Taking Aim at ShotSpotter: Gunshot Surveillance, The Fourth Amendment, and an Argument for Sonic Security

Table of Contents

I. Introduction

Despite numerous attempts to address gun violence in the United States, it remains a persistent threat and intractable public health crisis. The statistics are staggering. In each of the last three years, the total number of deaths due to gun violence surpassed 40,000 with suicide accounting for roughly 55%

of deaths in 2020, 53% in 2021, and 54% in 2022.[1] During this time, however, defensive use of a firearm failed to top more than 2,000 incidents.[2] Before the end of the first month of 2023, the United States suffered more than 3,000 deaths resulting from gun violence,[3] more than forty mass shootings,[4] and a school shooting perpetrated by a six-year-old student.[5]

The constant stream of fresh stories about mass shootings, homicides, and accidental shootings "has become an ordinary facet of human life."[6] It paints a picture of a nation in crisis; a nation that has lost its way and is unable to protect its citizens from unabated gun violence.[7] Moreover, the pain and suffering caused by gun violence is not merely physical; it is also emotional and psychological.[8] It creates fear, mistrust, and a sense of hopelessness in communities inundated with routine gunfire.[9] Undoubtedly, no easy remedy exists because the gun violence issue is complex, multifaceted, and inextricably tethered to deeply entrenched social, political, and constitutional values.[10] Solutions exist, however, and more than 135 cities across the United

1. *See Past Summary Ledgers*, GUN VIOLENCE ARCHIVE, https://www.gunviolence archive.org/past-tolls (last visited Feb. 8, 2023). The Gun Violence Archive ("GVA") provides free online public access to gun violence data compiled from more than 7,500 sources. *Id.*; *see also* New York State Rifle & Pistol Ass'n v. Bruen, 597 U.S. 1, 83 (2022) (Breyer, J., dissenting) (citing the GVA as an authoritative source) ("Gun violence has now surpassed motor vehicle crashes as the leading cause of death among children . . . .").

2. *See Past Summary Ledgers*, *supra* note 1. Under the GVA's methodology, incidents involving defensive use of a firearm include homeowners thwarting a home invasion, store clerks preventing a robbery, and individuals who stop sexual assault. *Id.*

3. *Number of Deaths in 2023*, GUN VIOLENCE ARCHIVE, https://www.gunviolence archive.org/reports/number-of-gun-deaths?year=2023 (last visited Feb. 29, 2024).

4. *Mass Shootings in 2023*, GUN VIOLENCE ARCHIVE, https://www.gunviolencearchive. org/reports/mass-shooting?year=2023 (last visited Feb. 29, 2024).

5. Denise Lavoie, *Lawyer: Warnings Boy Had Gun Ignored Before He Shot Teacher*, AP NEWS (Jan. 25, 2023, 7:11 PM), https://apnews.com/article/newport-news-school-shooting-a40dfad64388aadf1f90211177412522.

6. Alexandra S. Gecas, Note, *Gunfire Game Changer or Big Brother's Hidden Ears?: Fourth Amendment and Admissibility Quandaries Relating to ShotSpotter Technology*, 2016 U. ILL. L. REV. 1073, 1076.

7. *Id.*

8. *See* Sarah R. Lowe & Sandro Galea, *The Mental Health Consequences of Mass Shootings*, 18 TRAUMA, VIOLENCE, & ABUSE 62, 62 (2017).

9. *See id.* at 63, 79.

10. *See* APA PANEL OF EXPERTS, AM. PSYCH. ASS'N, GUN VIOLENCE: PREDICTION, PREVENTION, AND POLICY, 1, 4 (2013), https://www.apa.org/pubs/reports/gun-violence-report.pdf.

States are blanketing neighborhoods with technology primed to listen for the smoking gun.[11]

ShotSpotter is an acoustic gunshot detection system ("AGDS") that uses a network of sensors to detect and locate gunfire in real-time.[12] This technology is touted as a way to increase public safety and improve crime scene response times by arming law enforcement with near real-time information about gunfire incidents.[13] That said, the use of ShotSpotter as a form of public monitoring raises questions about the extent of security citizens enjoy over the sounds they create—in this case, not merely the sounds of gunfire, but any innocuous noise loud enough to trigger an alert.[14] ShotSpotter presents an urgent and important constitutional question: whether the Supreme Court's governing interpretations of a bedrock constitutional right—the right to be secure from unreasonable searches—is fundamentally wrong. At a time when the nation is already facing a "stress test" characterized by "suspicions and investigations; a pattern of governmental lying" and "a rising fear of authoritarian and autocratic patterns,"[15] it is fair to wonder whether arming law enforcement with around-the-clock acoustic surveillance is a silver bullet or a loose cannon.

This Comment explores the economic and sociocultural realities of ShotSpotter's promise to inhibit gun violence and offers a framework under the Fourth Amendment with which to take aim at ShotSpotter before it becomes the new norm. Additionally, this Comment adds to existing scholarship on ShotSpotter in three ways. First, this Comment is the first to address the company's recent and unexpected corporate rebrand. Second, this Comment is the first to analyze ShotSpotter under the landmark Supreme Court case, *Carpenter v. United States*.[16] Third, this Comment lays the foundation to defend Sonic Security—the right to be secure in the sounds we produce—as a core civil right.

Part I provides an overview of ShotSpotter, including a foray into the company's corporate rebrand, how the technology operates, where it is

11. *See About SoundThinking*, SOUNDTHINKING, https://www.shotspotter.com/company/ (last visited Feb. 29, 2024).

12. Amanda Busljeta, Comment, *How an Acoustic Sensor Can Catch a Gunman*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 211, 213-14 (2016).

13. *See ShotSpotter: Save Lives and Find Critical Evidence with the Leading Gunshot Detection System*, SOUNDTHINKING, https://www.soundthinking.com/law-enforcement/leading-gunshot-detection-system/ (last visited Feb. 29, 2024).

14. *See* Busljeta, *supra* note 12, at 214.

15. Harry F. Tepker, *An Introductory Essay: Old Principles for an (Allegedly) Brave New World*, 71 OKLA. L. REV. 17, 17 (2018).

16. 585 U.S. 296 (2018).

deployed, and examples of its successes and failures. Part II maps the existing legal frameworks for analyzing ShotSpotter under the Fourth Amendment, including both the stop and frisk framework and the search and seizure framework. Part II concludes that both frameworks are inadequate for tackling modern surveillance technology that, like ShotSpotter, surreptitiously records in public spaces.

Given the lack of a viable challenge to ShotSpotter under current Fourth Amendment jurisprudence, Part III presents a new interpretation to reinvigorate the right of the people to be secure in their persons—including the right to be secure in the sounds they produce. Relying on positive law and sociocultural principles, Part III concludes that the failure to honor a right to Sonic Security is antithetical to foundational principles of the Fourth Amendment including autonomy, freedom, and democracy.

II. Introducing ShotSpotter: Your Not-So-Friendly Neighborhood Surveillance Tool

A 2016 study of Oakland, California and Washington, D.C. revealed that only 12.4% of gunshots were reported to the police.[17] In some parts of the United States, the "steady beat of gun violence is so persistent . . . people rarely call the police to report the shootings."[18] ShotSpotter promises to resolve the gap between shots fired and shots reported while simultaneously contributing to saving victims and finding evidence.[19] ShotSpotter's Senior Vice President of Marketing explained that "ShotSpotter alerts lead to fast, precise police responses . . . and lead to victims being located and saved as well as evidence being found to help identify the perpetrator."[20] For example, "in one year alone, first responders saved fifty-seven gunshot

17. Dennis Mares & Emily Blackburn, *Acoustic Gunshot Detection Systems: A Quasi-Experimental Evaluation in St. Louis, MO*, 17 J. EXPERIMENTAL CRIMINOLOGY 193, 194 (2021).

18. Matt Drange, *We're Spending Millions on This High-Tech Surveillance System Designed to Reduce Gun Violence. Is It Making a Difference?*, FORBES (Nov. 17, 2016, 8:30 AM), https://www.forbes.com/sites/mattdrange/2016/11/17/shotspotter-struggles-to-prove-impact-as-silicon-valley-answer-to-gun-violence/?sh=638fd0d131cb.

19. Mares & Blackburn, *supra* note 17, at 195.

20. Johana Bhuiyan, *Detroit Extends Contract with Controversial Gunshot Surveillance Firm*, GUARDIAN (Oct. 16, 2022, 4:28 PM), https://www.theguardian.com/usnews/2022/oct/11/detroit-contract-extend-shotspotter-surveillance-firm; Gecas, *supra* note 6, at 1083 ("ShotSpotter's unparalleled accuracy functions to pinpoint crime scenes that can better lead to criminal apprehension while saving victims' lives.").

victims" because personnel responded to the scene faster due to ShotSpotter's rapid gunshot detection.[21]

In best cases, officers arrive at the scene "before the shooter flees."[22] But even when the gunfire produces no victims and the shooter has absconded, officers are in a better position to recover evidence. For example, law enforcement in Worcester, Massachusetts, responding to ShotSpotter alerts collected "180 shell casings, recover[ed] three weapons, and gather[ed] an additional 60 pieces of evidence" in just one year.[23] Finally, "[w]itnesses have been found and criminal cases solved" because officers, who otherwise may have never received a 911 call, were able to investigate the gunshot alert.[24]

While ShotSpotter is on the cutting edge of technology to address the dearth in reported shootings, it is not new. In fact, ShotSpotter was founded decades ago in 1996 by Robert Showen.[25] ShotSpotter was originally based in California with prototypes first tested in Redwood City, California.[26] Today, the company enjoys an ever-increasing nationwide reach as it is in more than 150 cities,[27] fourteen university campuses,[28] and even the White House.[29] The company's booming customer list is counterbalanced by only a few ex-customers, including the cities of Dayton, San Antonio, and Canton.[30] Additionally, Chicago has a three-year, $33 million contract, but

---

21. Busljeta, *supra* note 12, at 219.

22. *Id.* at 212.

23. *Id.* at 218.

24. Gary Craig, *Is Shot Spotter Reliable Enough? Critics Question Human Equation Behind Technology*, DEMOCRAT & CHRONICLE (Rochester, N.Y.) (Nov. 20, 2017, 11:13 AM), https://www.democratandchronicle.com/story/news/2017/11/17/shot-spotter-technology-relshot-spotter-technology-coming-under-increased-scrutiny-judicial-communit/844335001/

25. See Katherine Kornei, *Physicist Pinpoints Urban Gunfire*, APSNEWS, June 2018, at 3, 3, https://www.aps.org/publications/apsnews/201806/upload/June-2018-rev3.pdf.

26. *Id.*

27. *See About SoundThinking*, *supra* note 11. "Big cities with even bigger gun problems," such as Chicago and New York City, are among the company's major clients. Todd Feathers, *Police Are Telling ShotSpotter to Alter Evidence from Gunshot-Detection AI*, VICE: MOTHERBOARD (July 26, 2021, 8:00 AM), https://www.vice.com/en/article/qj8xbq/police-are-telling-shotspotter-to-alter-evidence-from-gunshot-detecting-ai.

28. *See* ShotSpotter, Inc., Annual Report (Form 10-K) (Mar. 28, 2022).

29. Mares & Blackburn, *supra* note 17, at 194.

30. Dayton, Ohio began services in 2019 but cancelled four years later. Alejandro Figueroa, *Dayton Police Department Won't Be Renewing ShotSpotter Contract for 2023*, WYSO (Oct. 6, 2022, 1:15 PM), https://www.wyso.org/local-and-statewide-news/2022-10-06/dayton-police-department-wont-be-renewing-shotspotter-contract-for-2023. San Antonio

the city is embroiled in a lawsuit over the misuse of ShotSpotter to erroneously charge sixty-five-year-old Michael Williams with murder.[31] Williams spent nearly one year in jail until charges were finally dropped when the prosecution refused to defend the ShotSpotter data.[32]

Despite more than two decades of unparalleled growth, ShotSpotter issued a press release in April 2023 to announce a total corporate rebranding campaign.[33] One component of the rebranding strategy involves a name change to SoundThinking, which "reflects the company's focus on public safety" and its "community-focused solutions" that improve "violence prevention, social services and economic assistance."[34] This Part explores the company's rebranding campaign and its addition of new tools that expand the invasiveness of ShotSpotter. Second, this Part explains how the technology's hardware, software, and humanware[35] operate.

A. ShotSpotter's Corporate Rebrand

In April 2023, ShotSpotter announced its decision to adopt a new identity under the name SoundThinking.[36] The company's press release does not identify the impetus for the sudden identity crisis, but a data reporter for the Marshall Project speculates that the name change was a reactive measure "shortly after the company's stock lost about a third of its value following

---

ditched ShotSpotter in 2017. Vianna Davila, *S.A. Cuts Funding to $550K Gunshot Detection Program That Resulted in 4 Arrests*, MY SAN ANTONIO (Aug. 15, 2017, 8:29 AM), https://www.mysanantonio.com/news/local/article/City-pulls-plug-on-pricey-gunshot-detection-system-11817475.php. And Canton, Ohio replaced ShotSpotter with a competitor at the start of 2020. Kelly Byer, *Canton Expanding Police Camera Wi-Fiber Surveillance System in Northeast*, REPOSITORY (Apr. 19, 2021, 10:29 PM), https://www.cantonrep.com/story/news/2021/04/19/canton-expands-wi-fiber-police-surveillance-system-northeast/7257207002/.

31. Jim Daley, *CEO Says Johnson's 2024 Budget Includes ShotSpotter*, SOUTH SIDE WEEKLY (Nov. 9, 2023), https://southsideweekly.com/soundthinking-ceo-says-johnsons-2024-chicago-budget-includes-shotspotter/; Garance Burke & Michael Tarm, *Lawsuit: Chicago Police Misused ShotSpotter in Murder Case*, AP NEWS (July 21, 2022, 5:33 PM), https://apnews.com/article/gun-violence-technology-crime-chicago-lawsuits-3e6145f63c96593866cf89ac01ce7498.

32. Burke & Tarm, *supra* note 31.

33. Press Release, SoundThinking, ShotSpotter Changes Corporate Name to Soundthinking and Launches Safetysmart Platform for Safer Neighborhoods (Apr. 10, 2023), https://www.soundthinking.com/press-releases/shotspotter-changes-corporate-name-to-soundthinking-and-launches-safetysmart-platform-for-safer-neighborhoods/.

34. *Id.*

35. ShotSpotter relies on sensors, algorithms, and human reviewers to determine if a recorded noise is a gunshot. *See* discussion *infra* Sections II.B, II.C, and II.D. This Comment uses "humanware" to describe the human review phase.

36. Press Release, SoundThinking, *supra* note 33.

Chicago Mayor Brandon Johnson's election."[37] It is a plausible theory because Chicago is "one of SoundThinking's largest" customers, adding roughly "$8 million in revenue each year," and Chicago's Mayor vowed to terminate the contract.[38] At the very least, SoundThinking CEO Ralph Clark stated the name change mirrors the company's goal of achieving "optimal public safety outcomes."[39]

The rebrand is not a total overhaul, however, because the "flagship acoustic gunshot technology, ShotSpotter, will retain its name as a product."[40] Instead, the rebrand signals a restructuring of SoundThinking's core services into "an integrated suite" called the SafetySmart Platform.[41] The SafetySmart Platform is a centralized hub where customers can access four data-driven tools named CrimeTracer, CaseBuilder, ResourceRouter, and ShotSpotter.[42] While the focus of this Comment is the entanglement of ShotSpotter and the Fourth Amendment, it is not possible to appreciate the epic reach of ShotSpotter without also understanding the interplay between all four tools. When operated in tandem, the civil rights concerns already inherent in ShotSpotter are magnified.

The first tool, CrimeTracer (formerly known as COPLINK X), is a proprietary search engine that visually emulates the Google search bar and produces results in a format similar to Westlaw where users can toggle filters, sort, and generate geospatial visualizations. SoundThinking boasts CrimeTracer as "the largest network of police agency data in the United States" because it contains "more than 1 billion criminal justice records from across jurisdictions."[43] For example, CrimeTracer enables investigators to access a web of data including court documents, mugshots, tip lines, shell casing reports, vehicular data, Be On the Lookout ("BOLO") reports,

37. Geoff Hing, *How Tech Like ShotSpotter Thrives Despite Public Pushback*, MARSHALL PROJECT (May 27, 2023, 12:00 P.M.), https://www.themarshallproject.org/2023/05/27/chicago-gun-violence-shotspotter.

38. *Id.* It is doubtful that the souring Chicago contract and corresponding stock hit were the sole impetus for the name change. It is equally likely that the company desired distance from the growing body of academic criticism or desired a genuine marketing effort to illuminate the company's new products.

39. Press Release, SoundThinking, *supra* note 33.

40. *Id.*

41. *Id.*

42. *Id.*

43. *CrimeTracer*, SOUNDTHINKING, https://www.soundthinking.com/law-enforcement/crime-analysis-crimetracer/ (last visited Jan. 9, 2024); Ralph Clark, *ShotSpotter Is Now SoundThinking*, SOUNDTHINKING (Apr. 10, 2023), https://www.soundthinking.com/blog/shotspotter-is-now-soundthinking/.

probation or parole information, and warrants.[44] The exact composition of the data is a mystery, including what percentage of the data is comprised of ShotSpotter alerts. But both tools promise similar results: "identify offenders in near real-time" and "[e]nhance situational awareness even during routine traffic stops."[45] Since CrimeTracer automatically coalesces multiple strands of data into one encyclopedic web, the revealing nature of even a single ShotSpotter alert is likely magnified. Particularly because CrimeTracer leads into the second tool, CaseBuilder, "with one click."[46]

CaseBuilder is a cloud-based software package that promises to improve management of cases and investigations.[47] The key benefit for customers is the ability to "collaborate on investigations from a single, shared digital case folder."[48] For example, CaseBuilder allows investigators to manage staff assigned to a case, combine evidence into one folder so connections become detectable, and craft checklists for progressing through a case.[49] Importantly, CaseBuilder enables investigators to "gain insights with link analysis to connect seemingly unrelated details."[50] That means what was originally a single, siloed ShotSpotter alert is now effortlessly compiled into a comprehensive platform that includes "historical data"[51] and pin maps that reveal the location associated with a datapoint.[52]

The third tool, ResourceRouter, generates patrol routes so that "officers are at the right place at the right time to maximize crime prevention while also guarding against over and under policing."[53] Unlike the other tools on the SafetySmart Platform, ResourceRouter is geared more towards optics and the relationships officers develop within the communities they patrol.[54] For example, ResourceRouter promises to improve accountability because supervisors can track "how patrol officers are spending time on shifts" and

---

44. *CrimeTracer*, *supra* note 43.

45. *Id.*

46. *Id.*

47. *CaseBuilder*, SOUNDTHINKING, https://www.soundthinking.com/law-enforcement/investigation-management-casebuilder/ (last visited Feb. 29, 2024).

48. *Id.*

49. *Id.*

50. *Id.*

51. *Informational Webinar: After 48 Hours: The Art and Science of a Gun Crime Investigation – Part Two*, SHOTSPOTTER, https://go.soundthinking.com/first-48-part-2 (last visited Nov. 1, 2023).

52. *CaseBuilder*, *supra* note 47.

53. *ResourceRouter*, SOUNDTHINKING, https://www.soundthinking.com/law-enforcement/resource-deployment-resourcerouter/ (last Feb. 29, 2024).

54. *See id.*

"evaluate what tactics officers are using to deter crime."[55] Tactics may include a display of force such as a stop and frisk, but they can also involve non-enforcement strategies like visiting businesses, walking through vacant buildings, and engaging with community members.[56]

Unlike ResourceRouter, "traditional predictive policing methods" such as Hot Spot Analysis, Predictive Policing, and Gut-Based patrols "are often cited as . . . inherently biased and discriminatory" because they rely principally on historical data and heuristics.[57] Instead, ResourceRouter ostensibly promotes impartiality in two ways. First, its machine learning model intentionally excludes "personally identifiable information."[58] The *Citizen's Guide to ResourceRouter*, produced by SoundThinking, elaborates that the exclusion of personally identifiable information means that arrest data, demographics, and social media are not used in the model.[59] In other words, SoundThinking purports that its algorithm is neutral to race, age, and socioeconomic status.

Second, its machine learning model intentionally incorporates near real-time "objective *non-crime* data . . . to minimize the potential for bias."[60] Rather than relying purely on crime data, the model factors in "public data" such as: weather reports, census reports, temporal data that tracks holidays or school schedules, natural terrain data that provides information on valleys or waterways, and Homeland Infrastructure Foundation-Level Data (HIFLD) that tracks the location of points of interest such as schools and hospitals.[61] One example in the *Citizen's Guide to ResourceRouter* is the potential correlation between crime and the location of liquor establishments.[62] By incorporating non-crime data into the model, the company hopes to discover new correlations to improve their models that forecast crime risks.

---

55. *Id.*; Paul Lusczynski, *The Importance of Police Transparency*, SOUNDTHINKING (Apr. 4, 2022), https://www.soundthinking.com/blog/the-importance-of-police-transparency/.

56. SOUNDTHINKING, A CITIZEN'S GUIDE TO RESOURCEROUTER 4 (2023), https://www.soundthinking.com/wp-content/uploads/2021/03/2023-05-18-ResourceRouter-Citizens-Guide.pdf [hereinafter CITIZEN'S GUIDE TO RESOURCEROUTER].

57. *Id.* at 2.

58. *Id.* at 5.

59. *Id.*

60. *Id.* (emphasis added).

61. *Id.* at 6.

62. The correlation between liquor stores and crime may be relevant. For example, in the aftermath of a suspected drunk-driving incident, police officers have sought warrants to search a vehicle's "black box," which contains details about the accident, the driver, passengers, and whether the vehicle was recently driven to a liquor store. *See, e.g.*, State v. Anderson, 445 S.W.3d 895 (Tex. App. 2014).

The model also relies on "gunfire occurrence data" imported from ShotSpotter.[63] Yet the *Citizen's Guide* points out that, while gunfire is considered a legitimate input for the model, traffic stops are not because they "create negative feedback loops with enforcement bias."[64] At first blush, this strategy appears proper from a data modeling perspective. When a ShotSpotter alert is the catalyst for a traffic stop, the two events are highly correlated. The inclusion of two highly correlated variables in a single regression "distorts the results" and wreaks havoc on the ability to interpret the model.[65] Often, the simplest solution—particularly for regression analysis—is to remove one of the variables.[66] Yet, this strategy is troublesome in this context because it decouples the ShotSpotter alert from the critical information gleaned from an officer's subsequent investigation. An investigation might reveal, for example, that the alert was a false positive triggered by a firework rather than a firearm.[67] An officer's subsequent report might also reveal whether the gunshots were fired by an officer rather than a suspect.[68] A model that fails to account for false positives or shooter identity is equally likely to produce negative feedback loops and enforcement bias. It is alarming that law enforcement officers may act based on a misplaced reliance on a black-box machine learning algorithm that is propped up by potentially false or misleading gunshot data.

Finally, the fourth tool comprising the SafetySmart Platform—and the central focus of this Comment—is ShotSpotter. Whereas the other tools in the SafetySmart suite are software packages and apps, ShotSpotter is both a physical device and a software package.[69] Consequently, it can be deconstructed into its hardware, software, and humanware components.

B. How ShotSpotter Works

1. Hardware

ShotSpotter is an AGDS, which is a listening device calibrated to record the sound waves produced by gunshots.[70] From a hardware perspective, each

63. CITIZEN'S GUIDE TO RESOURCEROUTER, *supra* note 56, at 6.

64. *Id.* at 5.

65. *See* Jong Hae Kim, *Multicollinearity and Misleading Statistical Results*, 72 KOREAN J. ANESTHESIOLOGY 558, 560-64 (2019).

66. *See id.*

67. *See* discussion *infra* Section II.B.

68. *See* discussion *infra* Section II.B.

69. Throughout this Comment, "ShotSpotter" may refer to either the physical device, the software package, or both.

70. Mares & Blackburn, *supra* note 17, at 194.

acoustic sensor contains a relatively simple combination of audio recording circuitry and wireless data transmission capabilities.[71] ShotSpotter typically installs between fifteen and twenty sensors "[r]oughly the size of a medium pizza"[72] per square mile.[73] The sensors are designed to "look like a rooftop fan" and are often installed in elevated locations like utility poles and privately owned buildings.[74] Sensors may even be installed on residential homes, provided that the company privately contracts to lease the space and installs the sensor on the right home.[75] SoundThinking CEO Ralph Clark explained that the sensors are elevated so they are less likely to record ambient noise.[76] Although ShotSpotter "want[s] to be where the problem is," the exact location of any given sensor is undisclosed to permit surreptitious recording and to prevent vandalism.[77]

Supposedly, the sensors are not "lurking at every corner"[78] ready to capture casual conversations or "indoor communications."[79] The sensors are calibrated to detect only "impulsive" audio noise including any noise that goes "bang, boom, or pop."[80] One SoundThinking employee testified that the trigger sound "could be anything" that has a "sharp enough rise in time . . . and a rise in amplitude," like fireworks, loud trucks, and construction equipment.[81] Two of the more popular examples of trigger sounds that might

71. *See* Jay Stanley, *ShotSpotter CEO Answers Questions on Gunshot Detectors in Cities*, ACLU (May 5, 2015), https://www.aclu.org/news/privacy-technology/shotspotter-ceo-answers-questions-gunshot.

72. Gecas, *supra* note 6, at 1080; Busljeta, *supra* note 12, at 214.

73. Stanley, *supra* note 71.

74. Gecas, *supra* note 6, at 1080; *see* Craig, *supra* note 24.

75. *ShotSpotter Device Mounted on House Without Owner's Knowledge*, TARGET 11 NEWS (Sept. 27, 2018, 6:46 PM), https://www.wpxi.com/news/top-stories/shotspotter-device-mounted-on-house-without-owner-s-knowledge-1/842332068/.

76. Busljeta, *supra* note 12, at 214.

77. Gecas, *supra* note 6, at 1078-80.

78. *Id.* at 1076.

79. Busljeta, *supra* note 12, at 215.

80. State v. Hill, 851 N.W.2d 670, 678 (Neb. 2014); Busljeta, *supra* note 12, at 213; Jonah Owen Lamb, *Courtroom Testimony Reveals Accuracy of SF Gunshot Sensors a 'Marketing' Ploy*, SAN FRANCISCO EXAMINER (July 11, 2017), https://www.sfexaminer.com/news/courtroom-testimony-reveals-accuracy-of-sf-gunshot-sensors-a-marketing-ploy/article_915b5ea6-3d17-5132-9166-c6934b461b97.html.

81. Brief for Amici Curiae at 12, Commonwealth v. Ford, 182 N.E.3d 1013 (Mass. App. Ct. 2022) (No. 20-P-1334), https://www.macarthurjustice.org/wp-content/uploads/2021/05/Commonwealth-v-Ford-Amicus-Brief.pdf (quoting Testimony of Paul Greene, ShotSpotter Manager of Forensic Services, at 113:19-114:2, California v. Reed, No. 16015117 (Cal. Super. Ct. S.F. County July 5-6, 2017)).

result in false positives include a car backfiring[82] or a helicopter.[83] Temporarily setting aside reliability concerns, one thing is clear: sounds reaching the decibel threshold are recorded agnostically.[84] In other words, the sensors are not discriminatorily filtering gunshots based on the shooter's status as a law-abiding civilian, militant, criminal, or law enforcement officer.

Once recorded, a short audio snippet is stored in ShotSpotter's cloud computing system[85] where it is kept for "hours or days, not weeks" and overwritten "on a rolling basis."[86] The snippets are designed to include only a "very narrow audio window" that is approximately two seconds before the concussive noise that triggered the sensor and four seconds after.[87]

2. Software

After recordation and memorialization, the sound bites are analyzed by the company's software. The first wave of audio-screening occurs when the data is filtered through the company's two proprietary algorithms.[88] The first algorithm triangulates the location where the concussive sound was produced.[89] Using an algorithm sounds mysterious, but SoundThinking assures its customers that it is nothing more than "math and physics," that "the approach has been around since WW1," and that the company has been transparent due to its publication of an article explaining how audio processing works.[90] Second, another algorithm classifies the percussive noise

82. Gecas, *supra* note 6, at 1079; Busljeta, *supra* note 12, at 214; Matthew Guariglia, *It's Time for Police to Stop Using ShotSpotter*, ELEC. FRONTIER FOUND. (July 29, 2021), https://www.eff.org/deeplinks/2021/07/its-time-police-stop-using-shotspotter.

83. Ethan Waters, *Shot Spotter*, WIRED (Apr. 1, 2007, 12:00 PM), https://www.wired.com/2007/04/shotspotter/.

84. Gecas, *supra* note 6, at 1079.

85. Brief for Amici Curiae, *supra* note 81, at 12 (citing Testimony of Paul Greene, *supra* note 81, at 14:8-15:16).

86. Busljeta, *supra* note 12, at 215.

87. Craig, *supra* note 24; *see also* Stanley, *supra* note 71.

88. Busljeta, *supra* note 12, at 214; *SoundThinking Responds to False Claims*, SOUNDTHINKING, https://www.shotspotter.com/shotspotter-responds-to-false-claims/ (last visited Feb. 29, 2024).

89. *See, e.g.*, JOSEPH M. FERGUSON & DEBORAH WITZBURG, OFF. OF INSPECTOR GEN., CITY OF CHI., OIG FILE NO. 21-0707, THE CHICAGO POLICE DEPARTMENT'S USE OF SHOTSPOTTER TECHNOLOGY 4 (2021), https://igchicago.org/wp-content/uploads/2021/08/Chicago-Police-Departments-Use-of-ShotSpotter-Technology.pdf; *SoundThinking Responds to False Claims*, *supra* note 88.

90. *See SoundThinking Responds to False Claims*, *supra* note 88.

as a gunshot.[91] SoundThinking claims the algorithm filters out most sounds that are not gunshots.[92] Yet, because SoundThinking can hide behind claims that the algorithm is proprietary, independent testing and verification is relatively sparse. Accordingly, the company's self-proclaimed transparency remains questionable.[93]

SoundThinking recently restructured its website to include an entire page dedicated to "debunking the top myths" about how ShotSpotter operates.[94] The company claims that independent auditing confirms that ShotSpotter does not suffer from a high false positive rate.[95] But the "independent" auditor was Edgeworth Economics—a data analytics consulting firm that was hired by SoundThinking to audit data it obtained from SoundThinking personnel.[96] Funding for Edgeworth Economics is not disclosed in the report.[97]

3. Humanware

As intimated, ShotSpotter's software is not the final decision maker in the classification of sounds as gunshots. Instead, it employs humanware as the final verification that the recorded sound is indeed a gunshot.[98] The humanware step begins with a SoundThinking operator evaluation and concludes when the officer's device is pinged with an alert similar to a banner notification that accompanies a text message on a smartphone.[99] First, the sound data is transferred to the company's call-center staff located in either

91. Craig, *supra* note 24; Stanley, *supra* note 71.

92. *See SoundThinking Responds to False Claims*, *supra* note 88.

93. *See* Elizabeth A. Rowe & Nyja Prior, *Procuring Algorithmic Transparency*, 74 ALA. L. REV. 303, 305-08 (2022) (criticizing ShotSpotter's lack of transparency due to claiming a trade secret); Craig, *supra* note 24 (explaining that the proprietary nature of ShotSpotter's data was likened to the Colonel Sanders fried chicken recipe by one reporter critical of the lack of transparency).

94. *See SoundThinking Responds to False Claims*, *supra* note 88.

95. EDGEWORTH ECON., INDEPENDENT AUDIT OF THE SHOTSPOTTER ACCURACY, 2019-2022, at 1 (2023), https://www.edgeworthconomics.com/assets/htmldocuments/Independent%20Audit%20of%20the%20ShotSpotter%20Accuracy%202019-2022.pdf.

96. *Id.* at 3.

97. *Id.* at 1-5.

98. Craig, *supra* note 24; Stanley, *supra* note 71.

99. *See Frequently Asked Questions*, SHOTSPOTTER, https://www.soundthinking.com/faqs/shotspotter-faqs/ (last visited Apr. 21, 2024); SoundThinking, *How ShotSpotter Protects Your Community and Saves Lives*, YOUTUBE (June 28, 2023); State v. Carter, 183 N.E.3d 611, 612 ("In describing the ShotSpotter system, [the officer] testified that 'whenever a ShotSpotter alert goes off, it pops up as a notification on your phone' and gives the location that the shots came from with a certain radius and the number of shots fired.").

Newark, California or Washington D.C.[100] SoundThinking's human operators, who are often hired with only a high school diploma, are not sophisticated audio technicians.[101] Despite a lack of expertise, operators are charged with listening to the extracted sound bite and visually inspecting the waveform to issue a subjective judgment on whether the noise was in fact a gunshot.[102] They may also add additional information like how many weapons were fired.[103] This entire process from recordation via hardware to algorithm processing via software and then operator review via humanware occurs in under one minute.[104] And, according to the company, it is 97% accurate.[105] If the operator, acting as the final gatekeeper, determines that the sound is a gunshot, then the alert is pushed to a law enforcement officer's device and the second phase of the humanware component is initiated.[106]

Verification is presumed complete before the alert pings the officer's device. Thus, unlike the prior steps, confirming whether the sound was a gunshot is not a lauded feature of this phase. In fact, SoundThinking does not describe officer review as a feature of its services, but it is crucial to bookmark the analysis with how the officers interact with the alert because it informs the Fourth Amendment legal analysis. Officers "use a program on their laptops or smart phones called Alert Console," which displays notifications as badges and banners like any other smart phone app.[107] Visually, the end-user display turns "shots fired into dots on a map"[108] so that officers have a "bird's-eye view of the area"[109] where the alleged firearm was discharged.

---

100. Chris Mills Rodrigo, *Gunshot Detection Firm ShotSpotter Expands with New DC Office*, THE HILL (July 14, 2021, 3:18 PM), https://thehill.com/policy/technology/563028-gunshot-detection-firm-shotspotter-expands-with-new-dc-office/; Stanley, *supra* note 71.

101. Brief for Amici Curie, *supra* note 81, at 13.

102. *See* Stanley, *supra* note 71; Guariglia, *supra* note 82 ("The sensors themselves can only determine whether there is a loud noise that somewhat resembles a gunshot. It's still up to people listening on headphones to say whether or not shots were fired."); *SoundThinking Responds to False Claims*, *supra* note 88.

103. Busljeta, *supra* note 12, at 213.

104. *Id.*

105. Press Release, MacArthur Just. Ctr., ShotSpotter Generated Over 40,000 Dead-End Police Deployments in Chicago in 21 Months, According to New Study (May 3, 2021), https://www.macarthurjustice.org/shotspotter-generated-over-40000-dead-end-police-deployments-in-chicago-in-21-months-according-to-new-study/.

106. Stanley, *supra* note 71.

107. Gecas, *supra* note 6, at 1080; *see* sources cited *supra* note 99.

108. Drange, *supra* note 18.

109. Gecas, *supra* note 6, at 1080.

Armed with seemingly trustworthy data, officers make real-time decisions affecting how they respond to the alert. For example, if the gunfire registers as consecutive bursts discharged from a fully automatic weapon, then "you don't send just one officer into that situation."[110] The alert can also indicate "whether a gun was fired from a car" and officers may respond accordingly.[111] In a survey commissioned by SoundThinking, officers signaled a high level of deference to the gunshot detection data when they explained that an alert makes them "pretty damn sure" they are apprehending an active shooter.[112] But when officers arrive at an actionless scene, they may have no way to determine if the alert was a false positive or if the suspect got away because they typically were not on the scene to hear the noise that triggered the alert.[113] In Chicago, for example, officers failed to report *any* false positives, despite a report from the city's Inspector General that revealed 90.9% of ShotSpotter alerts were dead ends.[114] Edgeworth Economics, the "independent" auditor that evaluated ShotSpotter data, acknowledged that the false positive rate depends on clients reporting dead-end alerts.[115] Curiously, Edgeworth reported no statistical significance between clients with high versus low reporting rates, which suggests that officer reporting is moot when evaluating ShotSpotter's efficacy.[116]

Under the Fourth Amendment, however, the debate over ShotSpotter's accuracy might be a red herring. Arguably what matters is what law enforcement officers *perceive*, not necessarily the *actual* accuracy or reliability of the technology.[117] When officers perceive a high level of accuracy, the alert creates confirmation bias for whatever they may encounter

110. Stanley, *supra* note 71.

111. Gecas, *supra* note 6, at 1083.

112. NICK SELBY ET AL., CSG ANALYSIS, SHOTSPOTTER GUNSHOT LOCATION SYSTEM EFFICACY STUDY 23 (2011), https://www.defendyouthrights.org/wp-content/uploads/2017/10/Shot-Spotter-Gunshot-Location-System-Efficacy-Study.pdf.

113. In at least one lower court opinion, the officers were close enough to hear the gunshot themselves. State v. Hill, 851 N.W.2d 670, 690 (Neb. 2014). Any challenge to the use of ShotSpotter was "somewhat dubious given that the sounds of gunshots in the general area identified by ShotSpotter were simultaneously heard by" the same officers who responded to the alert. *Id.*

114. *See* FERGUSON & WITZBURG, *supra* note 89.

115. EDGEWORTH ECON., *supra* note 95.

116. *Id.*

117. *See* Elizabeth E. Joh, *The Unexpected Consequences of Automation in Policing*, 75 SMU L. REV. 507, 526-28 (2022).

while investigating. Thus, innocent pedestrians become suspicious based on their mere proximity to the location identified by ShotSpotter.[118]

To compound the issue, what used to be a single, siloed ShotSpotter alert is now automatically linked to the abundant data housed in the SafetySmart Platform. Regardless of whatever events actually take place on the ground, the fact that SoundThinking is expertly marketed as a sophisticated tool rooted in cold-hard data likely biases officer decision-making. Imagine the uninformed and innocent bystander interacting with an officer who was (1) quickly dispatched by ResourceRouter, (2) armed with a ShotSpotter alert indicating the bystander is standing within five yards of a gunshot, (3) in a location CaseBuilder identified as historically violent, and (4) connected to nearby suspicious activity through the link analysis provided by CrimeTracer. Admittedly, that concocted scenario is among the worst imaginable, but the coalescence of immense surveillance powers used to invade a person's sense of security is what the Fourth Amendment is supposed to guard against.

III. Introduction to the Fourth Amendment

The Fourth Amendment protects individuals from unreasonable searches and seizures by the government.[119] The relevant text of the Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[120] In addition, the Amendment dictates the requirements that must be satisfied when the government obtains a warrant to validate any search or seizure.[121] The fifty-four words comprising the Fourth Amendment are the subject of lively debate between civil libertarian values and society's interest in effective law enforcement. In striking that balance, two dominant Fourth Amendment frameworks are relevant for taking aim

118. In *Ybarra v. Illinois*, the Supreme Court held that "a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." 444 U.S. 85, 91 (1979). In *Ybarra*, the police had a warrant to search a bar and the bartender for drugs. *Id.* at 88. When police arrived, however, they performed cursory searches of "a dozen or so" customers who happened to be present during the execution of the warrant. *Id.* at 98 (Rehnquist, J., dissenting). By the same logic, a person's "mere propinquity" to a ShotSpotter alert does not dispense with the need to obtain probable cause (to search or seize) or reasonable suspicion (to stop and frisk). *See id.* at 91 (majority opinion).

119. U.S. CONST. amend. IV.

120. *Id.*

121. *Id.*

at tools like ShotSpotter: the stop and frisk framework or the search and seizure framework.

A. Stop and Frisk

This Section begins by explaining how the stop and frisk framework differs from alternative interactions a civilian could have with a police officer. Next, this Section explores the origins of the stop and frisk framework, including leading theories on why the Supreme Court diverged from precedent. Second, this Section argues that the reasonable suspicion standard is deeply flawed because it unfairly tips the scales in favor of expedient—rather than prudent—enforcement of the law. Third, this Section concludes that SoundThinking will continue to prevail in lower courts as long as the analysis continues to center on the stop and frisk interaction, rather than challenging the constitutionality of ShotSpotter as a search. Finally, even though SoundThinking escapes constitutional muster under the stop and frisk framework, lower courts' characterization of ShotSpotter as merely a means to and end causes the company to suffer reputational harm.

1. Origins of the Stop and Frisk Framework

Not every interaction with law enforcement results in an unconstitutional restraint on a person's liberties.[122] An irreducible quantity of interactions can occur between police and civilians, but the law attempts to confine those interactions on a spectrum from least to most constitutionally suspect. At one end of the spectrum, the least constitutionally suspect type of interaction is classified as an encounter.[123] Examples of an encounter include brief consensual conversations in public places[124] and consensual searches of personal belongings.[125] Unlike stops or seizures, police must

122. *See, e.g.*, United States v. Mendenhall, 446 U.S. 544 (1980).

123. *See* N.Y.C. Police Dep't, Procedure No. 212-11, Patrol Guide: Investigative Encounters: Requests for Information, Common Law Right of Inquiry and Level 3 Stops (Oct. 15, 2016), https://www.nyc.gov/html/nypd/downloads/pdf/analysis_and_planning/212-11.pdf (describing the levels of encounters in the State of New York and federally); *see also* Terry v. Ohio, 392 U.S. 1, 16 (1968) (noting the variety of encounters that the police have with individuals on the street and refusing to "canvass in detail" the constitutional limitations on a policeman's power to confront a citizen in encounters).

124. *See* Florida v. Royer, 460 U.S. 491 (1983).

125. *See* Florida v. Bostick, 501 U.S. 429 (1991).

satisfy very minimal thresholds to justify an encounter.[126] As long as the interaction is consensual and the person's freedom of movement is not restrained by physical force or a show of authority, then the interaction is not inherently constitutionally suspect.[127]

At the other end of the spectrum, the most constitutionally suspect interaction is classified as a seizure. Examples of seizure under the Fourth Amendment include *de facto* arrests[128] or a "meaningful interference with an individual's possessory interests in [their] property."[129] Because a seizure is the most restrictive type of interaction, officers must have probable cause, a warrant, or an exception must apply.[130]

Somewhere in the middle of the spectrum is the elusive stop and often concomitant frisk.[131] Unlike a seizure, which requires probable cause, a stop is justified when it is supported by reasonable suspicion.[132] The stop and frisk framework and subsequent reasonable suspicion standard was the product of judicial invention in a famous case, *Terry v. Ohio*.[133]

In *Terry*, an officer dressed in plainclothes was on patrol near a shopping center in Cleveland, Ohio.[134] Around 2:30 in the afternoon, his attention was drawn to two African American men who were standing on the corner.[135] The officer could not articulate exactly what caught his eye, but he considered their conduct suspicious and said at trial that he "just didn't

126. PRINCIPLES OF THE L., POLICING § 4-02 (AM. L. INST., Combined Revised Tentative Drafts Jan. 2023), https://www.policingprinciples.org/wp-content/uploads/2023/01/Policing-Tentative-Draft_1-31-23.pdf.

127. *Mendenhall*, 446 U.S. at 553 ("We adhere to the view that a person is 'seized' only when, by means of physical force or a show of authority, his freedom of movement is restrained.").

128. *See* Dunaway v. New York, 442 U.S. 200, 208 (1979).

129. *See* United States v. Karo, 468 U.S. 705, 712 (1984).

130. *Dunaway*, 442 U.S. at 201, 210-13.

131. Although "stop and frisk" is typically uttered as one phrase, a stop is legally distinct from a frisk. Thus, the stop and frisk analysis requires a two-step analysis. *See* THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 151-57, 228-29. (2d ed. 2014).

132. *See Terry*, 392 U.S. at 27 (permitting a stop and frisk search only when an officer acts on "specific reasonable inferences which he is entitled to draw from the facts in light of his experiences"); *see also id.* at 37 (Douglas, J., dissenting) (coining the term "reasonable suspicion").

133. *See Terry*, 392 U.S. at 30-31.

134. *Id.* at 5.

135. *Id.*

like 'em."[136] During his observation of the two suspects, the officer witnessed odd behavior and concluded that the two suspects were planning to rob a nearby store.[137] Fearing that one of them was carrying a gun, the officer elected to take action before any violence ensued.[138] As he approached the men, he announced his status as a law enforcement officer and then grabbed one of the men, forcefully spun him around, and patted the exterior of the man's clothing.[139] The officer repeated the process for the second suspect and discovered through each "patdown" that both men were armed with pistols.[140]

The facts in *Terry* were an enigma because they did not fit neatly into either end of the spectrum: the interaction could not be classified as an encounter because it was not consensual, but classifying the interaction as a seizure would require the officer to have probable cause or a warrant—a threshold that was problematic for officers on the beat reacting quickly to prevent crime.[141] Facing a dilemma and desiring a more lenient standard that favored efficient and effective law enforcement, the Supreme Court announced the stop and frisk rule. Under the stop and frisk analysis, an officer's conduct is constitutional so long as the officer has reasonable suspicion to believe that crime is afoot to justify the stop and reasonable suspicion to believe the suspects are armed and dangerous to justify the frisk.[142]

2. Reasonable Suspicion Is a Flawed Standard

The reasonable suspicion standard required to justify a stop and frisk is deeply flawed because it undermines the rights and dignity of individuals who are targeted by police surveillance. Although it is touted as a necessary tool for the efficient and effective enforcement of the law, it allows officers

136. Terry's defense counsel recalled this exchange when reflecting on his representation of Terry thirty years after the case was decided. Louis Stokes, *Representing John W. Terry*, 72 ST. JOHN'S L. REV. 727, 729-30 (1998).

137. *Terry*, 392 U.S. at 6.

138. *Id.*

139. *Id.* at 7.

140. *Id.*

141. This is a diminishing threshold, however, because electronic warrants ("e-warrants") allow magistrate "judges to review and then approve or deny warrant applications on computers, smartphones, and tablets." Tracy Hresko Pearl, *On Warrants & Waiting: Electronic Warrants and the Fourth Amendment*, 99 IND. L.J 1, 3 (2023).

142. *See Terry*, 392 U.S. at 30-31.

to stop and frisk individuals based on comparatively minimal evidence.[143] The standard is also inherently subjective and at risk of abuse because it gives law enforcement wide latitude to target suspects based on their race, ethnicity, or other discriminatory criteria[144]—for example, proximity to a high-crime neighborhood outfitted with ShotSpotter sensors. Academics complain that this standard results in a disproportionate number of encounters between officers and minority populations and that it reinforces systemic racism.[145] Furthermore, it is questionable whether the stop and frisk tactic is effective at reducing crime.[146] Instead, scholars theorize it produces negative externalities such as an erosion of trust and destruction of the relationships between law enforcement and the communities they serve.[147]

---

143. *See* Akhil Reed Amar, Terry *and Fourth Amendment First Principles*, 72 ST. JOHN'S L. REV. 1097, 1098-99 (1998) (describing a "good *Terry*" and a "bad *Terry*" where the "good *Terry*" is "*proportionate* to legitimate governmental purposes" and focuses "not only on privacy and secrecy but also on *bodily integrity* and *personal dignity*").

144. For example, the Seventh Circuit condoned the actions of five members of a special task force that descended upon a parked vehicle in a high crime area and pulled the African American occupants out, allegedly to determine whether the car was parked illegally. United States v. Johnson, 823 F.3d 408, 409-10 (7th Cir. 2016), *aff'd*, 874 F.3d 571 (7th Cir. 2017). The dissent lambasted the reasonable suspicion standard for permitting such aggressive tactics simply for "parking while black." *Id.* at 412 (Hamilton, J., dissenting).

145. *See* Tracey Maclin, Terry v. Ohio*'s Fourth Amendment Legacy: Black Men and Police Discretion*, 72 ST. JOHN'S L. REV. 1271, 1275-77, 1285-87 (1998).

146. *See, e.g.*, John MacDonald, *Does Stop-and-Frisk Reduce Crime?*, U. PA. SCH. OF ARTS & SCIS.: DEP'T OF CRIMINOLOGY, https://crim.sas.upenn.edu/fact-check/does-stop-and-frisk-reduce-crime (last visited Apr. 7, 2024) (concluding investigative stops do not play a meaningful role in crime reduction); David Weisburd et. al., *Do Stop, Question, and Frisk Practices Deter Crime?: Evidence at Microunits of Space and Time*, CRIMINOLOGY & PUB. POL'Y, Nov. 2015, at 1, 1-2 (suggesting that while stop question and frisk policies worked, it is unclear whether other similar policies may be more effective and less costly or harmful to police legitimacy); Dan Keating & Harry Stevens, *Bloomberg Said 'Stop and Frisk' Decreased Crime. Data Suggests It Wasn't a Major Factor in Cutting Felonies*, WASH. POST (Feb. 27, 2020), https://www.washingtonpost.com/nation/2020/02/27/bloomberg-said-stop-frisk-decreased-crime-data-suggests-it-wasnt-major-factor-cutting-felonies/.

147. *See* Scott E. Sundby, *An Ode to Probable Cause: A Brief Response to Professors Amar and Slobogin*, 72 ST. JOHN'S L. REV. 1133, 1137-38 (1998) ("[T]he Amendment also becomes part of the mutually reinforcing consent that flows between the citizenry and the government, a form of reciprocal trust: The citizenry gives its consent and trust to the government to be governed and the government, in turn, trusts the citizenry to exercise its liberties responsibly. . . . This idea of trust is why probable cause must be the center of the Fourth Amendment universe rather than . . . merely one satellite in orbit around a general reasonableness balancing test."); *see also id.* at 1133-35.

To illustrate why reasonable suspicion is a constitutionally suspect standard, look no further than the annual crime data reported by the Federal Bureau of Investigation (FBI).[148] Arrest data, excluding traffic offenses, is sorted into more than twenty categories.[149] In 2021, drug abuse violations were the leading cause of an arrest, resulting in more than 665,000 arrests nationwide.[150] In that same year, there were more than 661,000 arrests attributed to simple assault.[151] By comparison, possession of a weapon constituted the eighth most frequent cause for an arrest, resulting in just over 113,000 arrests.[152] Additional categories include larceny, fraud, robbery, rape, vagrancy, and driving under the influence.[153] The last category listed, however, is simply termed "Suspicion."[154]

In 2021, there were seven arrests for "Suspicion," but in 2020 there were 460 arrests for "Suspicion."[155] In 2019, there were 1,325 arrests for "Suspicion."[156] And in the last ten years, the aggregate frequency of "Suspicion" arrests was 20,552—more than four times that of manslaughter by negligence and more than six times that of human trafficking associated with commercial sex acts.[157] But "Suspicion" is not a crime in the United States. What this means, then, is that suspects were arrested by officers who wanted to further their investigation but likely did not possess enough evidence to justify filing a specific charge.[158]

---

148. *See Trend of Violent Crime from 2012 to 2022*, FED. BUREAU OF INVESTIGATION CRIME DATA EXPLORER, https://cde.ucr.cjis.gov/LATEST/webapp/#/pages/explorer/crime/crime-trend (last visited Feb. 5, 2023). The data is visually manipulable on the FBI's Crime Data Explorer.

149. *Arrest Offense Counts in the United States*, FED. BUREAU OF INVESTIGATION CRIME DATA EXPLORER, https://cde.ucr.cjis.gov/LATEST/webapp/#/pages/explorer/crime/arrest (last visited Feb. 29, 2024).

150. *Id.*

151. *Id.*

152. *Id.*

153. *Id.*

154. *Id.*

155. *Id.*

156. *Id.*

157. *Id.*

158. This is what happened to Elijah McClain, a young African American male who died during a *Terry* stop in Aurora, Colorado in 2019. Within less than eight seconds of getting out of his police cruiser, the officer was already physically aggressive with McClain and shouting: "I have a right to stop you because you are being suspicious." NBC News, *Minute-to-Minute Breakdown Leading up to Elijah McClain's Deadly Stop*, YOUTUBE (June 27, 2020), https://www.youtube.com/watch?v=dGlHMZQtO7U. McClain was wearing a mask walking home from a local convenience store. *Id.*

Although the number of arrests reported under the "Suspicion" category have dwindled over time, it is still frequent enough that the FBI reports it without so much as an acknowledgement. Unfettered gun violence is surely not the hallmark of a thriving nation, but the trifecta of ShotSpotter surveillance, the easily satisfied dictates of reasonable suspicion, and the possibility of an arrest for mere "Suspicion" is likewise not the hallmark of a free and just society.

3. ShotSpotter Will Continue to Escape Constitutional Attack as Long as Lower Courts Fixate on Stop and Frisk

The stop and frisk framework is a natural starting point for combatting ShotSpotter in the lower courts because it is the primary interaction that results in charges against the defendant.[159] In other words, without the stop and frisk interaction, the aggrieved party would not have been dragged into court. Generally, lower court opinions favor ShotSpotter because they tend to focus on three factors: (1) officer response time to the location indicated by the ShotSpotter alert; (2) defendant's physical proximity to the location indicated by the ShotSpotter alert; and (3) officer testimony pointing to additional suspicious behavior that satisfies the reasonable suspicion standard. Because rapid response time is correlated with observing the defendant's proximity to the location, the analyses for the first two factors tend to collapse together.

First, lower courts seeking to validate a stop and frisk emphasize the officer's rapid response time and subsequent observation of the defendant's physical proximity to the location identified by the alert. In a 2021 case, for example, the Supreme Court of Wisconsin pointed out that officers were able to arrive "on scene [in] no more than *one minute*" and spotted the defendant "basically [in] the exact location" indicated by the alert.[160] Defense counsel countered that proximity cannot serve as the basis for reasonable suspicion because ShotSpotter only "tells officers what, when, and where, but not who."[161] The court disagreed, however, and reinforced that "the timing of events is key" because although the defendant "could have been a random pedestrian out for a walk," the officers had no

159. This is likely why the stop and frisk framework dominates the analysis in Circuit Court opinions that address ShotSpotter. *See, e.g.*, Harvey Gee, *"Bang!": ShotSpotter Gunshot Detection Technology, Predictive Policing, and Measuring* Terry*'s Reach*, 55 U. MICH. J. L. REFORM 767, 797-804 (2022). And it is likely a factor in why lower court opinions never address the search doctrines. *See infra* Section III.A.3.

160. State v. Nimmer, 975 N.W.2d 598, 601 (Wis. 2022) (emphasis added).

161. *Id.*

obligation to "rule out any alternative explanation for his presence at the scene."[162]

Similarly, the Court of Appeals of Ohio evaluated ShotSpotter and concluded that response time and the defendant's physical proximity were key facts that weighed in favor of finding the reasonable suspicion quantum satisfied. In that case, officers were on a "routine patrol in a marked cruiser" when they received a ShotSpotter alert.[163] The officers were operating under the belief that "less than 30 seconds elapse[d] between the shots being detected and the alert being issued."[164] After receiving an alert on his phone, the officers responded "in less than four minutes."[165] When they arrived, they noticed the defendant approximately fifty feet from the location identified by ShotSpotter.[166] In addition, "the officers did not observe anyone else in the area, any motor vehicle traffic, or any activity on any adjacent property."[167] Given their rapid response time coupled with the fact that the defendant was the only person in close proximity to the location identified by the alert, the officers approached the individual to continue their investigation.[168]

Circuit courts have similarly relied on response time and proximity as indicators that the reasonable suspicion standard was satisfied. For example, the United States Court of Appeals for the District of Columbia noted that officers relying on ShotSpotter arrived on scene within only a minute and a half of the alert.[169] Likewise, the Seventh Circuit found the timing argument compelling even though the officers arrived at the scene a little more than five minutes after the ShotSpotter alert was pushed to their device.[170] According to the Seventh Circuit, "[c]ommon sense counsels that a person may take minutes rather than seconds to flee" the scene of a crime, destroy evidence, or hide.[171]

From a policy perspective, an emphasis on response time and physical proximity is sensible. Assuming ShotSpotter accurately pinpoints the gunshot location, officers responding quickly may be in a better position to observe the original crime scene and offer aid to gunshot victims.

162. *Id.* at 605, 606.
163. State v. Carter, 183 N.E.3d 611, 612 (Ohio Ct. App. 2022).
164. *Id.*
165. *Id.* at 612, 613.
166. *Id.* at 613.
167. *Id.*
168. *See id.*
169. United States v. Jones, 1 F.4th 50, 53 (D.C. Cir. 2021).
170. United States v. Rickmon, 952 F.3d 876, 883 (7th Cir. 2020).
171. *Id.*

Furthermore, when response time is fast, it is logical to investigate nearby individuals who may have been involved in the incident or possess information about the concussive noise that caused the ShotSpotter alert. In this sense, ShotSpotter alerts create "an acoustic trail of breadcrumbs, from which it [is] reasonable to infer that the person responsible for the potential gunshots would be at or near the location where the ShotSpotter had last activated."[172] While response time and proximity are part of the reasonable suspicion calculus, one Massachusetts trial judge aptly explained that "[i]t is the police investigation *as a result of a [ShotSpotter] alert* that is primarily determinative on the issue of reasonable suspicion."[173]

When the Seventh Circuit Court of Appeals analogized ShotSpotter to an anonymous tipster, it "question[ed] whether a single ShotSpotter alert would amount to reasonable suspicion."[174] This conclusion is likely because ShotSpotter lacks the indicia of reliability that the Fourth Amendment demands for anonymous tipsters.[175] Furthermore, unlike investigative tools like drug-sniffing dogs, ShotSpotter is not currently subjected to any regulatory requirements like a maintenance record or record of false positives.[176] Thus, when upholding the constitutionality of a stop and frisk, lower courts overwhelmingly emphasize officer testimony pointing to additional suspicious behavior that satisfies the reasonable suspicion quantum.[177] The idea is that, even if there are concerns with ShotSpotter, officers cannot be expected to turn a blind eye to additional suspicious conduct they observe first-hand. Consequently, under the stop and frisk framework, it is immaterial whether ShotSpotter serves as the catalyst that draws officers to the scene.[178] Therefore, it is also immaterial whether ShotSpotter is accurate or reliable. For example, the Appeals Court of Massachusetts described ShotSpotter as a gateway that did "little more

172. Commonwealth v. Ford, 182 N.E.3d 1013, 1018 (Mass. App. Ct. 2022).

173. *Id.* at 1017 (emphasis added).

174. *Rickmon*, 952 F.3d at 881.

175. *See* Alabama v. White, 496 U.S. 325, 328 (1990) ("We concluded that, while the unverified tip may have been insufficient to support an arrest or search warrant, the information carried sufficient 'indicia of reliability' to justify a forcible stop.") (quoting Adams v. Williams, 407 U.S. 143, 147 (1972)).

176. *See* Florida v. Harris, 568 U.S. 237, 244-46 (2013) (examining a drug dog's prior "hits" and "misses" in the field).

177. *See* State v. Nimmer, 975 N.W.2d 598, 601 (Wis. 2022); *see also* State v. Carter, 183 N.E.3d 611, 613 (Ohio Ct. App. 2022).

178. *See Ford*, 182 N.E.3d at 1019.

than point the police in the right direction to investigate the *possibility* of a shot being fired."[179]

ShotSpotter is a prime example of the failures of the reasonable suspicion standard of proof because officers can point to a range of conduct that, without the ShotSpotter alert, might otherwise seem innocuous. For example, officers in *Carter* noticed that the defendant's "right side was canted away" as they approached from behind.[180] With only this information, the officer performed a patdown in search of weapons.[181] Although the patdown did not reveal a firearm, it was nonetheless a fruitful frisk because the officer found methamphetamines on the defendant.[182] The Court of Appeals of Ohio ultimately concluded the officers had reasonable suspicion to support the frisk.[183]

Likewise in *State v. Nimmer*, officers claimed that the suspect "accelerated his pace" away from the officer's squad car and then began digging around on his left side and shielding his left shoulder from officers.[184] One of the officers responding that night was a "nine-year police veteran" whose typical duties included responding to gun violence.[185] Based on his experience, he explained that his strategy for responding to a ShotSpotter alert included evaluating the suspect's "response . . . upon sight of police [to] see if they are shot, see if they take off running, [or to] see if they start grabbing any part of their clothing."[186]

While this approach survives constitutional muster under the stop and frisk framework, it warrants concern from top executives at SoundThinking. Lower court opinions that over-emphasize an officer's subjective on-the-scene assessment of additional suspicious conduct dodge an analysis of ShotSpotter's reliability. Consequently, lower court opinions do not claim ShotSpotter is a precise, predictable, or reliable tool. Instead, ShotSpotter is characterized as merely a means to an end. Regardless of its reliability, it is the tool that puts boots on the ground, and once officers are on the scene, they can point to any other "suspicious" behavior to justify

179. *Id.* at 1018 (emphasis added). The court then describes ShotSpotter as "merely as an indicator of 'potential' gunshots" that warrants additional investigation. *Id.* at 1017 n.8.

180. *Carter*, 183 N.E.3d at 613. Although the defendant "was merely walking down the sidewalk, both officers clearly testified that he canted his body in such a manner that they were unable to observe his right side." *Id.* at 629.

181. *Id.* at 613.

182. *Id.*

183. *Id.* at 633.

184. 975 N.W.2d 598, 599 (Wis. 2022).

185. *Id.* at 600.

186. *Id.*

their stop. When lower courts sidestep the reliability analysis, it undermines SoundThinking's reputation because it portrays the technology as a loose cannon.

ShotSpotter will continue to evade constitutional attack as long as lower courts rely on the stop and frisk framework. Even when a false positive ShotSpotter alert is the catalyst for an interaction, the inescapable reality is that reasonable suspicion is a standard too-easily satisfied. Instead, the more effective strategy to take aim at ShotSpotter requires attacking the technology before a *Terry* stop ever occurs.

B. Search and Seizure

This Section explains how the reasonable suspicion standard required for a stop and frisk differs from the probable cause standard required for a search and seizure. Next, this Section outlines the four core doctrines the Court uses to analyze whether government conduct constitutes a search under the Fourth Amendment. Finally, this Section concludes that ShotSpotter will remain immune to challenges under the Fourth Amendment unless the Court adopts a new approach.

Unlike the Court's stop and frisk analysis, the issue of whether government conduct constitutes a search and seizure has puzzled the Court since the birth of the nation. Consequently, the Court has developed a series of rational taxonomies for ordering human affairs and guiding lower courts in determining whether a search has occurred. That taxonomy is comprised of four core tests: (1) the *Jones* Physical Intrusion test, which resurrected the trespass doctrine;[187] (2) the *Katz* Reasonable Expectation of Privacy test;[188] (3) the *Kyllo* test, which Justice Scalia invented to manage emerging technologies;[189] and (4) the Court's recent adoption of the *Carpenter* test that modifies *Katz* for information disclosed to third parties.[190] Each of the four tests can function as either a sword for law enforcement or as a shield for citizens, but it would be questionable to assume that any single test sufficiently protects citizens from ShotSpotter.

187. *See* United States v. Jones, 565 U.S. 400 (2012).
188. *See* Katz v. United States, 389 U.S. 347 (1967).
189. *See* Kyllo v. United States, 533 U.S. 27 (2001).
190. *See* Carpenter v. United States, 585 U.S. 296 (2018).

1. Jones*: Trespass Doctrine Keeps Easy Cases Easy While Not Thwarting ShotSpotter*

Technical trespass was an early search doctrine adopted by the Court in *Olmstead v. United States.* Roy Olmstead was a suspected bootlegger who was caught after federal agents installed wiretaps in the building where he maintained an office and in the streets near his home.[191] In a 5-4 decision, the Court found no Fourth Amendment violation because the wiretaps were inserted "without trespass upon any property of the defendants."[192] While the Court admitted surreptitious wiretapping was arguably unethical, the officers had not committed a technical trespass by merely recording conversations within the four corners of the defendant's home.[193]

There are numerous examples, however, where the trespass doctrine shielded citizens from surveillance. For example, an unconstitutional search occurs when the police use a drug-sniffing dog to gather sensitive information in curtilage—the land immediately surrounding and associated with the home.[194] The Court has similarly used the trespass doctrine to invalidate installation of a GPS tracking device onto the suspect's vehicle because it permitted surveillance of the vehicle while it was in private areas of the home, such as the garage.[195] Likewise, in *United States v. Jones*, the defendant's location was surreptitiously tracked when officers attached a beeper to his vehicle.[196] Officers used the beeper to track the defendant's movements for about a month.[197] Writing for a unanimous Court, Justice Scalia invalidated the surveillance because the officers physically intruded into the defendant's property by attaching the beeper to the vehicle.[198]

When the trespass doctrine applies, and especially in the context of the home, it is a nearly insurmountable barrier to government surveillance.[199] Unfortunately, the logic of physical intrusion falls apart in tough cases like digital eavesdropping and ShotSpotter surveillance because the trespass doctrine is rooted in property law. The property law approach to sound

191. *See* 277 U.S. 438, 455-57 (1928).
192. *Id.* at 457.
193. *See id.* at 468.
194. Florida v. Jardines, 569 U.S. 1, 5-6 (2013).
195. United States v. Knotts, 460 U.S. 276, 281-82 (1983).
196. 565 U.S. 400, 402 (2012).
197. *Id.* at 403.
198. *Id.* at 410.
199. Kyllo v. United States, 533 U.S. 27, 31 (2001) (stating that "the right of a man to retreat into his own home and there be free from unreasonable government intrusion" is sacrosanct).

waves and particulate intrusions is a legally cognizable claim typically sounding in nuisance rather than trespass.[200] As Justice Sotomayor explained, the trespass doctrine is simply "ill suited to the digital age," and though it makes easy cases easy, the test is not apt for thwarting ShotSpotter.[201]

2. Katz*: Hollow Promises of the Reasonable Expectation of Privacy Test*

Desiring a more workable and flexible test, Justice Harlan crafted the famous Reasonable Expectation of Privacy test in *Katz v. United States*.[202] It is not a strictly formalistic test, but it has two prongs that need to be satisfied before the Court will find an impermissible search.[203] The first prong is whether the individual, by his conduct, "exhibited an actual (subjective) expectation of privacy."[204] This prong includes whether an individual has shown that "he seeks to preserve [something] as private."[205] The second prong is whether an individual's expectation of privacy is "one that society is prepared to recognize as 'reasonable.'"[206] Often the first prong is easy to satisfy, but privacy interests are won and lost on the Court's analysis of the second prong. On balance, the *Katz* test expands the protection afforded by the Fourth Amendment because, as the majority famously asserted, the Fourth Amendment "protects people, not places."[207]

In *Katz*, government agents, acting without a warrant, attached an electronic eavesdropping device to the outside of a glass telephone booth to record incriminating conversations while the defendant was inside the booth.[208] Justice Stewart explained that the defendant demonstrated a reasonable expectation of privacy in the contents of his communications

200. *See* Dobbs v. Wiggins, 929 N.E.2d. 30, 38-39 (Ill. App. Ct. 2010) (holding that barking dogs are a nuisance if the aggrieved party can demonstrate an invasion of the right to quiet use and enjoyment of the land); Johnson v. Paynesville Farmers Union Coop. Oil Co., 817 N.W.2d 693, 700-01 (Minn. 2012) (holding that particulate matter such as pesticides is not a trespass when it blows in the wind and damages nearby crops).

201. *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

202. *See* 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

203. *Id.* at 361 (Harlan, J., concurring).

204. *Id.*

205. *Id.* at 351 (majority opinion).

206. *Id.* at 361 (Harlan, J., concurring).

207. *Id.* at 351 (majority opinion).

208. *Id.* at 348.

because he entered the phone booth and shut the door not to keep out "the intruding eye," but "the uninvited ear."[209]

Additionally, the Court explained that the expectation of privacy was one that society was prepared to accept as reasonable because a person using a phone booth can take comfort in knowing that "the words he utters into the mouthpiece will not be broadcasted to the world."[210] Thus, although the phone booth was on a public sidewalk, it became a "temporarily private place whose momentary occupants' expectation of freedom from intrusion" was one society was prepared to recognize as reasonable.[211]

Although the *Katz* framework expanded the Fourth Amendment in beneficial ways, it also led to the Third-Party Doctrine. The central rule for cases involving the Third-Party Doctrine is that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[212] In addition, the Court has explained that when a person voluntarily conveys information to a third party, he assumes the risk that the information may be divulged to the police or exposed to the public.[213]

For example, in *California v. Greenwood*, police officers asked a local trash collector to pick up the respondent's trash bags from the curb and to turn them over to the police for investigation.[214] Officers "searched through the rubbish" and found evidence related to the use of narcotics.[215] The Court ruled that, even though an opaque trash bag may contain evidence of the intimate activities associated with the sanctity of a man's home, a search had not occurred because it is common knowledge that trash bags left on a curb are easily accessible to animals, children, strangers, scavengers, snoops, and any member of the general public.[216]

Similarly, in *United States v. White*, officers used a wired informant to record conversations within a restaurant, a car, and inside a home with a suspect believed to be dealing narcotics.[217] Like *Greenwood*, the Court reasoned the defendant had voluntarily conveyed information to a third party with no guarantee that the third party would not disclose the information from the conversation to the police or anybody else.[218]

209. *Id.* at 352.
210. *Id.*
211. *Id.* at 361 (Harlan, J., concurring).
212. Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
213. *Id.* at 744.
214. 486 U.S. 35, 37 (1988).
215. *Id.* at 37-38.
216. *Id.* at 40.
217. 401 U.S. 745, 747 (1971).
218. *Id.* at 749.

Recognizing the benefits of capturing the verbatim dialogue of an incriminating conversation via a recording, the Court stated the simultaneous third-party recording and transmission of face-to-face conversations between the defendant and the informant was not a search within the meaning of the Fourth Amendment.[219] The Court found no "justifiable and constitutionally protected expectation" of privacy in the conversations that a person may later reveal to the police.[220] The logic was fundamentally rooted in a tort-based assumption of risk policy. According to the majority in *White*, if someone "sufficiently doubts [the] trustworthiness" of a companion, then he bears the risk that his disclosures will later be shared with law enforcement.[221] Otherwise "if he has no doubts, or allays them, or risks what doubt he has, the risk is his."[222]

The assumption of risk argument is dubious, however, for two reasons. First, it fundamentally misunderstands the Fourth Amendment. Returning to the Amendment's text, it was intended to protect "the right of *the people* to be secure in their persons . . . against unreasonable searches" performed by *the government*.[223] It does not protect the people against unreasonable searches conducted by their civilian counterparts.[224] In fact, such a construction would violate the state action doctrine, which clarifies that the Constitution does not apply to private entities or actors.[225] Thus, the Reasonable Expectation of Privacy test must be abandoned as a tool to thwart persistent surveillance technology like ShotSpotter. To take aim at technologies like ShotSpotter, the Court must fortify the Fourth Amendment as a shield against unreasonable *governmental* intrusions, rather than societal expectations. After all, "[w]hen all the might of the leviathan is turned on a person" when the state pursues a criminal prosecution, it is unrestrained sovereign police powers we fear, not our neighbors.[226]

Second, the assumption of the risk argument is impractical in the modern digital world, which the dissenting Justices in *Smith v. Maryland* predicted. Justice Marshall, joined by Justice Brennan, argued that a person

219. *See id.* at 751.
220. *Id.* at 749.
221. *Id.* at 752.
222. *Id.*
223. U.S. CONST. amend. IV.
224. *See* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW 532 (6th ed. 2020) ("Private conduct generally does not have to comply with the Constitution.").
225. *Id.* at 532-36.
226. NEIL GORSUCH, A REPUBLIC, IF YOU CAN KEEP IT 183 (2019).

"cannot help but accept the risk of surveillance" unless he is prepared to "forgo use of what for many has become a personal or professional necessity."[227] Today, with ShotSpotter sensors installed in unknown locations and surreptitiously recording at all times, the Reasonable Expectation of Privacy framework dictates that we accept the risk when we produce a loud concussive noise that is recorded by the device.

The *Katz* test was doomed from the start. Whether a privacy expectation qualifies as reasonable is unpredictable.[228] Even worse, it invites the Justices to inject their own subjective preferences into the equation.[229] Furthermore *Katz* led to the Third-Party Doctrine perversion and the assumption of risk logic that is ill-fitting when applied to modern surveillance technology like ShotSpotter.[230] Compared to 1967, when *Katz* was decided, intrusive technology is far more prominent in everyday life. Today, people regularly use apps to post photos of the interior of their homes; use watches and apps to record sensitive health data; rely on digital calendars that tell exactly when and where we will be at any given time; and share location data on social media. The list is nearly endless of everyday occurrences where a person has unknowingly forfeited their reasonable expectation of privacy by making intimate details more accessible.

Thus, even if an individual has an objective expectation of privacy in the sounds they produce on a public sidewalk, it is practically impossible to conclude that they have a subjective expectation of privacy that society is prepared to accept. After all, individuals assume the risk when they produce loud concussive noises outside. Without a reasonable expectation of privacy, the onus to achieve security in the sounds people produce falls upon the sound producer. In other words, no matter how sophisticated government surveillance becomes, it is the sound producer's responsibility to build thicker walls, mute or muffle sounds, and become a recluse because the only security absolutely guaranteed by *Katz* is privacy in the home.

Finally, *Katz* famously promised to use the Fourth Amendment as a shield that "protects people, not places."[231] Yet time and again, the Court's analysis is infected by an emphasis on locations rather than a bubble of security that follows people wherever they venture. In the context of ShotSpotter, the failure to defend "persons, not places" is painfully

227. Smith v. Maryland, 442 U.S. 735, 749-50 (1979) (Marshall, J., dissenting).
228. *See* Carpenter v. United States, 585 U.S. 296, 394 (2018) (Gorsuch, J., dissenting).
229. *Id.*
230. *Id.* at 394-96.
231. Katz v. United States, 389 U.S. 347, 351 (1967).

evident.[232] Sounds produced inside garner stronger protections. Whereas sounds produced in public places, even if produced in empty spaces, warrant weaker protections. In conclusion, the "persons, not places" phrase has become a hollow promise negatively shaping the ability to use the Fourth Amendment to protect the sounds we produce.

3. Kyllo*: A Technology Framework with a Built-In Expiration Date*

In assessing whether a search has occurred, the Court may consider the impact of sense-enhancing technologies. As Justice Scalia articulated in *Kyllo*, it would be "foolish" to pretend that the degree of privacy afforded to citizens by the Fourth Amendment has not been dramatically impacted by technological advancements.[233] Over the last few decades, the Court has grappled with a variety of devices including thermal-imaging devices,[234] beepers,[235] aerial surveillance,[236] pen registers,[237] and drug-sniffing dogs.[238] Each device presents unique issues for the Court to address, but the rule is clear: a search occurs when officers obtain information about the interior of the home with the use of "sense-enhancing technology" that is "not in general public use."[239] Once the technology is in general public use, however, this test is no longer applicable. Thus, the test has a built-in expiration date.

In *Kyllo*, the defendant was growing marijuana inside his garage, and officers used a thermal imaging device to scan the heat emanating from the lights used to stimulate growth of the marijuana plants.[240] A technical trespass had not occurred because the police pointed the thermal imaging device at the garage while they were seated in a cruiser parked across the street.[241] Justice Scalia, however, was determined to craft a test that would continue the Court's longstanding preservation of the sanctity of the

232. *See* Jasmine E. McNealy, *Sonic Privacy*, 24 YALE J. L. & TECH. 365, 371-72 (2022) (discussing the public versus private dichotomy and correlating degrees of privacy expectations in each space).

233. Kyllo v. United States, 533 U.S. 27, 33 (2001).

234. *See id.* at 29.

235. *See* United States v. Knotts, 460 U.S. 276 (1983); United States v. Jones, 565 U.S. 400 (2012).

236. *See* California v. Ciraolo, 476 U.S. 207 (1986).

237. *See* Smith v. Maryland, 442 U.S. 735 (1979).

238. *See* Florida v. Jardines, 569 U.S. 1 (2013); Rodriguez v. United States, 575 U.S. 348 (2015).

239. Kyllo v. United States, 533 U.S. 27, 34-35 (2001).

240. *Id.*

241. *Id.*

home.[242] *Kyllo* was a self-proclaimed effort to take the long view by adopting a rule that would "take account of more sophisticated systems that are already in use or in development."[243]

Kyllo is perhaps an obvious starting point for analyzing ShotSpotter under the Fourth Amendment because ShotSpotter is a novel technology, used to enhance an officer's auditory senses, and is not currently in the general public use. However, the self-inflicted expiration date built into the *Kyllo* test is a major drawback because AGDS will soon become part of the general public use.

First, AGDS like ShotSpotter are a potentially powerful tool in a city's holistic crime prevention strategy, particularly as the barriers to entry diminish over time. Although the ShotSpotter price tag has historically served as a barrier, cities embracing the Smart City Movement may soon set their sights on acquiring the technology.[244] For example, a city outfitted with fully integrated technology such as GE's smart streetlights—a technology that can likely be implemented with less political pushback—will experience a windfall because it is easy to incorporate ShotSpotter sensors by tacking them onto existing smart infrastructure.[245] Consequently, "entire cities" can be blanketed with sensors instead of "just focusing on problem neighborhoods."[246]

Second, typical AGDS rely on a series of sensors designed for mounting on light poles or rooftops,[247] but there are also market participants that supply vehicle-mounted or hand-held portable systems.[248] As these methods continue to gain traction—perhaps for parents who want to include portable AGDS in their child's school backpack—the technology moves

242. *Id.* at 37.

243. *Id.* at 36.

244. *See, e.g.*, Van Fisher, *The Baltimore County Police Department's New Tool, 'ShotSpotter,' Has a History of Mixed Results*, PERRY HALL PATCH (Perry Hall, Md.) (July 18, 2023, 7:01 PM), https://perma.cc/98RW-JCQ8 ("The Baltimore City Police Department renewed its contract with ShotSpotter in 2021 following lengthy debates about whether it was worth the $760,000 price tag."); *Smart, Safe Cities: GE's Smart Streetlights to Include Gunshot Detection*, KOVA CORP, https://www.kovacorp.com/smart-safe-cities-ges-smart-streetlights-to-include-gunshot-detection (last visited Mar. 1, 2024).

245. *Smart, Safe Cities: GE's Smart Streetlights to Include Gunshot Detection*, *supra* note 244.

246. *Id.*

247. Guariglia, *supra* note 82.

248. *Gunshot Detection System Market*, STRAITS RSCH., https://straitsresearch.com/report/gunshot-detection-system-market (last visited Mar. 1, 2024).

closer into the general public use and therefore falls within the *Kyllo* expiration date.

For example, a Tulsa, Oklahoma, company boasted success in developing an AGDS that has a "wrist display the size of a cell phone tethered . . . to a powerful shoulder-worn data unit [a] little bigger than a bar of soap."[249] For the Tulsa company, the portable AGDS are successful in military operations because they triangulate the location of enemy gunfire and relay that information "all within half a second."[250] Not only are some devices portable, but they are perhaps becoming permanent attachments on guns themselves in "the fourth line of emerging firearm technology."[251] This era of interactive smart guns includes "live streaming the view from the gun's scope, or by tracking discharges . . . through online blockchain ledgers" and "automated recording, memorializing, and archiving events for subsequent replay."[252] Whether portable or attached to the gun itself, AGDS will likely continue to become more accessible for general public use.

Finally, market saturation is yet another way that the technology can quickly enter general public use. As the number of market participants increases, for example, there may be a decline in the costs associated with using the technology. Currently the market for both indoor and outdoor AGDS is global and growing—particularly in countries facing mounting social and political pressures to thwart mass shootings.[253] ShotSpotter is a trailblazer,[254] but other market participants include Sentri, Boomerang, Databuoy, and Shooter Detection, LLC.[255] As a small sample of the global market, AGDS providers in France include ACOEM, CILAS, and Thales

249. Kirby Lee Davis, *Tulsa Startup Targets Huge Niche with Gunshot Detection System*, J. REC. (Okla. City) (Aug. 17, 2010), https://journalrecord.com/2010/08/17/tulsa-startup-targets-huge-niche-with-gunshot-detection-system-general-news/.

250. *Id.*

251. Dru Stevenson, *Smart Guns, the Law, and the Second Amendment*, 124 PENN ST. L. REV. 691, 693 (2020).

252. *Id.* (noting that these devices offer bilateral accountability). That is, accountability for officers shooting unarmed suspects and as an authentication check in self-defense claims. *Id.* Stevenson likens this technology to the "black boxes" already inside cars that constantly record speed, acceleration, braking, and turns. *Id.* at 696.

253. *Gunshot Detection System Market*, *supra* note 248 ("Gunshot Detection System Market size is expected to reach USD 2160 million by 2030 . . . .").

254. *See* Angrej Singh, *Evaluating the Growing Movement to Stop ShotSpotter*, TECH POL'Y PRESS (Oct. 5, 2022), https://techpolicy.press/evaluating-the-growing-movement-to-stop-shotspotter/; Gecas, *supra* note 6, at 1078.

255. Gecas, *supra* note 6, at 1081; *Gunshot Detection System Market*, *supra* note 248.

Group.[256] As market competition continues to grow, it is more likely that AGDS will trigger *Kyllo's* "general public use" expiration date.

In conclusion, even if *Kyllo* is currently a fitting test, it is questionable how long that framework will continue to shield citizens from uninvited and undesirable surveillance from surreptitious recording devices like ShotSpotter.

4. Carpenter*: An Incomplete Cure*

The legal landscape changed dramatically, however, in 2018. *Carpenter v. United States* was a constitutional thunderbolt issued in response to Cell-site Location Information ("CSLI"). Despite the dictates from *Katz* and its progeny that data voluntarily disclosed to third parties is not shielded, the Court held that law enforcement officers must seek a warrant before downloading historical cell site information from a cell phone.[257] Cell-cite location data, similar to AGDS, functions by pinging various cell towers and then using those signals to triangulate the phone's location.[258] In *Carpenter*, the police suspected the defendant had participated in a robbery and used his phone's location data to place him at the scene of the crime.[259] In fact, the "location records clinched the case" for the prosecution.[260]

Even though the data was voluntarily conveyed to a third-party, the Court rejected the stilted Third-Party Doctrine analysis because the data collected from a phone is "detailed, encyclopedic, and effortlessly compiled."[261] In abandoning the Third-Party Doctrine, the *Carpenter* Court also described phones as a "feature of human anatomy" that "faithfully follows its owner" throughout the day.[262] Phones contain a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[263] Like the dissenting Justices pointed out in the original Third-Party Doctrine cases, the majority also acknowledged that sharing such data is inescapable.[264] Furthermore, the Court returned to the promise in *Katz* that the Fourth Amendment "protects people, not

256. *Gunshot Detection System Market*, *supra* note 248.
257. *See* Carpenter v. United States, 585 U.S. 296, 320 (2018).
258. *Id.* at 297-98.
259. *Id.* at 306.
260. *Id.* at 303.
261. *Id.* at 309.
262. *Id.* at 311 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).
263. *Id.* at 315.
264. *Id.*

places." As the majority described, Fourth Amendment protections are not shed merely by stepping into the public sphere.[265]

The majority opinion in *Carpenter* drew four separate dissents. The first was a coalition comprised of Justices Kennedy, Thomas, and Alito. This cohort believed that the cases establishing the Third-Party Doctrine should have resolved the case.[266] Regardless of how unsavory the Third-Party Doctrine is for modern applications, they argued it is prudential to apply the existing precedent.[267] The second dissenting opinion was issued by Justice Thomas.[268] He used the case as a platform to launch a fiery attack against the *Katz* Reasonable Expectation of Privacy test.[269] In his view, *Katz* is not rooted in the text of the Amendment.[270] Instead, the analysis should focus on "*whose* property was searched."[271] The cell-site records did not belong to the defendant because they were the property of the cell phone provider.[272] Under that logic, the Third-Party Doctrine would operate to foreclose any privacy interests in the data voluntarily conveyed to the cell phone provider.[273] The third dissenting opinion was issued by Justice Alito and joined by Justice Thomas. Justice Alito echoed Justice Thomas' concerns about how the cell-site records did not belong to the defendant but added that the Court should have reinforced the government's power to subpoena documents.[274] Finally, Justice Gorsuch's dissent proposed a new theory rooted in property law and bailments.[275]

Out of all four Search doctrines, *Carpenter* provides the strongest argument to take aim at ShotSpotter. Undoubtedly, ShotSpotter—particularly when operated in tandem with the entire SafetySmart platform—produces exactly the kind of "detailed, encyclopedic, and effortlessly compiled" data that concerned the Court in *Carpenter*. But applying *Carpenter* to ShotSpotter is an imperfect solution for three reasons.

---

265. *Id.*
266. *See id.* at 321-23 (Kennedy, J., dissenting).
267. *Id.*
268. *See id.* at 342-61 (Thomas, J., dissenting).
269. *Id.* at 343.
270. *Id.*
271. *Id.* at 342.
272. *Id.*
273. *Id.*
274. *Id.* at 363-64, 374 (Alito, J., dissenting).
275. *See id.* at 399-402 (Gorsuch, J., dissenting).

First, *Carpenter* was a self-proclaimed "narrow" rule meant to apply to only "the record of . . . physical movements as captured through CSLI."[276] Second, *Carpenter* is not applicable to obtaining cell-site location records in real time.[277] ShotSpotter, however, is regularly advertised as a tool that provides officers with real-time data. All three components of ShotSpotter's review of a concussive noise—hardware, software, and humanware—occur in approximately one minute.[278] And officers receive a push notification that allows them to arrive on scene in a matter of minutes.[279] Furthermore, SoundThinking claims that it does not store ShotSpotter data in perpetuity.[280] Unlike the CSLI data collected by the phone companies in *Carpenter*, SoundThinking stores the data for hours or days, but not weeks.[281] Finally, Carpenter does not apply to privacy invasions that result from national security or an "urgent situation."[282]

IV. An Argument for Sonic Security

We produce sounds. Sonic footprints are an inescapable feature of the human condition, physics, and societal interactions. But it was not until recently that our sounds have been subjected to memorialization through surreptitious government surveillance. Casually overhearing a conversation is one thing, but technology like ShotSpotter "allows listeners to hear more than they could with the natural ear" and to store it in a memory device not nearly as evanescent as the human mind.[283] Furthermore, with the advent of always-listening voice assistants like Alexa, Cortana, and Siri, "the opportunities for businesses to eavesdrop on consumers have soared."[284] In response to COVID-19, for example, scientists were motivated to develop technology that could analyze the sounds produced by a cough to render a diagnosis.[285]

Some of these advancements represent extraordinary leaps in technology and medicine, but in the wrong hands they all have the potential for abuse.

---

276. *Id.*
277. *Id.* at 316 (majority opinion).
278. Busljeta, *supra* note 12, at 213.
279. *See supra* notes 155-57 and accompanying text.
280. Busljeta, *supra* note 12, at 215.
281. *Id.*
282. *Carpenter*, 585 U.S. at 320.
283. McNealy, *supra* note 232, at 379.
284. Dacia Green, *Big Brother Is Listening to You: Digital Eavesdropping in the Advertising Industry*, 16 DUKE L. & TECH. REV. 352, 356-57 (2018).
285. McNealy, *supra* note 232, at 367.

As more cities invest in the Smart City Paradigm, where everything from streetlights to trash cans are connected through a network of arterial circuitry, the potential for abuse skyrockets.[286] Scholars across varied backgrounds agree that "the perception of being watched changes how people act."[287] Jeremy Bentham's famous depiction of the Panopticon, for example, illustrates how the human psyche reacts to the mere *potential* for persistent surveillance.[288] Without Sonic Security, people are deprived of "agency, status, and relationships" that are central to claims of "personhood, dignity, and entitlement."[289] When robbed of the ability to produce sound due to a fear of punishment, we are fundamentally robbed of the ability to define ourselves.[290]

The project to safeguard Sonic Security must begin with the constitutional text. The Fourth Amendment begins with a two-word phrase "The right," which, when relying on authoritative sources from the founding era, "probably meant to readers in 1791 something quite close to what it means to readers today."[291] It is "a reference to and enshrinement of fundamental natural or political rights" deriving from John Locke.[292] The Amendment proceeds next to "The right of the people to be secure in their persons."[293] "'Secure' too had a familiar meaning: 'Free from fear [or] danger.'"[294] David Gray, a renowned Fourth Amendment scholar, concludes that this introductory phrase to the Amendment "guarantees a collective right of the people to live in a state or condition characterized by freedom from fear or danger against some manner of threat to themselves."[295]

However, the Amendment does not shield *all* searches, only *unreasonable* searches.[296] In determining the reasonableness of a search, the Court has "balanced the intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental

286. *See Smart, Safe Cities: GE's Smart Streetlights to Include Gunshot Detection*, *supra* note 244.

287. McNealy, *supra* note 232, at 369.

288. *See* DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 8 (2017).

289. *Id.* at 7.

290. *Id.*

291. *Id.* at 144.

292. *Id.* at 146.

293. U.S. CONST. amend. IV.

294. GRAY, *supra* note 288, at 157.

295. *Id.*

296. U.S. CONST. amend. IV (emphasis added).

interests."[297] It is undisputable that the United States is plagued by gun violence and the nation has a tantamount interest in eradicating it.[298] To that end, ShotSpotter is a powerful and promising tool. Yet the weight bearing on the other side of the scale—an intrusion against Sonic Security—is not slight. Unfettered use of ShotSpotter to surreptitiously record day-to-day conduct exposes citizens to daily losses in the right to be secure in our persons. And that burden of losing Sonic Security is not limited to criminals suspected of "suspicious" activity.[299]

Despite the Fourth Amendment's textual promise to protect the "right of the people to be secure in their persons," no adequate safeguard exists for Sonic Security.[300] Section II(A) concludes that the stop and frisk framework is an inadequate safeguard for Sonic Security because the reasonable suspicion quantum is rigged against civilians. Section II(B) argues that the existing search and seizure frameworks fail to adequately safeguard Sonic Security against pervasive surveillance techniques like ShotSpotter. Because the right to control the sounds we produce is intimately associated with autonomy and the freedom to be left alone, this Part argues that Sonic Security is a right protected by the Fourth Amendment. This analysis focuses on originalist and historical justifications, existing positive law at both the state and federal levels, and economic and sociocultural justifications as applied directly to ShotSpotter.

A. Positive Law Indicates a Preference for Sonic Security, but the Current Landscape Is Fragmentary and Underinclusive

In his rousing dissent in *Carpenter*, Justice Gorsuch delivered a cautionary message for those seeking to challenge surveillance techniques under the Fourth Amendment.[301] By failing to discuss "positive law rights," the litigant in *Carpenter* "forfeited perhaps his most promising line of argument."[302] When the record is bereft of positive law arguments, as Justice Gorsuch argues, courts resolve to "the usual *Katz* hand-waiving," which deprives litigants of the "development of a sound or fully protective

297. Maryland v. Buie, 494 U.S. 325, 331 (1990).

298. *See supra* Part I.

299. *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 465 (1990) (Stevens, J., dissenting) (addressing alcohol checkpoints) ("These fears are not . . . solely the lot of the guilty. . . . Unwanted attention from the local police need not be less discomforting simply because one's secrets are not the stuff of criminal prosecutions.").

300. U.S. CONST. amend. IV.

301. Carpenter v. United States, 585 U.S. 296, 406 (2018) (Gorsuch, J., dissenting).

302. *Id.*

Fourth Amendment jurisprudence."[303] State and federal legislatures have yet to address AGDS head on.[304] Consequently, the current body of positive law for Sonic Security is fragmentary and underinclusive. Nonetheless, this Comment provides a brief overview of the prominent federal and state eavesdropping and privacy statutes and argues that the patchwork of positive law protections warrants a stronger defense of Sonic Security under the Fourth Amendment.

1. State and Federal Eavesdropping Statutes

In the United States, there are various federal and state statutes that regulate eavesdropping, or the act of surreptitiously listening to or recording the private communications of others. These laws are intended to protect individuals' privacy rights and to ensure that personal communications are not intercepted or recorded without the consent of all parties involved. While various statutes safeguard "individual data sets—such as health care information or student data," the United States lacks a holistic and comprehensive privacy law that "cuts across wide swaths of personal information."[305]

At the federal level, one of the more significant laws that regulates eavesdropping is the Electronic Communications Privacy Act ("ECPA") of 1986. The ECPA prohibits the unauthorized interception of electronic communications, including telephone conversations, emails, and text messages.[306] It also regulates the use and disclosure of communications that have been intercepted.[307] Another federal law that regulates eavesdropping is the Foreign Intelligence Surveillance Act ("FISA"), which was passed in 1978.[308] It provides a framework for the government to conduct surveillance on foreign intelligence targets within the United States, but it

303. *Id.*

304. Smriti Krishnan, Note, *Tiger by the Tail?: Navigating Modern Technologies and Privacy Interests*, 42 L. & PSYCH. REV. 103, 104 (2018) ("Notably, the parameters for law enforcement's information-gathering via technologies in some contexts are still being statutorily defined.").

305. Alex Alben, *Privacy, Freedom, and Technology—or "How Did We Get into This Mess?"*, 42 SEATTLE U. L. REV. 1043, 1045 (2019).

306. *See* Lindsey Barrett & Ilaria Liccardi, *Accidental Wiretaps: The Implications of False Positives by Always-Listening Devices for Privacy Law & Policy*, 74 OKLA. L. REV. 79, 93 (2022).

307. *Id.*

308. *See* Jeffrey S. Brand, *Eavesdropping on Our Founding Fathers: How a Return to the Republic's Core Democratic Values Can Help Us Resolve the Surveillance Crisis*, 6 HARV. NAT'L SEC. J. 1, 7 (2015).

also provides some protections for US citizens and legal residents.[309] Finally, Title III of the Omnibus Crime Control and Safe Streets Act is frequently cited as a defense to uninvited eavesdropping.[310]

At the state level, each state has its own eavesdropping laws. Some states have "two-party consent" laws, which require all parties involved in a communication to consent to its recording or interception.[311] Other states have "one-party consent" laws, which allow one party to a conversation to record or intercept it without the consent of the other party.[312] In general, companies that intercept, use, or disclose the contents of recorded communications without user consent likely violate laws in jurisdictions that apply the two-party consent requirement.[313]

It is unclear how the one-party or two-party consent rules would apply to ShotSpotter. Even if ShotSpotter is not live listening to private conversations, the contents of at least some communications could be recorded in the window before or after the percussive noise. Additionally, if there are several percussive noises in a row, ShotSpotter might capture full sentences or phrases that could implicate culpability in a criminal defendant's trial. At the very least, technology like ShotSpotter in the hands of an ordinary citizen would likely violate the two-party consent standard. This implies that at least some states are signaling a preference for Sonic Security in an age of pervasive and surreptitious recording.

Furthermore, a few states like Oklahoma and California have enacted additional statutes to provide Sonic Security for their respective citizens. Oklahoma crafted an Invasion of Privacy and Peeping Tom statute[314] and a legally cognizable cause of action sounding in private nuisance[315] to protect its citizens from the uninvited eavesdropper. Similarly, the California Consumer Protection Act ("CCPA") applies because ShotSpotter also records audio and memorializes the audio in a dataset.[316] To ensure compliance with the CCPA, ShotSpotter is required to disclose the

309. *Id.* at 10-12.

310. McNealy, *supra* note 232, at 376-78; Gecas, *supra* note 6, at 1096-97.

311. Barrett & Liccardi, *supra* note 306, at 94-95.

312. *Id.*

313. *Id.* at 81.

314. Jane Dunagin, Comment, *Incoming: Regulating Drones in Oklahoma*, 69 OKLA. L. REV. 457, 472-73 (2017).

315. *Id.* at 470-71.

316. *See* Robert L. Rembert, Comment, *TikTok, WeChat, and National Security: Toward a U.S. Data Privacy Framework*, 74 OKLA. L. REV. 463, 489-90 (2022) (arguing for privacy as a human right).

information it collects.[317] The company provides a table where it explains that it may collect information such as: names, email addresses, phone numbers, browsing history, search history, physical location or movements, and audio or similar information.[318] Most of that data is likely generated from website traffic, not from ShotSpotter sensors. But the "[a]udio or similar information" description is mysteriously vague.[319]

2. Clues from the Model Rules of Professional Conduct

The Model Rules of Professional Conduct ("MRPC") for the legal profession offer guidance for preserving confidentiality against an uninvited listener. With a few commonsense exceptions, Model Rule 1.6 dictates that lawyers have a duty of confidentiality to prospective, current, and former clients.[320] To comply with the rule, lawyers must "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to" confidential information.[321] The comments to the MRPC further elaborate that the reasonableness of a lawyer's efforts include factors such as "the sensitivity of the information, the likelihood of disclosure . . . [and] the cost [and difficulty] of employing additional safeguards."[322]

While the MRPC is not a mandatory source of authority for the layman, it is a potent analogue for how to evaluate Sonic Security. Curiously, as long as an attorney acts reasonably—for example, by shutting the door to keep out the uninvited ear—the onus is on the listener, not the speaker.[323] Thus, the mere fact that words must be uttered, or sounds must be produced, to advance the relationship is not necessarily sufficient to destroy Sonic Security in the attorney-client relationship.

In the context of ShotSpotter, it is sensible to place the onus on the listener because it is not reasonable to demand silence whenever civilians dare to venture from their home. It is unreasonable for civilians to carry the burden to inoculate themselves against persistent government surveillance. And it is neither reasonable, nor socially preferrable, to incentivize silencers, execution-style shootings, indoor violence, or any other perverse

317. *See ShotSpotter Community Privacy Protections*, SOUNDTHINKING, https://www.soundthinking.com/privacy-policy/ (last updated Apr. 10, 2023).

318. *Id.*

319. *Id.*

320. MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N 1995).

321. *Id.*

322. *Id.* r. 1.6 cmt. 18.

323. *Id.* r. 1.6 cmt. 19.

action a shooter might perform to minimize the acoustic footprint of a gunshot. Ultimately, although sonic security is a two-way street requiring the sound producer to take reasonable precautions, the onus should be on the listener when the sound-producer's burden exceeds reasonable measures.

State and federal statutes have attempted to address eavesdropping, but without comprehensive guidance tailored to modern surveillance techniques that are surreptitious, pervasive, and eternal, many kinds of audio are uncovered.[324] Consequently, "individuals often have the burden of maintaining their own privacy by withholding information or foregoing transactions that are otherwise conditions of everyday life."[325] In the context of ShotSpotter, this realization is shattering. Despite attempts to statutorily safeguard Sonic Security against eavesdropping and surveillance, civilians are ultimately straddled with the responsibility to mute themselves or muffle their innocuous, albeit percussive, noises that may attract undesired attention from the local ShotSpotter sensors.

B. Even if ShotSpotter Survives Constitutional and Statutory Scrutiny, It Is Not a Defensible Tool for Policing Gunfire

ShotSpotter is an ideal catalyst for legislators and judges to revisit Sonic Security because it is not a defensible tool for policing gunfire. From a sociocultural and pragmatic perspective, ShotSpotter is defective for four principal reasons. First, it's not clear that ShotSpotter substantially deters crime. Second, although it can promote accountability, it is frequently criticized for a lack of transparency. Third, reports indicate that ShotSpotter may be engaged in endeavors to falsify efficacy. Finally, ShotSpotter has been criticized for leading to the disproportionate over-policing of African American and Latino neighborhoods.

First, the impetus behind the creation of ShotSpotter was to deter crime[326] and minimize the "collateral costs of gun violence."[327] Although the exact location of the sensors remains unknown to prevent vandalism, the deterrent effect is triggered by a "common-knowledge effect."[328] In theory, when criminals suspect their actions are being recorded, they are

---

324. *See* Thomas P. Crocker, *Ubiquitous Privacy*, 66 OKLA. L. REV. 791, 793 (2014).

325. *Id.*

326. Mares & Blackburn, *supra* note 17, at 195.

327. ShotSpotter's CEO used the phrase "collateral costs" to describe the larger impact gun violence has on the social psyche. *See* Drange, *supra* note 18. For example, a child who goes to bed fearing gun violence is a collateral cost. *Id.*; Gecas, *supra* note 6, at 1083.

328. *Id.*

"more likely to abstain from shooting."[329] However, the deterrent effect is premised on the assumption that "the technology is advertised or at least visible."[330] Unlike surveillance cameras, the fact that ShotSpotter sensors are "inconspicuous and secured high above street level" likely does little to deter crime.[331] One study of St. Louis, for example, concluded ShotSpotter had little deterrent impact on gun-related crime and did not "provide consistent reductions in police response time, nor aid substantially in producing actionable results."[332]

Furthermore, it is unclear what *exactly* the technology deters. If a criminal suspect knows they are being recorded *outside*, they might resort instead to firing guns *inside* where closed quarters may improve the lethality of their aim. Or, because the company has admitted the sensors have a hard time recording "execution-style" shootings, perhaps outdoor shootings will continue to happen but only in close range.[333] Another alternative is that firearm owners will engage in a type of "privacy protest" by investing in suppressors and other silencing toolkits.[334] And, even if the technology does deter crime, the National Rifle Association and other gun rights advocates would likely argue AGDS, like smart guns, "would do little to address adult suicide—the leading cause of firearm death."[335] If heightened surveillance is supposed to deter crime, then ShotSpotter seems at best reactive, rather than preventative.[336] Rather than increasing officer presence via routine patrols, AGDS "increase[s] police presence *after* the offense occurs."[337]

Second, much like body-worn cameras, the fact that the audio data is memorialized provides a footing for officer and civilian accountability. Because the sensors are agnostic—they detect gunfire regardless of who fired—the accountability argument applies equally to officers and civilians. A memorialized recording of the location, number of shots fired, and time elapsed between shots all contribute towards painting a better-informed image of how the events transpired. Thus, an officer faced with accusations

329. *Id.*

330. Mares & Blackburn, *supra* note 17, at 195.

331. *Id.* at 196.

332. *Id.* at 207.

333. Gecas, *supra* note 6, at 1085-86.

334. *See* Elizabeth E. Joh, *Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion*, 55 ARIZ. L. REV. 997, 1009-10 (2013).

335. Stevenson, *supra* note 251, at 709.

336. Mares & Blackburn, *supra* note 17, at 207; Bhuiyan, *supra* note 20 ("ShotSpotter specifically works to detect shots after they happen, it doesn't stop the shots from going off.").

337. Mares & Blackburn, *supra* note 17, at 207.

of using unnecessary force or a civilian mounting a self-defense claim can benefit from a digital record that supports their case.[338] At least one author, however, is fearful that "an *ex-ante* belief that it will be easier to show the legitimacy of a shooting . . . can subconsciously make [firearm] owners less hesitant or more likely to take a questionable shot."[339]

Furthermore, even if ShotSpotter promotes accountability, it has been criticized for lacking transparency. ShotSpotter has "a veneer of objectivity," but it is shrouded in layers of secrecy that renders the tool an investigative black box in courtroom proceedings.[340] For criminal defendants and judges, the lack of transparency is problematic because it deprives criminal defendants of "an opportunity to challenge" the reliability of the system as required by the Supreme Court in *Florida v. Harris*.[341] Although the company promises it is not lurking in the shadows live listening to conversations, the sensors did detect a portion of a street argument between Jonathan Flores and Jason Denison.[342] And in at least two cases, prosecutors have sought to introduce audio of voices recorded by ShotSpotter.[343] Despite its prolific adoption in major metropolitan cities across the country, "there remains little external validation of ShotSpotter from researchers or government agencies."[344]

Third, ShotSpotter produces an astonishing number of dead-end alerts, and recent scholarship suggests that the company alters the data to artificially improve accuracy ratings. The Chicago Office of Inspector General investigated ShotSpotter's efficacy over a span of eighteen months

338. Stevenson, *supra* note 251, at 733. "Justifire" is another product that can be used to collect real-time firearm data "for civilian gun owners who plan to use their guns to kill in self-defense and worry that they will face criminal charges afterward." *Id.* at 734.

339. *Id.* at 733.

340. Press Release, MacArthur Just. Ctr., *supra* note 105 (quoting Jonathan Manes, attorney).

341. 568 U.S. 237, 247 (2013) ("A defendant . . . must have an opportunity to challenge such evidence of a dog's reliability, whether by cross-examining the testifying officer or by introducing his own fact or expert witnesses.").

342. *See* Erica Goode, *Shots Heard, Pinpointed, and Argued Over*, N.Y. TIMES (May 28, 2022), https://www.nytimes.com/2012/05/29/us/shots-heard-pinpointed-and-argued-over.html.

343. At least one court admitted the audio into evidence. *See* People v. Johnson, No. A131317, 2013 WL 740387, at *4 (Cal. Ct. App. filed Feb. 27, 2013) ("The Shotspotter system captured the victim's voice referring to defendant by his nickname."). But another court refused to admit the evidence. *See* Commonwealth v. Denison, No. BRCR2012-0029 (Mass. Super. Ct. 2015) (refusing to admit ShotSpotter audio because it was a recording of "oral communication" that constituted an impermissible "interception" under the Massachusetts Wiretap Act).

344. Drange, *supra* note 18.

and found that for more than 50,000 alerts, only 9.1% led to "evidence of a gun-related criminal offense."[345] A 2021 independent study by the MacArthur Justice Center corroborated the Chicago Inspector General when it concluded "the vast majority of alerts generated by the system turn up no evidence of gunfire or any gun-related crime."[346]

ShotSpotter technology has a higher rate of error in urban settings because "gunshot detection and locational accuracy are sensitive to the complexities of the built environment."[347] Furthermore, the "Detailed Forensic Reports" that ShotSpotter provides to prosecutors warns that ShotSpotter is less than 100% accurate due to interference from "buildings, topography, foliage, periods of increased traffic or construction noise, and other urban acoustic noises."[348]

In May 2020, ShotSpotter was listening during protests following George Floyd's murder.[349] The sensors detected percussive sounds at 11:46 PM and originally tagged the sound as a firework.[350] But after a 911 alert was issued, "a ShotSpotter analyst manually overrode the algorithms and 'reclassified' the sound as a gunshot."[351] This data, which was "dramatically transformed" during the human-based review, eventually became the centerpiece of the prosecution against Michael Williams.[352] Williams spent nearly one year behind bars until prosecutors were pressed to defend the ShotSpotter evidence in a Frye hearing[353] and chose instead to withdraw "all ShotSpotter evidence against Williams."[354]

---

345. FERGUSON & WITZBURG, *supra* note 89, at 1-2.

346. Singh, *supra* note 254.

347. Brief for Amici Curiae, *supra* note 81, at 16 (citing Aguilar, *supra* note 101, at 281-82).

348. *Detailed Forensic Report*, SHOTSPOTTER (Feb. 2, 2015), https://www.shotspotter.com/wp-content/uploads/2019/05/DFR-Example-.pdf (hypothetical example of such a report).

349. Feathers, *supra* note 27.

350. *Id.*

351. *Id.*

352. *Id.*

353. Garance Burke et al., *How AI-Powered Tech Landed Man in Jail with Scant Evidence*, AP NEWS (Mar. 5, 2022, 12:23 PM), https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220. The *Frye* test is used to determine whether scientific evidence is admissible. For background on the history and evolution of *Frye*, see Jill Lepore, *On Evidence: Proving* Frye *as a Matter of Law, Science, and History*, 124 YALE L. J. 1092 (2015).

354. Feathers, *supra* note 27.

Finally, recent public outcries to terminate reliance on ShotSpotter are rooted in fundamental concerns about where the technology is deployed.[355] For example, one longitudinal study of deployments in Missouri, Ohio, and Georgia discovered the sensors were placed "almost exclusively in majority Black and brown neighborhoods."[356] Furthermore, in Chicago, the "white enclaves in the north and northwest of the city have no sensors at all, despite Chicago police data that shows gun crime is spread throughout the city."[357]A substantial body of academic research has already adequately chronicled the pervasive societal harms that stem from disproportionate policing of minority neighborhoods.[358] Suffice it to say that leaving some communities completely unmonitored leads to skewed perceptions of law-abidingness and creates a self-reinforcing, prejudicial cycle of hyper-surveillance.

The bottom line is that legislators and judges should revisit whether ShotSpotter deserves the considerable immunity that it currently enjoys from both Constitutional and statutory scrutiny. On the whole, ShotSpotter's crime deterrence effects are questionable, it lacks transparency and reliability, and it is a tool that has been used to disproportionately police minority communities. Fortifying Sonic Security under the Fourth Amendment is one potential pathway for taking aim at surveillance technologies like ShotSpotter.

V. Conclusion

Gun violence remains a persistent threat to the health, well-being, and sense of safety in the United States. Additionally, gun violence is so commonplace that many neighborhoods have ceased to report gunfire incidents.[359] ShotSpotter, an acoustic gunshot detection system, claims to

355. Singh, *supra* note 254 ("[A] growing national movement appears to be coalescing around calls to cancel ShotSpotter contracts.").

356. Todd Feathers, *Gunshot-Detecting Tech Is Summoning Armed Police to Black Neighborhoods*, VICE: MOTHERBOARD (July 19, 2021, 9:17 AM), https://www.vice.com/en/article/88nd3z/gunshot-detecting-tech-is-summoning-armed-police-to-black-neighborhoods.

357. Feathers, *supra* note 27.

358. Harvey Gee, *Reducing Gun Violence with ShotSpotter Gunshot Detection Technology and Community-Based Plans*, 100 OR. L. REV. 461, 469-83 (2022); Maclin, *supra* note 145, at 1275-76, 1285-87; Benjamin Goodman, Comment, *ShotSpotter–The New Tool to Degrade What is Left of the Fourth Amendment*, 54 UIC L. REV. 797, 820-21 (2021); Jordan Blair Woods, *Traffic Without Police*, 73 STAN. L. REV. 1471, 1515-25 (2021); *see* Khaled Ali Beydoun, *The New State of Surveillance: Societies of Subjugation*, 79 WASH. & LEE L. REV. 769 (2022).

359. *See supra* notes 17-18 and accompanying text.

decrease the gap between shots-fired and shots-reported. For almost three decades, the company has enjoyed nearly unchecked power to surreptitiously surveil citizens in more than 100 cities. Favoring efficiency over accuracy, ShotSpotter has become entrenched as the new tool to enforce law and order over unsuspecting pedestrians.

The existing machinery for redressing grievances against the use of ShotSpotter—assuming the aggrieved party is aware of its use in the first place—is haphazard, uneven, and inadequate. Under the stop and frisk framework, ShotSpotter enjoys substantial immunity from Fourth Amendment challenges because the reasonable suspicion quantum of proof is easily satisfied. Even if ShotSpotter is not as reliable as the company claims, officers brought to the scene of the crime via an alert can generally point to additional "suspicious" conduct that satisfies the reasonable suspicion requirement. As a gateway tool to a stop and frisk interaction, ShotSpotter is a loose cannon that erodes community trust, fosters a fear of chronic government surveillance, and disproportionately impacts minority communities classified as "high crime."

Current search and seizure jurisprudence results in similar outcomes. Since ShotSpotter is used to monitor soundwaves, the trespass doctrine is inapplicable. Under the *Katz* Reasonable Expectation of Privacy Test, sound producers have no expectation of privacy in the percussive noises that travel into the public domain. Consequently, the *Katz* framework results in a perverse universe where the sound producer must bear a hefty or otherwise distasteful burden of muting, muffling, or sequestering sounds to the only known location where security is assured—the home. As a novel technology, ShotSpotter may temporarily be challenged under *Kyllo,* but the test's built-in expiration date means that protection is temporary. Finally, although *Carpenter* peels back the reach of *Katz*, it is a self-proclaimed narrow ruling that will likely offer only limited protection of long-term sonic data collection.

In conclusion, the commands of the Fourth Amendment are rigorous. By its plain text, the amendment promises the right to be *secure* in our *persons*. It is impossible to enjoy the panoply of benefits afforded by the Fourth Amendment without a commensurate right to security in the sounds we inevitably produce in the routine unobserved realization of our identities. Whether the Fourth Amendment is leveraged as a sword for efficient gunshot surveillance or as a shield against pervasive surveillance will depend on whether the Court embraces Sonic Security. Certainly, it is vital that the law is vigorously administered so that criminals are discovered and

brought to justice. Yet "[p]anic is always a poor counselor"[360] and, in the long run, society has an overwhelming competing interest in the preservation of life free from the arbitrary interference of unreasonable governmental surveillance.

Emily A. Fogg

360. ALAN BARTH, THE PRICE OF LIBERTY 17 (1961) ("[Panic] can lead at times to a senseless sacrifice of the very values which it is the function of law enforcement to sustain and secure. If there is danger from the outcasts of society who violate the law, there is also danger from the law-abiding who, in an excess of anxiety, may jettison liberty for the sake of safety.").