans/?cn-reloaded=1.

RiverEdge Park. "Be a Sponsor." Accessed November 20, 2018. https://riveredgeaurora.com/sponsor/.

Rodríguez Bolívar, Manuel Pedro. *Transforming City Governments for Successful Smart Cities*. Cham, Switzerland: Springer, 2015. http://public.eblib.com/choice/publicfullrecord.aspx?p=3567486.

Scassa, Teresa. "Who Owns All the Data Collected by 'Smart Cities'?" *Toronto Star*, November 23, 2017. https://www.thestar.com/opinion/contributors/2017/11/23/who-owns-all-the-data-collected-by-smart-cities.html.

Schneier, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. 1st ed. New York: Norton, 2016.

Survey Sampling International (blog). "The Top 4 Things You Should Know about Geo-Fencing." May 27, 2013. https://www.surveysampling.com/blog/top-4-things-know-geofencing/.

Talon, Mike. "Cloud 101: Geofencing." *Stratoscale* (blog), September 21, 2016. https://www.stratoscale.com/blog/cloud/cloud-101-geo-fencing/.

Techopedia."What Is Facial Recognition?" Accessed October 7, 2018. https://www.techopedia.com/definition/32071/facial-recognition.

Thibodeau, Patrick. "Kiosks Are Looking at You, Too." InformationWeek. October 25, 2017. https://www.informationweek.com/big-data/ai-machine-learning/kiosks-are-looking-at-you-too-/d/d-id/1330207.

Totenberg, Nina. "Justices May Impose New Limits on Government Access to Cellphone Data." NPR. November 29, 2017. https://www.npr.org/2017/11/29/567348000/justices-may-impose-new-limits-on-government-access-to-cellphone-data.

Villasenor, John. "What You Need to Know about the Third-Party Doctrine." *Atlantic*, December 30, 2013. https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/.

Wilson, Marie. "RiverEdge Park Completes Longtime Aurora Vision." *Daily Herald*, June 10, 2013. http://www.dailyherald.com/article/20130610/news/706109913/.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California