EARS IN THE SKY: HOW THE TECHNOLOGY OF SHOTSPOTTER IS ERODING FOURTH AMENDMENT PROTECTIONS

GAGE RIGHTER*

I. INTRODUCTION

Imagine living in a high crime area and walking down the street with a friend. Out of nowhere, an officer flashes their lights and stops you both at gunpoint. When you ask why the officer stopped you, they respond, "because I received an alert that there was a gunshot detected in this area." You, however, are not engaged in illegal activity or acting nervous. You were simply stopped for being close to a gunshot and living in a high-crime area. Is that fair?

Whether you believe it is fair, several courts have held that officers investigating a high-crime area based on a gunshot detection system—called ShotSpotter—have reasonable suspicion to make investigatory stops.[1]

Now, you are arrested and at trial the prosecuting attorney plays a ShotSpotter audio recording of a conversation with you and your friend that occurred seconds after the gun was fired. The officer testifies that you shot the gun. You wonder, "how did they get this recording and when were they listening?" The answer is that ShotSpotter technology is constantly monitoring your conversations through the use of audio sensors installed on telephone poles, buildings, and street lights.[2] While ShotSpotter claims that, "human voices and street noise will never trigger a sensor" because they are not "loud enough," multiple instances have proved ShotSpotter technology can listen to and record conversations.[3] To verify the

---

[1] *See* United States v. Rickmon, 952 F.3d 876, 878 (7th Cir. 2020); State v. Hill, 288 Neb. 767, 851 N.W.2d 670 (2014); United States v. Funderburk, 2018 D.C. Super. LEXIS 14.

[2] *Acoustic Gunshot Detection*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/pages/gunshot-detection [https://perma.cc/5CNP-4YDT].

[3] *See* People v. Johnson, No. A131317, 2013 Cal. App. Unpub. LEXIS 1450 *3 (Feb. 27, 2013); T.D.P. v. City of Oakland, No. 3:16-cv-04132-LB, 2019 U.S. Dist. LEXIS 29624 *6 (N.D. Cal. Feb. 24, 2019); Erica Goode, *Shots Fired, Pinpointed and Argued Over*, N.Y. TIMES (May 28, 2012), https://www.nytimes.com/2012/05/29/us/shots-heard-pinpointed-and-argued-over.html?pagewanted=all [https://perma.cc/MVG4-7G89].

ShotSpotter's listening capabilities, I contacted my local law enforcement agency, where I was informed that it can, and does, pick up conversations.[4]

This Comment argues that ShotSpotter technology is used by police departments nationwide in a manner that violates the Fourth Amendment as it constantly monitors conversations and unjustly provides reasonable suspicion to officers, based primarily on geographic alerts. Part II contains a brief synopsis of how ShotSpotter functions and how departments rely on the technology. Part III discusses the various ways ShotSpotter can be integrated into other technology to further enhance the monitoring capabilities of law enforcement agencies. Part IV provides an in-depth review and analysis of foundational Fourth Amendment cases such as *Katz v. United States, Kyllo v. United States, United States v. Jones,* and *Carpenter v. United States* compared to ShotSpotter's surveillance technology, to show that an unreasonable search under the Fourth Amendment occurs when the government deploys ShotSpotter, without a warrant, to record conversations.

Part V contrasts that ShotSpotter is not an unreasonable search, and it examines the two antagonistic approaches taken by lower courts. That section provides a brief analysis of reasonable suspicion precedent to further the argument that the second approach—taken by the D.C District Court—should be adopted by all courts to prevent Fourth Amendment protections from eroding. Lastly, Part VI recommends implementing judicial or legislative oversight to provide restraint on emerging technologies that pose significant risks to constitutional protections.

II. SHOTSPOTTER TECHNOLOGY

A. What is ShotSpotter?

ShotSpotter is a gunshot detection software that "filters out ambient background noise such as traffic and wind, and listens for impulsive sounds characteristic of gunfire."[5] Once the sensor detects this sound, it analyzes the sound wave's sharpness, strength, duration, and delay time.[6]

---

[4] Interview with local law enforcement director of ShotSpotter. Similarly, Oakland Police Captain Ersie M Joyner III said to the Oakland Safety Committee "Of course there are audio sensors that are constantly recording." BUSINESS INSIDER, (Mar. 26, 2015). https://www.businessinsider.com/the-nypds-newest-technology-may-be-recording-conversations-2015-3 [https://perma.cc/9TME-5KZ4].

[5] *ShotSpotter Technology*, SHOTSPOTTER, https://www.shotspotter.com/technology/ [https://perma.cc/4KEH-92RJ].

[6] *Id.*

The system uses three sensors to detect sound waves that are considered to be derived from a gunshot.[7] Once the system receives the sound waves, the sensor sends "a small data packet to cloud servers where multilateration[8] is used based on time difference of arrival and angle of arrival of the sound to determine a precise location."[9] A database of gunshot sounds and frequencies is then used to determine if the sound was in fact a gunshot .[10] If the system determines the sound was generated by a gunshot through the database algorithm, the information goes to an acoustic expert in ShotSpotter's 24/7 Incident Review Center to confirm the initial diagnosis.[11] Based on the information, the acoustic experts can "append the alert with other critical intelligence such as whether a fully automatic weapon was fired or whether there are multiple shooters."[12] The ShotSpotter system's increased accuracy and speed indicate why many law enforcement agencies are integrating this technology. ShotSpotter offers police departments many other benefits, including estimates of crime scene locations, increased incident reports, increased dispatch times, and faster victim transportation times.[13] But this technology still has downfalls. For one, the system cannot describe any identifiable characteristics of the shooter, or shooters, that a 911 caller could.[14]

B. The Shift from 911 Callers to Automated ShotSpotter Alerts

According to ShotSpotter's data, "on average only twenty percent of gunfire incidents are reported" by individuals.[15] In the twenty-percent of reported gunfire incidents, the information takes several minutes to reach

---

[7] *Id.*

[8] G. Scott Shaw, *Multilateration (MLAT)* MULTILATERATION AND ADS-B, http://www.multilateration.com/surveillance/multilateration.html. (Multilateration is a proven technology that has been in use for many decades. It was developed for military purposes to accurately locate aircraft—many of which did not wish to be 'seen'—by using a method known as Time Difference of Arrival (TDOA).") [https://perma.cc/4J45-DCTC].

[9] *ShotSpotter Technology*, *supra* note 5.

[10] *Id.*

[11] *ShotSpotter Flex Q*&A, SHOTSPOTTER, https://www.shotspotter.com/wp-content/uploads/2020/10/ShotSpo tter-Flex--Oct-2 020.pdf [https://perma.cc/PT6N-E59X].

[12] *Id.*

[13] *Gunshot Detection,* SHOTSPOTTER, https://www.shotspotter.com/law-enforcement/gunshot-detection/ [https://perma.cc/42NE-F2A4].

[14] *Id.*

[15] *Id.*

nearby officers, which results in less accurate information and slower response times. In contrast, ShotSpotter "detects and locates gunfire to enable a fast and precise response to over 90% of gunfire incidents."[16] ShotSpotter advertises that it takes 60 seconds to notify the police department after a gun is shot.[17] ShotSpotter proposes that its system will help "identify shooters faster" and "disrupt the shooting cycle" through faster response times.[18] Based on such representation, police departments employing ShotSpotter take law enforcement actions assuming that the system is extremely accurate. Part V demonstrates how this shift from 911 callers to automated ShotSpotter alerts has led to courts incorrectly holding that officers have reasonable suspicion when primarily relying on ShotSpotter technology. Further, this substitution of automated systems for eye-witness accounts presents a haunting similarity to the shift in technological policing seen in China. Continued advancement and use of ShotSpotter technology in the United States creates the potential for technological policing taken even further, presenting new challenges for the courts.

III. THE FUTURE OF MASS MONITORING: INTEGRATING SHOTSPOTTER INTO OTHER SURVEILLANCE TECHNOLOGY

In Shenzhen, China, the government is using facial recognition technology to project images, with detailed personal information, of those who violate the law.[19] This technology was incorporated to humiliate citizens who are damaging society through their acts.[20] Nonetheless, the most shocking part about this technology is that the United States is merely one step away from running real time facial recognition software similar to China.[21] While law enforcement can currently run facial recognition after a

---

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] Dave Davies, *Facial Recognition and Beyond: Journalist Ventures Inside China's 'Surveillance State'*, NPR (Jan. 5, 2021), https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta [https://perma.cc/TH97-UTS40].

[20] *Id.*

[21] *See* Sam DuPont, *On Facial Recognition, the U.S. Isn't China-Yet*, LAWFARE (June 18, 2020), https://www.lawfareblog.com/facial-recognition-us-isnt-china-yet [https://perma.cc/LC9G-VZ7G].

crime has been committed, real time facial recognition is unavailable.[22] Despite lacking technological advancements for real time facial recognition, law enforcement agencies still possess many tools to recreate the same effects of real time facial recognition software.[23] One such tool is integrating ShotSpotter with other surveillance technology, such as license plate readers, records management systems (RMS), computer aid dispatch systems (CAD), video management systems (VMS), unmanned aerial vehicles (UAV), and predictive policing software.[24]

For example, in Columbus, Ohio, the Columbus Police Department has implemented the use of ShotSpotter along with license plate readers to identify potential suspects.[25] Once ShotSpotter identifies a gunshot, the system will automatically link to the license plate reader cameras and begin recording license plates to every vehicle in the area.[26] The recordings will then generate a list of vehicles and times that officers can combine with other evidence to narrow down the suspects.[27] Former Columbus Police Chief, Thomas Quinlan, noted that the department would use the data to track an individual car at multiple crime scenes over time.[28] The system essentially allowed law enforcement to take digital footprints of all the locations the vehicle traveled throughout the City and store them for future use.[29]

Similarly, in Chicago, Illinois, law enforcement agencies are using ShotSpotter in congruence with the city's 30,000 government-operated,

---

[22] *Id.*

[23] *Id.*

[24] *Partnerships*, SHOTSPOTTER, https://www.shotspotter.com/partners/#:~:text=ShotSpotter%20has%20worked%20with%20approximately,geospatial%20software%2C%20and%20even%20drones, (last visited Feb. 22, 2022), [https://perma.cc/K76R-MHHQ].

[25] Bill Bush, *Columbus Police Cameras to Analyze License Plates, but Not Facial Recognition Just Yet*, THE COLUMBUS DISPATCH (Dec. 8, 2020), https://www.dispatch.com/story/news/2020/12/08/columbus-police-cameras-record-license-plate-numbers-linden-hilltop/6479954002/ [https://perma.cc/A74B-ENRM].

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *See id.*

closed-circuit cameras.[30] In one instance, law enforcement tapped into an area alerted by ShotSpotter to track a gunman.[31] "Switching from one high-definition camera to the next," officers followed the fleeing gunman.[32] It is important to note that these are not regular cameras. They are high-definition cameras, "which are equipped with night vision technology," and are "so pristine that the officer was able to watch the man wipe sweat off his face."[33] While high definition cameras are currently integrated into ShotSpotter to provide visuals of the potential suspect, ShotSpotter is also being used to monitor and record conversations.[34] The integration of closed circuit cameras with ShotSpotter not only gives law enforcement constant "eyes," but also "ears" on the public[35] This creates a mass surveillance system capable of recording locations and conversations over an extended period.

IV. THE USE OF SHOTSPOTTER TO LISTEN IN ON CONVERSATIONS: A VIOLATION OF THE FOURTH AMENDMENT UNDER THE KATZ TEST

Reported cases are beginning to show that ShotSpotter is used to capture sounds that go far beyond gunshots.[36] As *People v. Johnson* recounts, on June 8, 2007, ShotSpotter detected and recorded not only two gunshots, but it also captured the last words of the homicide victim, Tyrone Lyles.[37] On the recording Mr. Lyles was heard saying, "Ar, Ar, why are you going to do me like that, Ar."[38] The voice recording was used as

---

[30] Timothy Williams, *Can 30,000 Cameras Help Solve Chicago's Crime Problem?* N.Y. TIMES (May 26, 2018), https://www.nytimes.com/2018/05/26/us/chicago-police-surveillance.html [https://perma.cc/3CNP-5ZRK].

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] Natalie Shoemaker, *Yet Another Technology is Secretly Listening in on You*, BIG THINK (Mar. 24, 2015), https://bigthink.com/ideafeed/is-an-urban-gun-detection-system-listening-for-more-than-just-gunshots [https://perma.cc/Z2ZM-S6M5].

[35] *See* Cara Buckley, *High-Tech 'Ears' Listen for Shots*, N.Y. TIMES (Nov. 20, 2009), https://www.nytimes.com/2009/11/22/nyregion/22shot.html [https://perma.cc/J7A7-AN4G].

[36] Goode, *supra* note 3; *See* People v. Johnson, No. A131317, 2013 Cal. App. Unpub. LEXIS 1450 (Feb. 27, 2013); *See generally* Commonwealth v. Raglin, 178 A.3d 868, 873 (Jan. 23, 2018).

[37] *Johnson*, 2013 Cal. App. Unpub. LEXIS 1450, at *4.

[38] *Id.* at *4.

evidence to convict the defendant of first-degree murder.[39] ShotSpotter states its primary purpose is to filter out outside noise and narrow the sound down to gunfire.[40] CEO of ShotSpotter, Ralph A. Clark, admitted that in exceptional circumstances the system will collect "noises that happen at exactly the time of the blast" give or take a couple seconds.[41] Nonetheless, critics of ShotSpotter are doubtful that the device is not actively listening for sounds—including private conversations—all the time.[42]

Weighing in on the privacy concern, Jay Stanley, a senior analyst at the American Civil Liberties Union's Speech, Privacy, and Technology Project, stated, "we are always concerned about secondary uses of technology that is sold to us for some unobjectionable purpose and is then used for other purposes."[43] ShotSpotter spokeswoman, Lydia Barrett, has sought to address some of these concerns.[44] "I can't remember in the history of our technology the sensors ever hearing a fight or some kind of argument going on."[45] Despite attempts to persuade the public that ShotSpotter is not actively listening, serious privacy rights are at stake.

A. The Katz Test: The Introduction of Zones of Privacy

Although the Constitution does not expressly include the right to privacy, the Supreme Court has noted that "zones of privacy" are created by "specific guarantees in the Bill of Rights."[46] One "zone of privacy" acknowledged by the Court is in the Fourth Amendment, which protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[47] While the Supreme

---

[39] *Id.* at *12.

[40] *See* Cale Guthrie Weissman, *The NYPD's Newest Technology May Be Recording Conversations,* BUSINESS INSIDER (Mar. 26, 2015). https://www.businessinsider.com/the-nypds-newest-technology-may-be-recording-conversations-2015-3 [https://perma.cc/6N7L-YHUD].

[41] *Id.*

[42] *Id.*

[43] Daniel Rivero, *Is NYC's New Gunshot Detection System Recording Private Conversations?* SPLINTER (Mar. 20, 2015, 3:34 PM), https://splinternews.com/is-nyc-s-new-gunshot-detection-system-recording-private-1793846543 [https://perma.cc/85CV-QDQ6].

[44] *Id.*

[45] *Id.*

[46] Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

[47] U.S. CONST. amend. IV.

Court has not confronted ShotSpotter to determine whether listening and recording conversations is a search that requires a warrant, it has confronted the issue of other similar surveillance technology.[48]

In *Katz*, federal agents placed a wiretap on the outside of a public phone booth to listen to the defendant's conversation.[49] Relying on the Supreme Court's previous ruling in *Olmstead v. United States*,[50] the government argued the wiretap was not a search because the device was installed without physically intruding onto the defendant's property or person.[51] However, the Court overruled the previous "trespass" line of reasoning and held that the Fourth Amendment "protects people, not places."[52] Therefore, physical intrusion is no longer an element of a search.

In addition, the Court held that what an individual "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[53] The proposition that private conversations are constitutionally protected in public areas plays a vital role in the argument that ShotSpotter's active listening qualities violates the Fourth Amendment. Justice Harlan, writing in the concurrence in *Katz*, formulated a two-part test to determine whether a search occurred.[54] The first part of the test requires "that a person has exhibited an actual (subjective) expectation of privacy."[55] After the person shows an actual expectation of privacy, the second part requires the court to evaluate whether "the expectation be one that society is prepared to recognize as 'reasonable.'"[56] In determining whether a law enforcement tactic is a search, subject to the warrant requirement, the Supreme Court mostly utilizes the *Katz* test. Thus, to determine whether the use of ShotSpotter should be considered a search, it

---

[48] *See* Olmstead v. United States, 277 U.S. 438 (1928); Katz v. United States, 389 U.S. 347 (1967); Kyllo v. United States, 533 U.S. 27, (2001); United States v. Jones, 565 U.S. 400 (2012); Carpenter v. United States, 138 S. Ct. 2206 (2018).

[49] *Katz*, 389 U.S. at 348.

[50] *Olmstead*, 277 U.S. at 466. ("The Fourth Amendment is not violated unless there has been an official search and seizure of a defendant's person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure.")

[51] *Katz*, 389 U.S at 352.

[52] *Id.* at 353.

[53] *Id.* at 351.

[54] *Id.* at 361.

[55] *Id.*

[56] *Id.*

must first be determined whether a subjective expectation of privacy for private conversations in public exists. Second, the expectation must be one society is willing to recognize as reasonable.

B. Technology Not in General Public Use

While *Katz* provided a general framework for courts to use, some critics pointed out the framework was "circular" and subject to "unpredictable" results.[57] The Supreme Court ultimately agreed that the framework was inefficient for emerging technology, and the Court enhanced the rule in *Kyllo v. United States*.[58] In *Kyllo,* officers used thermal-imaging technology to scan the exterior of the defendant's home to detect growth of marijuana.[59] As a result of the thermal-imaging scan, officers obtained a search warrant for the defendant's home.[60]

The issue for the Supreme Court was whether the imaging on the wall's exterior was a search.[61] The government and the dissent both argued that the thermal-imaging only detected heat radiating from the house's external surface and was therefore no different from a neighbor or member of the public who notices "rainwater evaporates or snow melts at different rates on the surface across its surfaces."[62] Nonetheless, the majority expressly rejected this line of reasoning and held that "where the government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[63] Similarly, ShotSpotter, without a warrant, uses technology unavailable for public use to monitor conversations that would previously have been undiscoverable by one not physically present. Thus, the Supreme Court's holding in *Kyllo* is instructive in determining whether ShotSpotter is a search that is subject to the warrant requirement.

---

[57] Kyllo v. United States, 533 U.S. 27, 34 (2001) (citing W. LaFave, Search and Seizure § 2.1(d), pp. 393–394 (3d ed. 1996); Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 S. CT. REV. 173, 188) [https://perma.cc/VQ35-NNQY].

[58] *Kyllo*, at 34.

[59] *Id.* at 30.

[60] *Id.*

[61] *Id.* at 31.

[62] *Id.* at 43.

[63] *Id.* at 40.

C. Long-term GPS Monitoring Impinges on the Right to Privacy

Although *Kyllo* may be binding in cases that involve surveillance technology invading the home, the Supreme Court left open the question of what occurs when surveillance technology monitors individuals in public places. Several years after *Kyllo*, the Supreme Court confronted this issue in *United States v. Jones*.[64] In *Jones*, federal agents attached a GPS monitor to Jones' vehicle and monitored its movements for twenty-eight days.[65] Using multiple satellites, the GPS tracked Jones' vehicle within fifty to 100 feet.[66] Using GPS locations that were accumulated over the twenty-eight days, the government connected Jones' location to a drug house and charged him with drug trafficking.[67]

Before trial, Jones filed a motion to suppress the data GPS data because it violated his right to privacy.[68] The District Court granted his motion in part, yet ultimately denied his motion regarding the data obtained while he was driving on public roads because "a person traveling an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[69] As a result, the jury found Jones guilty and sentenced him to life in prison.[70]

The D.C. Circuit Court of Appeals reversed the conviction on the grounds that admission of the GPS data violated the Fourth Amendment.[71] On appeal, the Supreme Court reverted back to the *Olmstead* physical intrusion test and held that the government's installation and use of the GPS data constituted a search under the Fourth Amendment.[72] Justice Alito, in his concurrence, believed that the case should have been decided on the prolonged tracking of Jones, instead of on the trespass.[73] Specifically, Justice Alito would have held the "use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[74]

---

[64] United States v. Jones, 565 U.S. 400 (2012).

[65] *Id.* at 403.

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] *Id.* (quoting United States v. Knotts, 460 U.S. 276, 281 (1983)).

[70] *Id.* at 404.

[71] *Id.*

[72] *Id.* at 404-5.

[73] *Id.* at 419.

[74] *Id.* at 430.

Justice Sotomayor, in her concurrence, echoed a similar opinion noting that "physical intrusion is now unnecessary to many forms of surveillance. With increasing regularity, the government will be capable of duplicating the monitoring undertaken in this case by enlisting factory-or-owner installed vehicle tracking devices or GPS-enabled smartphones."[75] The extended monitoring, even for short periods of time, could reveal a "wealth of detail" about a person's "familial, political, professional, religious, and sexual associations" that are all relevant in a *Katz* analysis.[76] Per Justice Sotomayor, being under constant government surveillance, "chills associational and expressive freedoms" that individuals use to express themselves in public.[77] Similarly, ShotSpotter's constant monitoring poses the same significant risk that the audio sensors may gather intimate details about an individual who seeks to exclude information from a third-party listening. However, since *Jones* was decided on the technicality of a physical intrusion, the concerns of Justices Alito and Sotomayor would not materialize until *Carpenter v. United States.*[78]

D. Reasonable Expectation of Privacy from Extended Surveillance: Accounting for More Sophisticated Systems

In *Carpenter*, four men were arrested for robbing a series of Radio Shacks and T-Mobile stores in Michigan and Ohio.[79] After one of the men disclosed a list of fifteen accomplices, the prosecutor applied for numerous court orders, under the Stored Communications Act, for cell phone records to determine if anyone on the list was connected to the crimes. [80] The records provided the locations for "calls origination and at call termination for incoming and outgoing calls during the four-month period when the string of robberies occurred."[81] Overall, the government received "12,989 location points," which was an average of "101 data points per day."[82] Based on this information, officers arrested and charged Thomas Carpenter

---

[75] *Id.* at 414-15.

[76] *Id.* at 415.

[77] *Id.* at 416.

[78] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[79] *Id.* at 2212.

[80] *Id.*

[81] *Id.*

[82] *Id.*

with six counts of robbery and six counts of having a firearm during a "federal crime of violence."[83]

At trial, Carpenter moved to suppress the evidence, claiming that the government violated his right to privacy when it obtained the record without a warrant.[84] The trial court and Sixth Circuit Court of Appeals both determined that Carpenter "lacked a reasonable expectation of privacy in the location information collected by the FBI because he shared that information with his wireless carrier."[85] On appeal, the Supreme Court reversed and remanded the case because the government's use of the cell phone locations without a warrant constituted an unreasonable search that violated Carpenter's reasonable expectation to privacy.[86]

In holding the use of the cell phone locations was a search, the Court reiterated its previous holding in *Katz,* that "a person does not surrender all Fourth Amendment protections by venturing into the public sphere."[87] Although Carpenter had an expectation in his physical movements, the government argued that under the third-party doctrine, his expectation of privacy was reduced because he knowingly shared his location.[88] Still, the Court rejected this argument because it would significantly extend the third-party doctrine.[89] Chief Justice Roberts, writing for the majority, pointed out that telephone companies that track data are not "'typical witnesses,' who keep an eye on comings and goings."[90] Instead, the companies are recording information continuously and the storage capabilities makes their memory nearly "infallible."[91] Similarly, ShotSpotter possesses the same capability of storing audio recordings for future use in trials.[92]

Moreover, in *Carpenter* the government argued that data collection "should be permitted because the data is less precise than GPS

---

[83] *Id.*

[84] *Id.*

[85] *Id.* at 2213.

[86] *Id.* at 2219.

[87] *Id.* at 2217 (citing Katz v. United States, 389 U.S. 347, 351-52 (1967)).

[88] *Id.* at 2219.

[89] *Id.*

[90] *Id.*

[91] *Id.*

[92] *See* People v. Johnson, No. A131317, 2013 Cal. App. Unpub. LEXIS 1450, at *4 (Feb. 27, 2013).

information."[93] The government argued the cell phone location data only provided an area in which Carpenter could have been placed, instead of his exact location.[94] Nonetheless, the Court noted that its adopted rule must "take account for more sophisticated systems that are already in use or in development."[95] Applying this futuristic principle, the Court recognized that some "wireless carriers have the capability to pinpoint a phone's location within 50 meters."[96] Despite this argument, the Court did not look at systems' current capabilities, but instead looked at the technology's potential.[97] Employing the Supreme Court's future capability method of analyzing technology, ShotSpotter poses a significant danger with enhancements and modifications to target conversations.

In reviewing the previous foundational cases to determine whether police use of surveillance technology triggers the protections of the Fourth Amendment under *Katz*, the Supreme Court has considered the technology's potential, its availability to the public, and the duration of the surveillance. Next, it is essential to determine if these factors, when applied to ordinary law enforcement uses of ShotSpotter, constitute a search that is subject to the warrant requirement.

E. ShotSpotter's Constant Surveillance Violates the Katz Test

Under the two-part *Katz* test, this note argues that ShotSpotter's capability to actively listen to private conversations is a search, which is subject to the warrant requirement. First, under the subjective inquiry, most courts tend to either defer to the individual or gloss over the requirement.[98] An individual subject to the active listening technology would be able to show a subjective expectation in their conversations by articulating the point that they intended their conversation to be shielded from governmental intrusion. Furthermore, an individual could produce

---

[93] *Carpenter*, 138 S. Ct. at 2218.

[94] *Id.*

[95] *Id.* (citing Kyllo v. United States, 533 U.S. 27, 36 (2001)).

[96] *Id.* at 2219.

[97] *Id.*

[98] Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 122 (2015).

evidence that reasonable precautions were made to prevent others from listening.[99]

Nonetheless, the second prong of the test involves a significant portion of the analysis because lower courts must be willing to recognize the subjective expectation as one that society views as objectively reasonable. Despite the hurdle, the lower courts must find that society is willing to recognize the reasonable expectation to be free from continuous surveillance. Not long ago, Edward Snowden leaked vital information that exposed the National Security Agency's surveillance of phone calls and electric communications.[100] In a public survey five years later, "57% of Americans said it was unacceptable for the government to monitor the communications of United States Citizens."[101] This survey data reinforces that society is willing to recognize the right to be free from constant surveillance as objectively reasonable.

It is important to recognize, though, that ShotSpotter is not listening to private telephone calls through wiretaps. Instead, it is listening to private conversations in public through audio sensors. The distinction between private and public locations matters because many prosecutors using ShotSpotter recordings advocate that there is no expectation of privacy in public because individuals voluntarily take the risk that others will overhear them.[102] While this argument bears some weight, the Court in *Katz* expressly held that just because an individual leaves the protection of his home and enters a public space does not eviscerate Fourth Amendment protections.[103]

---

[99] *See* Katz v. United States, 389 U.S. 347, 361 (1967) ("One who occupies a telephone booth shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that his conversation is not being intercepted").

[100] *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily,* THE GUARDIAN (June 6, 2013, 6:05 AM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/APZ2-TWHE].

[101] A.W. Geiger, *How Americans Have Viewed Surveillance and Privacy Since Snowden Leaks*, PEW RESEARCH CENTER (June 4, 2018), https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/ [https://perma.cc/BBN2-NZWD].

[102] Brian Fraga, *ShotSpotter Recording of Street Argument Raises Potential Privacy Issues* (Jan. 11, 2012), https://www.southcoasttoday.com/article/20120111/News/201110339 [https://perma.cc/4AUF-UY9P].

[103] *Katz*, 389 U.S. at 351.

The distinguishing fact highlighted by the Court in *Katz* was whether the individual sought to exclude the "uninvited ear."[104] To assume that an individual who speaks in a low voice and takes reasonable precautions to prevent others from hearing has no privacy in public would be a misinterpretation of *Katz* and would ultimately create no zones of privacy outside the home. In addition, individuals subject to ShotSpotter's listening capabilities cannot determine the sensors' locations.[105] That is, law enforcement agencies that contract with ShotSpotter keep the sensors hidden from communities.[106] As such, an individual cannot seek to exclude the "uninvited ear" without knowing where that ear is located, or even that the ear exists.

Additionally, ShotSpotter is not merely an individual who may happen to overhear a snippet of conversation passing by. Instead, ShotSpotter is a system comprised of twenty sensors per square mile that are actively listening at a frequency well above the capability of human ears.[107] To put this into perspective, a square mile is 640 acres. That means that each sensor has to cover roughly thirty-two acres to triangulate a location. No reasonable person could infer that a sensor capable of listening at that frequency is analogous to a person overhearing a conversation in public. A more analogous situation would be a person at every corner of every street listening at all hours, which an individual would see and know about.

The Supreme Court in *Kyllo* cautioned against human enhancing technology, not in the general public's use, being deployed to invade privacy.[108] It is important to note that ShotSpotter is a private company that prevents the public from accessing its technology and data.[109] Similar to *Kyllo*, police officers are using technology inaccessible to the public to obtain information that would not be obtainable absent the technological enhancement encroaching on individuals' right to privacy. If law

---

[104] *Id.* at 352.

[105] Rachel Holliday & Smith Gabriel Sandoval, *'ShotSpotter' Tested as Shootings and Fireworks Soar, While Civil Rights Questions Linger*, THE CITY, (July 5, 2020), https://www.thecity.nyc/2020/7/5/21312671/shotspotter-nyc-shootings-fireworks-nypd-civil-rights [https://perma.cc/Z8L2-7VDE].

[106] *Id.*

[107] *ShotSpotter Frequently Asked Questions*, SHOTSPOTTER, https://www.shotspotter.com/system/content-uploads/SST_FAQ_January_2018.pdf [https://perma.cc/EW8Q-DN5K].

[108] Kyllo v. United States, 533 U.S. 27, 40 (2001).

[109] Rivero, *supra* note 43.

enforcement agencies were to mimic the surveillance power of ShotSpotter with police officers, they would only cover a minor portion of the geographical area, even with all of their resources. Therefore, applying the traditional, two-part test formulated in *Katz,* ShotSpotter's active listening constitutes an unreasonable search under the Fourth Amendment.

If ShotSpotter is not considered a search using the traditional *Katz* test, under the Court's recent decisions in *Jones* and *Carpenter*, ShotSpotter could now constitute a search.[110] Similar to *Jones* and the use of GPS tracking*,* ShotSpotter is being used to monitor individuals for an extended period. Paired with license plate readers and closed-circuit cameras, ShotSpotter provides a digital footprint for law enforcement officers to compile and review. The time-stamped, geographical location is analogous to the extended GPS tracking in *Jones.*

ShotSpotter technology integrated with license plate readers and closed-circuit cameras actually gives law enforcement a broader net to cast than in *Jones*. After a gunshot, the license plate readers can obtain a long list of names and locations to store for later use. All it takes is for law enforcement agencies to compile these lists over time and create a map of all the locations where each car has been to recreate the tracking in *Jones*. Given the massive volume of monthly ShotSpotter alerts,[111] law enforcement agencies will have an endless supply of data to compile and compare. This type of mass surveillance was ruled an unconstitutional search in *Jones* and should be an unconstitutional search now.

The constant monitoring of conversations also poses a risk of its own because it could reveal the kind of intimate details that Justice Sotomayor was concerned about in *Jones.* The audio surveillance deployed by ShotSpotter could pick up intimate conversations between loved ones or friends. The sensors could pick up conversations that were intended to be private, such as "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense

---

[110] *See generally* United States v. Jones, 565 U.S. 400 (2012); Carpenter v. United States, 138 S. Ct. 2206 (2018).

[111] Haley Nelson, *Police See Increase in ShotSpotter Alerts Compared to Last Year, Loved Ones Left Grieving,* WSYX (Aug. 5, 2020), https://abc6onyourside.com/news/local/police-see-increase-in-shotspotter-alerts-compared-to-last-year-loved-ones-left-grieving [https://perma.cc/L2JU-M6JQ].

attorney."[112] Such recordings would infringe the deepest spheres of an individual's life, which society would not be willing to recognize as reasonable.

Responding to growing concerns of recording conversations, law enforcement agencies and ShotSpotter argue that the technology has procedural safeguards to protect individuals from live monitoring and recording conversations.[113] Despite its claims, ShotSpotter does not allow any independent research to be conducted out of concern that their proprietary rights would be infringed upon by competitors.[114] In addition to denying independent research, ShotSpotter has also insulated itself from public records requests through an exemption in the Federal Freedom of Information Act and also numerous state public records acts.[115] Without an ability to conduct independent research or request ShotSpotter data, individuals are at the mercy of the courts and law enforcement to protect their privacy rights.

Despite the opacity, lower courts should still find that ShotSpotter's constant listening and recording conversations is an unreasonable search. As the majority in *Carpenter* correctly identified, the technology should be viewed in light of its potential instead of its proposed use.[116] Although the cell site location technology used in *Carpenter* was less accurate than GPS, the Court created a rule based on the future developments that would allow the technology's precision to parallel GPS technology's.[117] Applying the same rationale, ShotSpotter should be held an unreasonable search because

---

[112] *Jones*, 565 U.S. at 415 (citing People v. Weaver, 2009 NY Slip Op 3762, 12 N.Y.3d 433, 882 N.Y. S2d 357, 909 N.E.2d 1995).

[113] Privacy Policy, SHOTSPOTTER, https://www.shotspotter.com/privacy-policy/ [https://perma.cc/K9PW-V9WL] (last modified May 19, 2020).

[114] Jason Tashea, *Should The Public Have Access to Data Police Acquire Through Private Companies?*, ABA JOURNAL (Dec. 1, 2016, 3 :00AM), https://www.abajournal.com/magazine/article/public_access_police_data_private_company [https://perma.cc/M8MM-P3MA].

[115] *Customer Success Training Bulletin,* SHOTSPOTTER (July 7, 2015), Retrieved from https://www.forbes.com/sites/mattdrange/2016/11/17/shotspotter-struggles-to-prove-impact-as-silicon-valley-answer-to-gun-violence/#56fc0af831cb [https://perma.cc/5MSC-C4FW].

[116] Carpenter v. United States*,* 138 S. Ct. 2206, 2216 (2018) ("At any rate, the rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development.'") (citing Kyllo v. United States, 533 U. S. 27, 36 (2001)).

[117] *Carpenter*, 138 S. Ct. 2206, at 2216.

of its potential to actively listen and record conversations. Therefore, applying *Jones* and *Carpenter* further bolsters the argument that ShotSpotter is a violation of the *Katz* test and should be held a search subject to the warrant requirement.

V. USING SHOTSPOTTER TO DETERMINE REASONABLE SUSPICION

If the courts hold that ShotSpotter is not an unreasonable search, the technology's application should be limited by courts to prevent the erosion of Fourth Amendment protections. While gunshot detections were normally reported by witnesses who describe an individual or a specific car, ShotSpotter only provides the location and the number of shots.[118] Based on the statistics provided by ShotSpotter, only 20% of gunshots are reported by callers.[119] In contrast, ShotSpotter detects and provides alerts for 90% of gunshots.[120] Since the modern eyewitness is replaced by ShotSpotter technology, courts must decide whether the alert provides reasonable suspicion for officers to make investigatory stops.[121]

Currently, courts take two approaches when determining reasonable suspicion.[122] The first approach provides that officers relying primarily on ShotSpotter alerts have individualized suspicion to stop any person in proximity to the ShotSpotter alert regardless of descriptive information that would identify the suspect.[123] In contrast, the second approach provides that officers primarily relying on ShotSpotter alerts, with no descriptive information pertaining to the suspect, lack individualized suspicion to make investigatory stops.[124] This Comment advocates that courts should adopt the second approach because it preserves privacy protections of the communities monitored by ShotSpotter technology. Furthermore, courts should adopt the second approach because the first approach significantly departs from prior Fourth Amendment precedent and opens the door for

---

[118] *ShotSpotter Technology, supra* note 5.

[119] *Gunshot Detection, supra* note 13.

[120] *Id.*

[121] *See generally* State v. Nimmer, No. 2020AP878-CR, 2020 Wisc. App. LEXIS 590 (Ct. App. Dec. 15, 2020); United States v. King, 439 F. Supp. 3d 1051 (N.D. Ill. 2020); State v. Hill, 288 Neb. 767, 851 N.W.2d 670 (2014).

[122] United States v. Rickmon, 952 F.3d 876, 878-81 (7th Cir. 2020); United States v. Carter, No. 20-005, 2020 U.S. Dist. LEXIS 121181, *8 (D.D.C. July 10, 2020).

[123] *Rickmon*, 952 F.3d 876, at 878-881.

[124] *Carter*, No. 20-05, 2020 U.S. Dist. LEXIS 121181 at *24.

further government intrusion. The following subsections lay a foundation of prior Supreme Court decisions necessary for furthering my argument.

A. Requirement of Individualized Suspicion

In *Terry v. Ohio* the Supreme Court held that "a police officer may in appropriate circumstances and in an appropriate manner approach a person for purposes of investigating possible criminal behavior even though there is no probable cause to make an arrest."[125] The Court specified that an officer who "observes unusual conduct which leads him reasonably to conclude in light of his experience that criminal activity may be afoot" can briefly detain an individual to make reasonable inquiries.[126]

The important distinction made by the Court is that a police officer "who observes" conduct that arises to reasonable suspicion is justified in stopping an individual. Despite this holding, lower courts have allowed officers to briefly detain individuals based on no observations or descriptions other than the ShotSpotter alert location.[127] In holding that officers have reasonable suspicion, lower courts equated the ShotSpotter notification to an anonymous tipster that corroborated the 911 dispatcher's call.[128]

B. Acting on Anonymous Tips Alone is Not Enough

However, the Supreme Court in *Florida v. J.L.* stated that an anonymous tip alone without any further investigation by police officers did not amount to reasonable suspicion.[129] In *J.L.*, an anonymous caller reported that a young black male standing at a particular bus stop wearing a plaid shirt was carrying a gun.[130] When police officers arrived at the bus stop, they saw J.L who was wearing a plaid shirt.[131] The police then proceeded to stop J.L and frisk him for weapons solely based on the anonymous tip.[132] The Supreme Court reasoned that "officers' suspicion

---

[125] 392 U.S. 1, 22 (1968).

[126] *Id.* at 30.

[127] *Rickmon*, 952 F.3d at 878–79; United States v. Diaz, No. 20-cr-176, 2020 U.S. Dist. LEXIS 191250, at *13–14 (S.D.N.Y. Oct. 14, 2020); United States v. Funderburk, 2018 D.C. Super. LEXIS 14, at *13–14 (Dec. 31, 2018).

[128] *Rickmon*, 952 F.3d at 882.

[129] 529 U.S. 266, 268 (2000).

[130] *Id.*

[131] *Id.*

[132] *Id.*

that J.L. was carrying a weapon arose not from any observations of their own but solely from a call" and thus did not satisfy the reasonable suspicion standard.[133]

Florida and the United States in an amicus brief argued that the *Terry* standard should be modified to license a "firearm exception" that would allow police officers who receive an anonymous tip alleging an illegal gun to stop and frisk regardless of the reliability of the tip.[134] Nonetheless, the Supreme Court declined to accept this position, stating that an exception to the already low standard of reasonable suspicion would "rove too far" from Fourth Amendment precedent.[135] The Court noted "if police officers may properly conduct Terry frisks on the basis of bare-boned tips about guns, it would be reasonable to maintain…that the police should similarly have discretion to frisk based on bare-boned tips about narcotics."[136] Thus, the Court did not extend this firearm exception to the reasonable suspicion standard out of concern that the exception would swallow the rule.[137] Despite the Supreme Court's holding, the Seventh Circuit in *United States v. Rickmon* implicitly created this exception.[138]

C. First Approach: Taking "Individualized" Out of Reasonable Suspicion

In *Rickmon*, Shotspotter detected two gunshots in Peoria, Illinois,.[139] Directly after the ShotSpotter alert was issued, the police dispatcher reported several cars leaving and a black male on foot.[140]

Five minutes after the call, officers arrived at the scene and pulled over the only car on the street despite seeing a large crowd at the end of the street.[141] The officer asked the driver of the vehicle whether he could search the vehicle, consent was provided, and the officer found a nine-millimeter handgun under the passenger seat.[142] Rickmon, who was the passenger, was charged with having weapons under disability.[143] In

---

[133] *Id.* at 270.

[134] *Id.* at 272.

[135] *Id.*

[136] *Id.*

[137] *Id.* at 273.

[138] *See generally* United States v. Rickmon, 952 F.3d 876 (7th Cir. 2020).

[139] *Rickmon*, 952 F.3d at 879.

[140] *Id.*

[141] *Id.*

[142] *Id.*

[143] *Rickmon*, 952 F.3d at 879.

response to this charge, Rickmon filed a motion to suppress, stating that the officer did not have reasonable suspicion to stop the vehicle.[144]

The Central District Court of Illinois denied Rickmon's motion to suppress because the court found that the officers' actions were objectively reasonable based on the totality of the circumstances.[145] These circumstances included the following: the short lapse of time between the dispatch and the stop; the 911 call of vehicles leaving the area; this vehicle being the only one the officer saw in close proximity (less than 300 feet from where the shots were reported to have come from); and the vehicle driving away from the area where shots reportedly originated.[146]

On appeal, the Seventh Circuit Court of Appeals affirmed the district court decision.[147] In affirming the district court, the Seventh Circuit equated ShotSpotter to an anonymous tipster instead of an eyewitness or known informant.[148] The court noted that the 911 call corroborated the ShotSpotter alert for the officer to have reasonable suspicion.[149] While the Seventh Circuit correctly pointed out *United States v. Burgess* held that "corroboration from multiple sources describing the general area and nature of the same crime exceeds the single police tip that alone can supply reasonable suspicion," the same rationale does not apply to ShotSpotter technology.[150]

In *Burgess,* the tipsters identified the color of the car involved in the shooting and pinpointed exactly where the vehicle would be located.[151] In contrast, the gunshot detection system and dispatcher in *Rickmon* did not indicate who fired the shots or what direction they came from. Further, the dispatcher did not provide a vehicle description or precise location. The only description was that cars were leaving and there was a black man on foot.[152] Unlike *Burgess,* where the caller provided an identifiable car color*,* the information here was generalized and provided no basis for stopping Rickmon specifically.

---

[144] *Id.*

[145] *Id.* at 880.

[146] *Id,*

[147] *Id.* at 885.

[148] *Id.* at 882.

[149] *Id.*

[150] *Id.* (citing United States v. Burgess, 759 F.3d 708 (7th Cir. 2014)).

[151] *Burgess,* 759 F.3d at 711.

[152] *Rickmon*, 952 F.3d at 879.

Here, the more applicable case would be *J.L.* because the ShotSpotter alert provided no identifiable characteristics for the officer to investigate. Similar to the anonymous call that only stated the suspect was a black male in a flannel shirt on the street corner, the information corroborated here only provided an approximate location and a general description. In fact, *J.L.* actually provides more of a description because it identified a specific pattern of shirt the alleged suspect was wearing, versus just stating that vehicles were leaving and a black male was on foot. The Seventh Circuit tried maneuvering around the fact that no identifiable characteristic was mentioned by stating that it was "4:45 a.m. and there was no other traffic."[153] However, the Seventh Circuit assumed that individuals driving at 4:45 a.m. do not work early morning shifts or travel at that hour.[154]

The Seventh Circuit also considered that the officer had prior interactions with this block because he previously responded to shots-fired calls there.[155] The block was not deemed a "high crime area," but based on the officer's experience, the court concluded criminal activity occurred frequently enough there to warrant further investigation.[156] However, ShotSpotter is only positioned in high crime areas.[157] To use this "high crime area" factor in the reasonable suspicion analysis would be unjust because it would give officers reasonable suspicion once a gunshot is detected without observing any suspicious behavior. The Seventh Circuit's argument is circular because ShotSpotter will only lead to increased notifications that reinforce the idea that a particular neighborhood is a high crime area. Relying on this factor would criminalize Rickmon and others for living in their own community, and it would subject them to numerous investigatory stops.

Although the court stated that multiple circumstances were combined to create reasonable suspicion, the circumstances all revolved around the ShotSpotter notification to justify the stop. For example, one of the factors the court used in its analysis is that the officer "encountered Rickmon's vehicle on the same block five-and-a-half minutes after he received reports of shots fired."[158] Under this logic, the court would have us believe that police officers can stop any vehicle on the street or surrounding streets that

---

[153] *Id.* at 884.

[154] *Id.* at 886.

[155] *Id.* at 884.

[156] *Id.* (citing *Illinois v. Wardlow*, 528 U.S. 119, 120 S. Ct. 673 (2000)).

[157] *Home*, SHOTSPOTTER, https://www.shotspotter.com/ [https://perma.cc/U49J-J8P5].

[158] *Rickmon*, 952 F.3d, at 883.

is in close proximity to a ShotSpotter alert. This would dispense the individualized requirement set out in Terry *v. Ohio*.[159] While the Supreme Court has required individualized suspicion, few exceptions have manifested. One such exception was created by the Supreme Court in *Navarette v. California.*

It is noteworthy that the Supreme Court in *Navarette v. California* held that officers did not need individualized reasonable suspicion to make an investigatory stop under certain circumstances.[160] In *Navarette,* California Highway Patrol officers received an anonymous tip from a 911 caller that a "Silver Ford 150 pickup[161] Plate of 8-David-94925" ran the caller off the roadway and was last seen five minutes earlier going southbound on "Highway 1 at marker 88."[162] Based on the tip, the officers believed that the vehicle was engaged in criminal activity and stopped the vehicle.[163] In holding that the officers had reasonable suspicion, the Court stated, "by reporting that she had been run off the road by a specific vehicle—a silver Ford F150 pickup, license plate 8D94925—the caller necessarily claimed eyewitness knowledge of the alleged dangerous driving."[164] Thus, the anonymous tip alone was sufficient to stop the vehicle.

However, *Navarette* is distinguishable from *Rickmon* for several reasons because the anonymous tip provided a detailed description that could only identify one vehicle. The anonymous tip in *Navarette* provided a license plate number, model, and color of the truck engaged in the criminal activity. In contrast, the ShotSpotter alert and dispatcher in *Rickmon* provided a general description that could identify multiple individuals and vehicles in the area.

Additionally, the Supreme Court in *Navarette* emphasized that the caller's claim of eyewitness knowledge of the dangerous driving provided an "indicia of reliability" that supplied the officers with reasonable suspicion.[165] Unlike the anonymous tip in *Navarette,* ShotSpotter provides no first-hand knowledge that any specific individual is engaged in criminal activity or armed and presently dangerous. Thus, the rare exception to

---

[159] 392 U.S. 1, 22 (1968).

[160] Navarette v. California, 572 U.S. 393, 397 (2014).

[161] *Id.* at 395.

[162] *Id.*

[163] *Id.* at 401.

[164] *Id.* at 399.

[165] *Id.* at 404.

individualized suspicion recognized in *Navarette* is not present when officers rely on ShotSpotter alerts.

Despite the holdings in *J.L.* and *Navarette*, the Seventh Circuit in *Rickmon* has extended reasonable suspicion to any individual in the surrounding location based primarily on a ShotSpotter alert. Chief Judge Wood, writing for the dissent in *Rickmon*, raised two questions that will undoubtedly remain in the following years.[166] The first question to be answered by future courts is, "what are the temporal and spatial limits of reasonable suspicion based on ShotSpotter alerts?"[167] The officer in *Rickmon* arrived at the scene approximately five minutes after the ShotSpotter notification.[168] If the officers had arrived six or seven minutes after the notification, would this affect the reasonable suspicion analysis? In addition, does the time taken to respond extend the area that officers are able to reasonably stop individuals?[169]

In some cities such as Tampa, Florida, ShotSpotter can narrow down a gunshot within seventy-five feet.[170] Should seventy-five feet be the limit for officers to stop individuals based on reasonable suspicion? The majority in *Rickmon* failed to answer this question but instead stated that each case must weigh the "totality of the circumstances."[171] By not establishing temporal limits or spatial limits, lower courts have broad discretion to decide how far reasonable suspicion extends. The broad latitude will cause inconsistent decisions where minutes or seconds could ultimately determine reasonable suspicion.

The second question posed by the dissent was whether officers would be entitled to "force their way into every house" on the street to search for the shooter.[172] While this poses a serious question, the question should be modified to consider whether officers would be justified, without a warrant, in pursuing an individual seen running from the suspected location into a home or vehicle that parks in a residential garage on the

---

[166] United States v. Rickmon, 952 F.3d 876, 885 (7th Cir. 2020) (Wood, C.J. dissenting).

[167] *Id.* at 886.

[168] *Id.* at 883.

[169] *Id.* at 886.

[170] Ryan Smith, *Tampa Police to Use ShotSpotter Technology in High-Crime Area,* WFTS (Dec. 18, 2018), https://www.abcactionnews.com/news/region-hillsborough/tampa-police-to-use-shotspotter-technology-in-high-crime-area [https://perma.cc/2KLM-H682].

[171] *Rickmon*, 952 F.3d at 881.

[172] *Id.* at 886.

street. In both circumstances, the courts would have to determine whether officers could enter the residence based on the ShotSpotter alert. Thus, by holding that officers have reasonable suspicion when relying primarily on ShotSpotter, the Seventh Circuit has eroded the individualized requirement set out in *Terry* and created various challenges for future courts.

D. Second Approach: Preservation of Fourth Amendment Rights

Five months after *Rickmon* was decided, the D.C District Court in *United States v. Carter* confronted the same issue of deciding whether officers primarily relying on ShotSpotter alerts had reasonable suspicion to make an investigatory stop.[173] Unlike Seventh Circuit, the D.C District Court held that the ShotSpotter alert did not provide officers with reasonable suspicion.[174] In *Carter,* the D.C. police received a ShotSpotter notification that possible shots had been fired in a high crime area.[175] When the officers arrived in the general vicinity within minutes of the alert, they only saw three individuals walking down the street.[176] The officers pulled up next to the three individuals, activated their emergency lights, and began to question them, thus detaining them.[177]

While standing and talking to the officers, Carter kept his right arm pinned against his body.[178] The officers believed that the individuals were armed and dangerous and conducted a pat down of the individuals.[179] While the officers were conducting a pat down on the first individual, Carter took off running, but was eventually caught and searched for weapons.[180] The officers obtained a firearm from Carter and charged him with unlawful possession of a firearm.[181]

At trial, Carter moved to suppress the evidence claiming that the officers did not have reasonable suspicion to make the investigatory stop.[182] In response, the government argued that the officers had reasonable

---

[173] United States v. Carter, No. 20-05, 2020 U.S. Dist. LEXIS 121181, at *24 (D.D.C. July 10, 2020).

[174] *Id.* *24.

[175] *Id.* at *1-2.

[176] *Id.*

[177] *Id.*

[178] *Id.* *4.

[179] *Id.* at *5.

[180] *Id.* at *5-6.

[181] *Id.* at *6.

[182] *Id.* at *8.

suspicion to stop the three individuals based on the ShotSpotter notification, the proximity to the alert, and the fact that the neighborhood was in a high crime area.[183] However, the court disagreed with the government and found that none of the reasons justified the stop.[184] In holding that the stop was not justified, the D.C District Court relied on its prior circuit's case law in *United States v. Delaney*.[185]

In *Delaney,* the D.C. Circuit Court of Appeals held that investigating an area where potential gunshots were fired does not raise any individualized "suspicion that the particular individual being stopped was engaged in wrongdoing."[186] The D.C. Circuit noted, "an individual's presence in an area of expected criminal activity, standing alone, is not enough to support a reasonable, particularized suspicion that the person is committing a crime."[187] In response, the government argued that the officers had individualized suspicion because ShotSpotter "identified a relatively small area" and the three individuals were the only people there.[188]

Unlike the officers in *Delaney*, the government argued that ShotSpotter's precision provided individualized suspicion within the radius that ShotSpotter identified.[189] However, the court cautiously noted that "attaching individualized suspicion to every person out and about in a residential area…would incriminate 'a very large category of presumably innocent people and, accordingly, cannot justify a seizure.'"[190] Therefore, unlike *Rickmon,* the court held that the officers were not justified in stopping the three individuals based primarily on the ShotSpotter notification in the high crime area.[191]

The decisions rendered in *Carter* and *Rickmon* deliver inconsistent rulings when determining the weight ShotSpotter alerts should have in a reasonable suspicion analysis. *Rickmon* proposes that officers may rely primarily on the alerts for reasonable suspicion whereas *Carter* suggests

---

[183] *Id.* at *14-15.

[184] *Id.* at *16.

[185] *Id.* at *16-17.

[186] United States v. Delaney, 955 F.3d 1077, 1087 (D.C. Cir. 2020).

[187] *Id.* at 1086 (quoting Illinois v. Wardlow, 528 U.S. 119, 124 (2000)).

[188] *Carter*, 2020 U.S. Dist. LEXIS 121181 at *16, 18.

[189] *Id.* at *16.

[190] *Id.* at *17 (quoting *Delaney*, 955 F.3d at 1087).

[191] *Id.* at *14-15.

that the alerts are not enough. Since reasonable suspicion determinations are so fact intensive, the differing decisions may not result in a circuit split.

Nonetheless, this Comment argues that lower courts addressing the issue should adopt the *Carter* line of reasoning because it provides a clear rule for determining whether law enforcement acting primarily on ShotSpotter alerts have reasonable suspicion to make investigatory stops. By ruling that ShotSpotter alerts alone are not enough for reasonable suspicion, lower courts will not have to determine the spatial and temporal limits of reasonable suspicion. A matter of feet or seconds may not be a determining factor in the outcome of cases. Moreover, communities where ShotSpotter technology is implemented will not be subject to investigatory stops for simply living in an area closely connected to a ShotSpotter alert. Thus, the decision in *Carter* preserves the Supreme Court's prior Fourth Amendment precedent in *J.L.* and *Terry*.

Unlike *Rickmon, Carter* does not license a firearm exception, which was expressly rejected in *J.L.*, that removes individualized suspicion because a gunshot was reported in the area. By requiring an officer to observe criminal behavior in addition to the ShotSpotter alert, *Carter* follows the Supreme Court's holding in *Terry* that officers must possess individualized suspicion. Thus, when determining whether an officer relying primarily on ShotSpotter has reasonable suspicion to make a brief detention, lower courts should adopt the *Carter* line of reasoning and hold that an officer does not have reasonable suspicion. Without the constraints and protections *Carter* imposes on law enforcement officers, neighborhoods that are already subject to repetitive investigatory stops will fall victim to a cycle of arbitrary and discriminatory stops based on geographic alerts.

VI. CONCLUSION

As ShotSpotter technology continues to expand into more than 100 cities in the United States,[192] courts must determine how law enforcement agencies can use ShotSpotter technology. This Comment argues that when law enforcement agencies use ShotSpotter technology to monitor and record conversations without a warrant, it is an unreasonable search under the Fourth Amendment. Applying the Supreme Court's holdings in *Katz, Kyllo, Jones* and *Carpenter*, it is apparent that extending monitoring of

---

[192] *ShotSpotter Cities*, SHOTSPOTTER, https://www.shotspotter.com/cities/ [https://perma.cc/M7VU-6UFU].

private conversations through the use of technology not in the public's use without a warrant, is an unreasonable search.

If courts rule that ShotSpotter is not an unreasonable search, this Comment advances that courts should still take precautions by holding that ShotSpotter alerts do not provide officers with reasonable suspicion. Given the shift from 911 callers to automated alerts, courts should not substitute eyewitness testimony with computer generated alerts. Allowing such substitution will create a precedent that significantly departs from the Supreme Court's holding in *J.L.* that anonymous tips are not enough for reasonable suspicion. The substitution will remove the requirement of individualized suspicion set forth in *Terry* and allow officers to detain people based on their proximity to a ShotSpotter alert. In order to prevent the erosions of the Fourth Amendment protections, courts should hold that officers relying primarily on ShotSpotter alerts do not have reasonable suspicion.

Moving forward, legislators and courts should be proactive with emerging technology such as ShotSpotter that pose significant Fourth Amendment concerns. Cities should incorporate legislation that provides some independent oversight of ShotSpotter technology. For example, in New York, public advocates have introduced legislation that would require quarterly reports on ShotSpotter's data.[193] These quarterly reports would include when the gunshots were fired, where the gunshots were fired, how many shooters, plus any other data detected by ShotSpotter.[194] By requiring these specific data points, law enforcement agencies will be prevented from using ShotSpotter technology in a manner that violates the Fourth Amendment. Requiring data transparency will give courts an unobstructed view of how law enforcement agencies are using the technology pursuant to the Fourth Amendment. In turn, this will provide legislative and judicial oversight of law enforcement practices that will ultimately protect the rights of citizens—such as Johnson, Rickmon, and Carter—who are subject to significant Fourth Amendment violations by ShotSpotter technology.

---

[193] Azi Paybarah, *Public Advocate Bill Asks For Gunfire-Detection Reports,* POLITICO, (Feb. 12, 2015), https://www.politico.com/states/new-york/city-hall/story/2015/02/public-advocate-bill-asks-for-gunfire-detection-reports-019689 [https://perma.cc/UG3B-XXQZ].

[194] *Id.*