Roderick & Solange
MacArthur
Justice
Center

Jonathan Manes
MacArthur Justice Center
160 East Grand Ave, 6th Floor
Chicago, Illinois 60611
O: (312) 503-0012
F: (312) 503-0891
E: jonathan.manes@macarthurjustice.org

www.macarthurjustice.org

November 21, 2022

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Ave., NW, Ste. CC-5610 (Annex B)
Washington, DC 20580

RE: Commercial Law Enforcement Surveillance Technologies
Commercial Surveillance ANPR, R111004

Dear Chairwoman Khan and Commissioners Phillips, Slaughter, Wilson, and Bedoya:

The MacArthur Justice Center ("MJC") submits this comment in response to the Commission's advance notice of proposed rulemaking ("ANPRM") regarding Commercial Surveillance and Data Security.

The Commission's ANPRM states a desire to address the ways in which Americans are surveilled in "the most basic aspects of modern life," including their "movements" and "faces."[1] We believe it is impossible to meaningfully pursue that goal unless the Commission's proposed rule and ultimate regulations encompass technologies created by private companies and sold to law enforcement. We accordingly urge the Commission to ensure that surveillance technologies sold to police, prisons, jails, and other law enforcement agencies are encompassed within the proposed and final rule.

This comment explains the regulatory void that the Commission can fill with respect to the law enforcement surveillance industry. We describe some of the harms that flow from the surveillance technologies that private companies are selling to law enforcement. We also propose specific regulatory interventions that the Commission could enact in this domain.

---

[1] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, 51273 (Aug. 22, 2022) https://www.govinfo.gov/content/pkg/FR-2022-08-22/pdf/2022-17752.pdf.

MJC is a national nonprofit civil rights organization that works primarily in the courts to seek justice for abuses in our criminal legal system and to redress the racial and social inequalities that flow from that system. This comment arises out of our work representing individual clients who have been abused by the criminal legal system as a result of commercial surveillance technologies used by police departments and other law enforcement agencies. The comment also draws upon our own independent research into certain technologies as well as the experience and information we have gathered through our work with organizers, grassroots advocates, public defenders, and other groups who advocate on behalf of people entangled in the criminal legal system.

The marketplace for law enforcement surveillance technologies is almost entirely unregulated, yet it profoundly affects how people are being treated by police, sheriffs, and other arms of the criminal legal system. We write to underscore that these surveillance products are fueling a variety of harms, particularly in communities of color, that range from false charges, illegal police stops, and unwarranted encounters with police, through to lost employment opportunities, disruptions to family life, and unwarranted reincarceration.

The Commission could do much to reduce those harms by enacting regulations targeting unfair and deceptive practices in this industry. Such regulations could help ameliorate structural problems in the market for law enforcement surveillance technology, which is currently plagued by secrecy, flawed products, and wildly irresponsible marketing claims.[2]

This comment proceeds in three parts. *First*, we briefly describe the range of commercial surveillance products currently on the market and explain why existing laws and institutions impose effectively no regulatory oversight with respect to the efficacy, reliability, use, and marketing of such products. *Second*, we illustrate some of the harms that can flow from the purchase and use of such unregulated technologies by focusing on two specific examples: acoustic gunshot detection technology (ShotSpotter) and location-tracking ankle monitors and similar electronic monitoring technologies. *Third*, we sketch regulatory interventions that

---

[2] The Commission has authority to regulate surveillance technology sold to law enforcement agencies even though many of the harms flow to members of the public rather than the government entities that typically contract for the technologies. The Commission has previously taken numerous enforcement actions against companies where their practices harmed members of the public with whom they did not directly do business. *See, e.g.*, FTC v. Accusearch Inc., 570 F.3d 1187 (10th Cir. 2009); FTC v. Neovi, Inc., 604 F.3d 1150 (9th Cir. 2010). Indeed, the Federal Trade Commission Act itself makes clear that the Commission's authority does not depend on a narrow understanding of consumer harm, but extends to any unfair or deceptive practices "in or affecting commerce." 45 U.S.C. § 15(a).

the Commission could consider that would reduce the unwarranted and harmful use of such technologies, reduce harms to civil rights and privacy when they are used, and permit more meaningful democratic control over the decision whether to purchase these profoundly consequential products in the first place.

1. **The private market for law enforcement surveillance technologies is vast and almost entirely unregulated.**

There are numerous private companies selling a wide variety of surveillance products to law enforcement agencies. These products include, for example, video surveillance devices; facial recognition software; ankle monitors that track location via GPS or radio frequency signals; ankle monitors that continuously measure blood alcohol concentration through the skin; acoustic sensors meant to detect and locate gunshots or other noises; vans equipped with X-Ray devices to scan inside buildings and cars; automated license plate readers to capture the location of cars; social media exploitation and analysis tools; and numerous software packages meant to forecast where certain types of crimes will occur or who will be involved in those crimes.

This is necessarily an incomplete list. Private companies are frequently devising new devices and products to sell to law enforcement. For instance, one prominent market player recently floated the idea of selling small surveillance drones equipped with taser electroshock weapons that could be deployed inside schools.[3]

Surveillance products sold to law enforcement operate in a regulatory void. There is no regular oversight or meaningful regulation of these devices and systems. This regulatory gap exists for several reasons.

First, private companies sell directly to thousands of individual police departments across the country. The fractured and decentralized patchwork of law enforcement agencies that buy and deploy these technologies means that uniform or consistent regulation will not exist without intervention from a higher level of government. Moreover, individual police departments are generally not equipped to independently audit or study such technologies and the marketing claims vendors make about them.

---

[3] *Press Release, Axon Announces TASER Drone Development to Address Mass Shootings,* AXON (June 2, 2022) https://investor.axon.com/2022-06-02-Axon-Announces-TASER-Drone-Development-to-Address-Mass-Shootings. After receiving broad public criticism of the idea, the company announced that it is "pausing work" on the taser drone product. Rick Smith, *Axon Committed to Listening and Learning So That We can Fulfill our Mission to Protect Life, Together*, AXON (June 5, 2022), https://www.axon.com/news/technology/axon-committed-to-listening-and-learning.

As far as we are aware, no state has an agency that regulates or has approval authority over police surveillance technology purchased at the local level. A small number of states have enacted targeted legal frameworks or restrictions on law enforcement's adoption of specific surveillance technologies—notably with respect to facial recognition technology.[4] But we are not aware of any state that has created a statewide legal or regulatory framework for law enforcement technologies more broadly.[5]

Second, the absence of meaningful regulation or oversight of this market is facilitated by the secrecy that shrouds many of the products sold to law enforcement. The purchase and deployment of such surveillance technologies by law enforcement is frequently invisible to the public. Indeed, new surveillance products can come into regular use by police before the public is even aware of their existence.[6]

Two examples illustrate the point. Police in numerous jurisdictions used cell-phone surveillance devices known as Stingrays or IMSI-catchers for years before their use finally came to light.[7] A coordinated effort to keep the technology in the shadows

---

[4] *See, e.g.*, Wash. Rev. Code Ann. §§ 43.386.010–901 (West 2022); Mass. Gen. Laws Ann. ch. 6, § 220 (West 2022); Cal. Penal Code § 832.19 (West 2022).

[5] Texas has established the Forensic Science Commission, which is tasked with investigating, regulating, and overseeing forensic disciplines and forensic laboratories relied upon in criminal proceedings. *See About Us,* TEXAS FORENSIC SCIENCE COMMISSION (last visited Nov. 20, 2022), https://www.txcourts.gov/fsc/about-us/. Its mandate is limited to assessing forensic methods and does not reach law enforcement surveillance technology more broadly.

A small number of municipalities have enacted local surveillance oversight ordinances that typically enact requirements for public notice and comment, official approval, and regular reporting with respect to the purchase of surveillance technologies. While these ordinances establish a measure of local oversight in a few specific municipalities, they are not equipped to serve as a regulatory check against unfair and deceptive practices in the surveillance industry more broadly. *See generally* Ari Chivukula, Tyler Takemoto, Catherine Crump & Juliana DeVries, *Local Surveillance Oversight Ordinances,* SAMUELSON LAW, TECHNOLOGY AND PUBLIC POLICY CLINIC (Feb. 2021), https://www.law.berkeley.edu/wp-content/uploads/2021/02/Local-Surveillance-Ordinances-White-Paper.pdf.

[6] Jonathan Manes, *Secrecy & Evasion in Police Surveillance Technology*, 34 BERKELEY TECH. L.J. 503, 507, 511–24 (2020), https://btlj.org/data/articles2019/34_2/03_Manes_Web.pdf.

[7] *Id.*; Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1 (2014), http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech1.pdf.

succeeded in preventing any external oversight of the law enforcement's use of the devices for years.

To take a more recent example, the Associated Press revealed only two months ago that police agencies across the country have for years been using a powerful cellphone location tracking tool marketed under the name "Fog Reveal."[8] According to the AP's reporting and records obtained by the Electronic Frontier Foundation, the system allows police to search billions of records from 250 million mobile devices by exploiting location data that is collected by mobile apps for the purpose of targeting ads to people based on their geography and movements. The product has been on the market since at least 2017 and yet its functions and (apparently) widespread adoption had, until the AP story, been almost completely unknown. The predictable consequence of such secrecy is that the technology evaded any meaningful regulation or oversight.

Remarkably, even the local elected officials that directly oversee local law enforcement agencies are sometimes kept in the dark about the surveillance tools that have been purchased and used by police.

For instance, in Chicago, the police department entered a contract to begin using Clearview AI's facial recognition software without any notice to the City's mayor or City Council.[9] The Mayor's Office only learned about the police's acquisition of the system after a New York Times exposé raised the public profile of the technology. This was not an isolated incident. For years, the Chicago Police Department evaded the city's budget process with respect to its purchase of surveillance technologies by buying equipment with money obtained through a civil asset forfeiture program controlled by the police itself.[10] Those off-the-books funds were used to purchase Stingray surveillance devices without any notice or oversight.[11] The New York Police Department has likewise purchased surveillance equipment, including facial

---

[8] Garance Burke & Jason Dearen, *Tech Tool Offers Police 'Mass Surveillance' on a Budget*, ASSOCIATED PRESS, Sep. 2, 2022, https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef.

[9] Tom Schuba, *Lightfoot's office was blindsided by CPD's use of controversial facial recognition software — then raised serious concerns*, CHICAGO SUN TIMES (May 20, 2021), https://chicago.suntimes.com/city-hall/2021/5/20/22444054/clearview-ai-facial-recognition-cpd-police-department-lori-lightfoots-privacy.

[10] Joel Handley, Jennifer Helsby & Freddy Martinez, *Inside the Chicago Police Department's secret budget*, CHICAGO READER, Sept. 29, 2016, https://chicagoreader.com/news-politics/inside-the-chicago-police-departments-secret-budget/.

[11] *Id.*

recognition software and mobile X-ray vans, using money from a special fund that was not subject to oversight from City Council or other municipal officials.[12]

Third, one might expect that surveillance technologies would be overseen by the courts and criminal legal process, particularly because of the close connection between such technologies and the investigations that lead to criminal prosecutions. However, courts fail to provide meaningful or effective oversight of police surveillance technologies. To be sure, case-by-case adjudication of challenges to police surveillance tools on behalf of individual criminal defendants is very important as a matter of due process and individual fairness, but it is an unreliable and structurally insufficient means of regulating and overseeing the market for police surveillance technologies.

Surveillance technologies typically come under judicial scrutiny in one of two ways. A criminal defendant may raise a Fourth Amendment suppression motion to challenge the lawfulness of the police's use of a technology or to question whether the technology is sufficiently reliable to be used as a basis for probable cause or reasonable suspicion. Alternatively, a criminal defendant might mount a *Daubert* or *Frye* challenge to the admissibility and scientific bona fides of trial evidence generated by a surveillance technology.

In practice, however, surveillance technologies frequently evade these forms of judicial oversight. Police and prosecutors often do not disclose the role that a surveillance product played in an investigation.[13] Even when there is notice to a criminal defendant, it is sometimes impossible for a defense attorney to obtain the information necessary about how a technology works (or doesn't work) in order to mount a robust challenge to its use or reliability.[14] Private surveillance companies can resist disclosure of key information about their products, for example invoking trade secrecy or other supposed privileges.[15] Criminal defense attorneys

---

[12] Sidney Fussell, *The NYPD Had a Secret Fund for Surveillance Tools,* WIRED, Aug. 10, 2021, https://www.wired.com/story/nypd-secret-fund-surveillance-tools/.

[13] Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 SANTA CLARA L. REV. 843 (2015), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2787&context=lawreview; *Dark Side: Secret Origins of Evidence in US Criminal Cases,* HUMAN RIGHTS WATCH, Jan. 9, 2018, https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases; Manes, *Secrecy & Evasion, supra* note 6.

[14] Manes, *Secrecy & Evasion, supra* note 6.

[15] Rebecca Wexler, *Life Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018) (discussing use of trade secrecy claims to prevent disclosure of information to criminal defendants), https://review.law.stanford.edu/wp-

representing individual clients are also often ill-equipped—both in terms of resources and expertise—to mount complex challenges to the use or reliability of surveillance technologies. Even if a defense attorney has the wherewithal to raise such a challenge, police and prosecutors can avoid a judicial determination simply by exercising their discretion to drop charges, drop evidence, or resolve the case with a favorable plea offer.[16] For all these reasons, judicial oversight of surveillance technologies is haphazard, uncertain, and frequently absent.

Even in the rare case where there is active judicial consideration of a criminal defendant's challenge to a surveillance technology, a single court's decision will often impose no meaningful constraints on the police's use of the same technology in other investigations or cases. Binding appellate authority regarding a specific surveillance method can take literally decades to develop.[17] By the time the courts manage to resolve important questions about a technology's lawful use or reliability—if they ever do at all—there may be decades of harm to the public.

As it stands, there is no agency or set of institutions—aside from the Commission—that can effectively regulate the market for law enforcement surveillance products in order to protect the interests of the public. For that reason, we urge the Commission to take up this issue and include the law enforcement surveillance industry within any rule that it seeks to enact.

2. The unregulated market for law enforcement surveillance products leads to a range of concrete harms.

The ANPRM asks for comment on ways that commercial surveillance can harm members of the public,[18] and members of the Commission have expressed particular interest in how such technologies can impair people's civil rights and "create

---

content/uploads/sites/3/2018/06/70-Stan.-L.-Rev.-1343.pdf; Manes, *Secrecy & Evasion, supra* note 6 at 552 (discussing application of law enforcement privilege to avoid disclosure of information about surveillance technologies).

[16] Manes, *supra* note 6; Soghoian & Pell *supra* note 7; Garance Burke et al., *How AI-powered tech landed man in jail with scant evidence*, ASSOCIATED PRESS, (March 5, 2022), https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220

[17] For example, police have for decades been acquiring and using cell-site location information to investigate people's movements over time. It was not until 2018 that the Supreme Court clarified, for the first time, that acquisition of such information by police is a Fourth Amendment search subject to the warrant requirement. *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

[18] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. at 51281.

discriminatory outcomes."[19] Members of the Commission have also encouraged the public to think broadly about such technologies affect people not just as "consumers" of products and services but more broadly as "workers, small business owner, and potential competitors to dominant firms."[20]

With that in mind, we describe here some of the harms to consumers from the purchase and use of police surveillance technologies and the data that those technologies generate and collect. We focus on two particular products: ShotSpotter noise detection technology and location-tracking ankle monitors and related technologies. These products have received perhaps less attention in the advocacy and policy communities than certain other surveillance tools, but they illustrate many of the concrete harms that can flow this unregulated industry. These technologies have resulted in false accusations of wrongdoing, unwarranted imprisonment, and loss of economic opportunities, in addition to privacy harms. There is also precious little evidence that the increasingly widespread use of these technologies offers countervailing benefits to public safety.

A. ShotSpotter noise detection technology

Overview of the Technology and Questions About Its Reliability

ShotSpotter is an audio surveillance system that purports to distinguish the sound of gunfire from other noises and to identify the sound's location. ShotSpotter sends alerts of supposed gunfire directly to local police, who are dispatched to the location that ShotSpotter provides to investigate.

ShotSpotter's service has three parts: *First*, ShotSpotter blankets neighborhoods with proprietary microphones installed on lampposts, buildings, and other structures. These microphones are always listening and recording the surrounding environment. The microphone device stores a rolling 30-hour window of audio locally, on the device itself. The microphones are sensitive enough to overhear the sounds of nearby voices.[21]

---

[19] Statement of Commissioner Rebecca Kelly Slaughter Regarding the Commercial Surveillance and Data Security Advanced Notice of Proposed Rulemaking, at 8, FEDERAL TRADE COMMISSION (Aug. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/RKS%20ANPR%20Statement%2008112022.pdf; Statement of Commissioner Alvaro Bedoya Regarding the Commercial Surveillance and Data Security Advanced Notice of Proposed Rulemaking, at 2–3, FEDERAL TRADE COMMISSION (Aug. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Bedoya%20ANPR%20Statement%2008112022.pdf

[20] Statement of Commissioner Rebecca Kelly Slaughter*, supra* note 19, at 7–8.

[21] *See, e.g.*, Cale Guthrie Weissman, *The NYPD's newest technology may be recording conversations*, BUSINESS INSIDER, (Mar. 26, 2015), https://www.businessinsider.com/the-nypds-newest-technology-

Second, whenever these microphones detect an "impulsive noise"—what ShotSpotter describes as any noise that goes "bang, boom or pop"[22]—an audio snippet is sent to ShotSpotter's central computing system. If multiple sensors detect a loud noise close in time, the audio snippets are processed through two secret, proprietary computer algorithms. One algorithm uses a machine learning system to make a first attempt at classifying the noise as the product of a gunshot or some other source like fireworks, a helicopter, etc.[23] Another algorithm attempts to locate where the sound originated by comparing small differences in the time that the noise was detected at each microphone. [24]

Third, ShotSpotter employs operators at call-center style facilities who review the output of these algorithms and can listen to the audio snippets themselves. These operators, who are hired with no prior audio or law enforcement expertise,[25] can and do override the algorithms to trigger alerts (or decline to trigger alerts).[26] When one of these employees issues an alert, it is sent out directly to local police, where officers are typically dispatched quickly to the location identified by ShotSpotter. Alerts are also typically sent to local police officers via a proprietary ShotSpotter app that is installed on department-issued mobile devices and which shows officers

---

may-be-recording-conversations-2015-3. ShotSpotter has taken voluntary steps to reduce the likelihood that law enforcement or others will gain access to these audio recordings for purposes of eavesdropping on conversations, but this remains a possible use and harm of the system. *See generally,* Policing Project, *Privacy Audit & Assessment of ShotSpotter, Inc.'s Gunshot Detection Technology,* NEW YORK UNIVERSITY SCHOOL OF LAW (2020), https://www.policingproject.org/s/PrivacyAuditandAssessmentofShotspotterFlex.pdf

[22] Testimony of Paul Greene, ShotSpotter Manager of Forensic Services, at Tr. 25:16-26:8, *California v. Reed*, No. 16015117 (Cal. Super. Ct. S.F. County, July 5–6, 2017) ("Greene Testimony in Reed") (testimony of ShotSpotter employee at Frye hearing in criminal case).

[23] *Id.* at Tr. 25:16–26:13, 113:19–114:2.

[24] *Id.* at Tr. 14:8–15:16; Joseph M. Ferguson & Deborah Witzburg, *The Chicago Police Department's Use of ShotSpotter Technology*, CITY OF CHICAGO OFFICE OF THE INSPECTOR GENERAL at 4 (Aug. 24, 2021), https://igchicago.org/wp-content/uploads/2021/08/Chicago-Police-Departments-Use-of-ShotSpotter-Technology.pdf ("The ShotSpotter system approximates the location of the possible gunshots [using] techniques for computing the source location of a sound based on the time of arrival and angle of arrival of sound waves at multiple surrounding sensors.").

[25] *Incident Review Center Specialist – Hiring All Shifts – FT/PT*, SHOTSPOTTER (last visited Nov. 20, 2022), https://www.shotspotter.com/career/service-operations-center-specialist-hiring-all-shifts-ft-pt/.

[26] Helen Webley-Brown, et al., *ShotSpotter and the Misfires of Gunshot Detection Technology*, at 7 Surveillance Technology Oversight Project, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT (July 14, 2022), https://www.stopspying.org/s/202277_ShotSpotter-Report_FINAL.pdf.

a "dot on the map" showing the purported location of the supposed gunshot.[27] In this way, ShotSpotter's operators are responsible for setting in motion a high-intensity police deployment responding to supposed gunfire.

Each stage of this process creates significant opportunities for error, and none of them has been subject to proper independent validation and testing so far as we are aware.[28]

Remarkably, despite the fact that ShotSpotter has been on the market for more than 20 years, there has never been a published, empirical study investigating how frequently the system triggers false alerts in response to noises like firecrackers, engine backfires, blown tires, and other sounds that are commonly mistaken for a gunshot. [29] There is simply no published, empirical data on the actual rate of false alerts generated by the system in general, let alone location-specific studies to determine how well it is performing in particular places. It is therefore impossible to know how often ShotSpotter is triggering alerts and sending policing out into neighborhoods in response to loud noises that are not gunfire.

In many cities, including Chicago, ShotSpotter's deployments are not even assessed using test-fired gunshots to see how frequently ShotSpotter *fails* to trigger an alert

---

[27] ShotSpotter, *ShotSpotter Mobile App* (last visited Nov. 20, 2022), https://www.shotspotter.com/shotspotter-mobile-app/.

[28] MJC has detailed the findings and concerns discussed here in more detail in a pair of *amicus* briefs filed in criminal prosecutions where police or prosecutors relied on ShotSpotter alerts. *See* Br. of Amicus Curiae Chi. Cmty. Based Organizations Brighton Park Neighborhood Council, Lucy Parsons Lab, and Organized Communities against Deportation, *State of Illinois v.* Williams, 20 CR 0899601 (Cir. Ct. of Cook Co., Crim. Div., May 3, 2021), available at https://www.macarthurjustice.org/wp-content/uploads/2021/05/Motion-for-Leave-to-File-Brief-as-Amici-Curiae-with-Ex.-A-Amicus-Brief-Attached.pdf; Br. for Amici Curiae Roderick and Solagne MacArthur Justice Center at Northwestern Pritzker School of Law and Innocence Project, Inc. in Supp. of Def.-Appellee and Affirmance, *Commonwealth v. Ford*, 2020-P-1334 (Mass. App. Ct., Sept. 24, 2021), available at https://www.macarthurjustice.org/wp-content/uploads/2021/05/Commonwealth-v-Ford-Amicus-Brief.pdf

[29] A 2016 report published by the Brookings Institution canvassed the evidence for ShotSpotter's rate of false-positive alerts and concluded that "[a]t this point, there is no reliable evidence about the rate of false positives in actual ShotSpotter data, and this is an area where future research would be helpful." *See* Jillian B. Carr & Jennifer Doleac, *The Geography, Incidence, and Underreporting of Gun Violence: New Evidence using ShotSpotter Data*, at 5, (Apr. 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2770506. We are aware of no subsequent studies testing the ShotSpotter system to determine the rate of false-positive alerts.

in response to actual gunfire (i.e. false negatives).[30] Nor does there appear to be empirical testing to determine whether the system is performing less accurately in some geographic areas, despite the fact that it is well known in the literature that local geography and the built environment can affect the propagation of the sounds upon which ShotSpotter relies.[31]

Similarly, there are serious concerns—and apparently no independent audits or oversight—of the proprietary machine learning algorithms that ShotSpotter uses. A technical paper published by ShotSpotter engineers, however, suggests that there may be serious problems with the design and implementation of the crucial noise-classification algorithm that is supposed to distinguish gunshots from other noises.[32] For example, the ShotSpotter paper explains that when ShotSpotter converts the raw audio snippets into an image format that is processed by the algorithm, ShotSpotter adds extraneous information that appears to have little to do with the actual sound that ShotSpotter's microphones picked up. ShotSpotter adds information about the number of "recent incidents" and "location of recent nearby incidents" before the algorithm attempts to classify the noise.[33] These pieces of information—which seem to concern *prior* noises rather than the specific noise event being assessed—could well lead the algorithm to overclassify noises as gunshots by placing significant weight on the presence of "nearby" or "recent" ShotSpotter alerts rather than focusing on features of the noise itself.

In addition, ShotSpotter engineers have conceded that there are errors in the samples that it uses to train the machine learning algorithms that classify noises as gunfire. In particular, ShotSpotter's engineers concede that ShotSpotter does not have independent knowledge about whether the audio samples that it uses to train its algorithm were actually produced by a gunshot, as opposed to some other source like firecrackers. In the words of ShotSpotter's technical paper: "In the vast majority of cases, ground truth . . . is not available, and it is to be expected it is to be

---

[30] Attachment G to Mot. to Exclude ShotSpotter Evidence Pursuant to *Frye* and Rule 403, *State of Illinois v.* Williams, 20 CR 089960 (Cir. Ct. Cook Co., Crim. Div., April 22, 2021) (Letter from Mike Will, ShotSpotter VP of Forensics and Technical Support, responding to a subpoena in a criminal case and stating "No live fire or DQV [Deployment Qualification Testing] was performed in any district as part of this service.")

[31] *See, e.g.*, Juan R. Aguilar, *Gunshot Detection Systems in Civilian Law Enforcement*, 63 J. Audio Eng. Soc'y 280, 281–82 (2015).

[32] Robert B. Calhoun, et al., *Precision and accuracy of acoustic gunshot location in an urban environment*, at 8 (Aug. 16, 2021), https://arxiv.org/pdf/2108.07377.

[33] *Id.*

expected that some training data are misidentified."[34] The paper explains that ShotSpotter's "human reviewers" simply label samples of "field collected data"—*i.e.* noises picked up by its sensors—in order to train the algorithm.[35] But there is no published evidence about whether ShotSpotter's human reviewers, examining disembodied audio snippets, can accurately distinguish gunshots from other sounds, and we are aware of no agreed standards in the scientific community about how to reliably classify noises as gunshots. Absent rigorous testing and validation—which, so far as we are aware has not happened, or at least has not been published—an algorithm trained in this way may produce unacceptably high false positive rates or could systematically misclassify some noises as gunfire.

The human reviewers who ultimately decide whether to trigger an alert are another potential source of unexamined error. Most troublingly, ShotSpotter refuses to disclose the basic protocol that these operators are trained to follow in order to decide whether to trigger alerts and set in motion a police response. ShotSpotter argues in court that this protocol—known as the "classification continuum"—is a trade secret and fights aggressively to keep it secret. However, in one criminal case a forensic audio expert retained by defense counsel was able to review this protocol while subject to a non-disclosure order. The expert's full opinion remains subject to a protective order, but in a public portion of his report he opines that "the document should be provided to anyone who deals with ShotSpotter systems so that the highly subjective nature of the gunshot determination is understood by those who use the information in the criminal justice system."[36] ShotSpotter is so reluctant to permit scrutiny of its operators' performance that it recently agreed to be held in contempt of court rather than disclose information about the qualifications and training of an analyst along with other basic information about potentially erroneous alerts.[37]

ShotSpotter has consistently made public statements that tend to mislead and deceive audiences about the how reliable the technology is. In particular, ShotSpotter repeatedly makes the marketing claim that its system is "97%

---

[34] *Id.*

[35] *Id.*

[36] Amended Mot. to Modify the ShotSpotter Protective Order at 5, *State v. Williams*, 20 CR 0899601 (Ill. Cir. Ct. Cook County May 10, 2021).

[37] Matt Chapman & Jim Daley, *ShotSpotter held in contempt of court: Rather than release documents, a ShotSpotter attorney requested the contempt order*, CHICAGO READER (July 26, 2022), https://chicagoreader.com/news-politics/shotspotter-held-in-contempt-of-court/.

accurate."[38] But a report commissioned by ShotSpotter itself in fact reveals that this supposed "accuracy" figure is not a measure of accuracy at all, and is not based on any actual testing of the system.[39] Instead, ShotSpotter calculates this supposed "accuracy" rate by simply *assuming* that every single one of its alerts corresponds to an actual gunshot. ShotSpotter then only counts an alert as an error if a local police department happens to send ShotSpotter a voluntary complaint that the system missed a gunshot or issued a false alert. If ShotSpotter concurs in its customer's complaint, ShotSpotter deducts the one alert from its assumption of 100% accuracy.[40]

Thus, when ShotSpotter says it is 97% accurate, what it is in fact reporting is that it receives 3 recognized complaints from customers for every 100 alerts that it sends out to police. This is not an "accuracy" rate in any scientifically respectable sense of the word. Among other things, the police officers who respond to ShotSpotter alerts (and could in theory file complaints with ShotSpotter) typically have no way to know what actually caused the loud noise that ShotSpotter detected. Moreover, in Chicago, a senior police official conceded in public testimony to the City Council that the department *never* sends complaints to ShotSpotter about false alerts. The statistic is thus nothing more than a rate of customer complaints and says nothing about the actual accuracy of the system's alerts. Yet ShotSpotter consistently touts

---

[38] *See, e.g.*, Jonathan Levinson, *Lobbying and lawsuits: How ShotSpotter convinced Portland to spend big on gunshot detection*, OPB (Nov. 7, 2022), https://www.opb.org/article/2022/11/07/shotspotter-convinced-portland-spend-big-controversial-gunshot-detection-technology/; Matt Masterson & Amanda Vinicky, *ShotSpotter Alerts 'Rarely' Lead to Evidence of Gun Crime: City Watchdog*, WTTW Chicago (Aug. 24, 2021), https://news.wttw.com/2021/08/24/shotspotter-alerts-rarely-lead-evidence-gun-crime-city-watchdog; Jon Schuppe & Joshua Eaton, *How ShotSpotter fights criticism and leverages federal cash to win police contracts*, NBC NEWS (Feb. 10, 2022), https://www.nbcnews.com/news/us-news/shotspotter-police-gunshot-technology-federal-grants-rcna13815; *ShotSpotter Respond™ Q&A,* SHOTSPOTTER (Dec., 2020), https://www.shotspotter.com/wp-content/uploads/2020/12/ShotSpotter-Respond-FAQ-Dec-2020.pdf ("5. How accurate is ShotSpotter's gunshot detection solution? The ShotSpotter system is highly accurate at detecting outdoor gunshots. In 2019 the system had a 97% aggregate accuracy rate across all of our customers including a very small false positive rate of less than 0.5% of all reported gunfire incidents."); *ShotSpotter Cities*, SHOTSPOTTER, https://www.shotspotter.com/shotspotter-cities/ (last visited Nov. 20, 2022).

[39] *Independent Audit of the ShotSpotter Accuracy*, EDGEWORTH ANALYTICS (March 28, 2022), https://www.edgeworthe conomics.com/wp-content/uploads/2022/03/Shotspotter-2022-Accuracy-Study.pdf

[40] *Id.*

this "97% accuracy rate" thereby misleading police departments, police officers, public officials, and members of the public alike.[41]

All of these concerns about ShotSpotter's transparency, reliability, and design have festered unresolved for years because there is no meaningful regulatory oversight of companies like ShotSpotter who sell surveillance technology to police departments.

Harms that flow from ShotSpotter technology

The deployment of ShotSpotter technology leads to a variety of documented harms. ShotSpotter prompts a massive number of high-intensity police deployments responding to supposed shots fired that, in fact, turn up no evidence of any kind of gun incident. Our original research[42], subsequently confirmed by Chicago's Office of Inspector General,[43] shows that more than 90% of ShotSpotter alerts lead police to find no evidence of any kind of gun-related incident—let alone evidence of an actual shooting—when they arrive at the location ShotSpotter sends them. In Chicago alone, this means that there are 31,640 unfounded ShotSpotter-prompted deployments every year and 87 on an average day.[44]

Each one of these deployments creates a dangerous, volatile, and unnecessary situation for people who happen to be in the vicinity of the ShotSpotter alert. They also sap significant resources that could be used in more effective ways to address gun violence and public safety.

ShotSpotter-prompted deployments also fuel a pattern of unwarranted police stops. The Chicago Inspector General identified more than 2,400 investigatory stops

---

[41] Any scientifically legitimate accuracy measure would have to separately assess the rate of false positives (i.e. alerts to non-gunfire) and false negatives (i.e. failure to alert to actual gunfire) as well as a separate assessment of the error rate with respect to the locations ShotSpotter provides for the sources of noises. *See generally* President's Council of Advisors on Science & Technology, *Report to the President: Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods*, EXECUTIVE OFFICE OF THE PRESIDENT, 44–66 (2016) (discussing fundamental principles regarding empirical validation of forensic methods similar to ShotSpotter, and observing that "It is necessary to have appropriate empirical measurements of a method's false positive rate and the method's sensitivity. [I]t is necessary to know these two measures to assess the probative value of a method.")

[42] MacArthur Justice Center, *Research Findings*, END POLICE SURVEILLANCE, https://endpolicesurveillance.com/research-findings/ (last visited November 17, 2022).

[43] *The Chicago Police Department's Use of ShotSpotter Technology*, CHICAGO OFFICE OF THE INSPECTOR GENERAL (August 24, 2021), https://igchicago.org/2021/08/24/the-chicago-police-departments-use-of-shotspotter-technology/

[44] MacArthur Justice Center, *Research Findings, supra* note 42.

linked to ShotSpotter alerts over the course of 18 months.[45] The Inspector General even found that police officers were justifying investigatory stops of residents based in part on a supposed high volume of ShotSpotter alerts in the general area *in the past*, so that the mere presence of ShotSpotter sensors (and the alerts that inevitably come along with them) can fuel police stops.[46]

ShotSpotter may lead police and prosecutors to falsely accuse people of crimes and bring false charges. Michael Williams, a 65-year old grandfather, was falsely accused of murder in Chicago because police put unwarranted faith in a ShotSpotter alert.[47] Mr. Williams was jailed in terrible conditions on these false charges for 11 months. When his defense attorneys mounted a vigorous challenge to the reliability of the ShotSpotter evidence and moved to exclude it, prosecutors dropped the ShotSpotter evidence rather than defend its reliability. Prosecutors subsequently conceded in court that without the ShotSpotter evidence they lacked any basis to continue prosecuting him.[48] Mr. Williams is now represented by MJC in a civil rights lawsuit asking the Court to end CPD's use and misuse of ShotSpotter and seeking justice for the year that was robbed from him.[49]

Another man, Silvon Simmons, was likewise prosecuted for murder on the basis of highly questionable ShotSpotter evidence in Rochester, New York. He was ultimately acquitted on the murder charges, and a related weapons conviction was reversed by the trial judge who concluded that evidence collected by ShotSpotter was too unreliable to sustain the conviction.[50]

---

[45] *The Chicago Police Department's Use of ShotSpotter Technology*, *supra* note 43.

[46] *Id.*

[47] Garance Burke et al., *How AI-powered tech landed man in jail with scant evidence*, ASSOCIATED PRESS (Mar. 5, 2022), https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220.

[48] Transcript of Proceedings, *State v. Williams*, No. 20 CR 0899601 at 3-4, (Ill Cir. Ct. Cook County July 23, 2022).

[49] Amended Complaint, *Williams et al. v. City of Chicago*, et al., No. 22-cv-3773 (N.D. Ill 2022), https://www.macarthurjustice.org/wp-content/uploads/2022/07/11.14.22-Amended-Complaint.pdf.

[50] *See* Reade Levinson & Lisa Girion, *A Black man risks all to clear his name - and expose the police,* REUTERS (Nov. 17, 2020), https://www.reuters.com/investigates/special-report/usa-police-rochester-trial/; Lisa Girion & Reade Levinson, *A U.S. city takes on its police union, and a nation is watching*, REUTERS (Nov. 17, 2020), https://www.reuters.com/investigates/special-report/usa-police-rochester-union/; Amended Complaint, *Simmons v. Ferrigno*, No. 17-cv-6176 (W.D.N.Y. Aug. 27, 2018).

ShotSpotter is also deployed overwhelmingly in predominantly Black and Latinx neighborhoods and it is only in these neighborhoods where ShotSpotter summons police for unnecessary and potentially dangerous encounters. In this regard, ShotSpotter is an example of what the Commission's ANPRM refers to as "[a]utomated system used by firms" that can "discriminate based on protected categories," particularly when deployed in discriminatory ways by customers.[51]

In Chicago, ShotSpotter is only deployed in the police districts that have the highest proportion of Black and Latinx residents and the lowest proportion of white residents.[52] 80% of Black residents of Chicago live under ShotSpotter's surveillance shadow; 70% of White residents do not. This racially-disparate deployment pattern appears to hold in other cities as well.[53] To the extent that ShotSpotter is fueling and providing technological justification for stop-and-frisk, false charges, and other aggressive and unwarranted law enforcement behaviors, it is thus doing so in a way that disproportionately harms people of color.[54]

ShotSpotter's surveillance system has these harmful consequences because its purpose is to dispatch police and shape where and how they are deployed. A number of other surveillance technologies including predictive policing software likewise influence police deployment decisions and so may produce similar harms.

ShotSpotter is also a data gathering tool, generating information about the supposed rates and location of gunfire. To the extent these statistics are faulty, they will tend to skew policy decisions, police tactics, and public perception. Moreover, the racialized deployment patter of ShotSpotter means that only those neighborhoods will be tagged with increased statistics about supposed gunfire that

---

[51] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, 51288 (Aug. 22, 2022) https://www.govinfo.gov/content/pkg/FR-2022-08-22/pdf/2022-17752.pdf

[52] MacArthur Justice Center, *The Burden on Communities of Color,* END POLICE SURVEILLANCE, https://endpolicesurveillance.com/burden-on-communities-of-color/ (last visited November 17, 2022).

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

[54] MJC has filed a class action lawsuit challenging Chicago's racially discriminatory use of ShotSpotter under the Equal Protection Clause as well as the Illinois Civil Rights Act, which prohibits disparate-impact race discrimination. The lawsuit also challenges the systematic misuse of ShotSpotter alerts to justify stop-and-frisks in violation of the Fourth Amendment. The Amended Complaint explains in more detail the problems with ShotSpotter technology and the discriminatory consequences of ShotSpotter's racially disparate deployment. *See* Amended Complaint, *Williams et al. v. City of Chicago, et al.*, No. 22-cv-3773 (N.D. Ill 2022), https://www.macarthurjustice.org/wp-content/uploads/2022/07/11.14.22-Amended-Complaint.pdf.

ShotSpotter inevitably produces. Like other surveillance technologies that generate data and statistics as a product of their surveillance, ShotSpotter can produce second-order harms by skewing decision-making and allocation of resources.

B. Electronic Monitoring Devices

Overview of the Technology and Questions About Its Reliability

Another category of law enforcement surveillance technology in increasingly common use is location monitoring services, often in the form of devices shackled to a person's ankle. Individuals are typically ordered to wear such devices as a condition of release from (or as an "alternative" to) incarceration in a jail, prison or immigration detention facility.[55] Thus, for example, people are ordered to wear an ankle monitor while awaiting criminal trial,[56] while immigration removal proceedings are pending,[57] while subject to the supervision of a juvenile court as a youth,[58] or as a condition of probation or supervised release imposed as part of a criminal sentence.[59]

Ankle monitors that track people's locations are built on one of two technologies: radio frequency or GPS.[60] Radio frequency ankle monitors, sometimes referred to as

---

[55] *Overview of Electronic Monitoring*, MEDIA JUSTICE, https://mediajustice.org/unshackling-freedom/what-you-should-know/ (last visited November 18, 2022); Yazmine Nichols et al., *Rethinking Electronic Monitoring: A Harm Reduction Guide*, AMERICAN CIVIL LIBERTIES UNION, (September 2022), https://www.aclu.org/report/rethinking-electronic-monitoring-harm-reduction-guide.

[56] Patrice James et al., *Cages Without Bars: Pretrial Electronic Monitoring Across the United States,* SHRIVER CENTER ON POVERTY LAW*,* (Sep. 2022), https://www.povertylaw.org/wp-content/uploads/2022/09/cages-without-bars-final-rev1.pdf.

[57] Aly Panjwani, *ICE Digital Prisons: The Expansion of Mass Surveillance as ICE's Alternative to Detention,* JUST FUTURES LAW, (May 2021), https://www.flipsnack.com/justfutures/ice-digital-prisons-1u8w3fnd1j.html;

[58] Catherine Crump, *Tracking the Trackers: An Examination of Electronic Monitoring of Youth in Practice*, 53 U.C. DAVIS L. REV. 795 (2019), https://lawreview.law.ucdavis.edu/issues/53/2/articles/files/53-2_Crump.pdf.

[59] Kate Weisburd, et al., *Electronic Prisons: The Operation of Ankle Monitoring in the Criminal Legal System*, George Washington University Law School Public Law Research Paper No. 2021-41 (September 27, 2021), at 6–8, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3930296

[60] *See* James*, Cages Without Bars*, *supra* note 56, at 11.

Another type of ankle monitor, known as a SCRAM device, measures and tracks a person's blood alcohol content by taking regular samples of the person's perspiration through the skin. *Id*.; Maya Dukmasova, *Cook County judge Vazquez's heavy use of sobriety monitor highlights oversight gaps*, INJUSTICE WATCH (Dec. 8, 2021), https://www.injusticewatch.org/news/judicial-conduct/2021/judge-

"curfew-monitoring" devices, operate by detecting whether the ankle monitor is in the vicinity of a base station located in the monitored person's home. These devices only alert authorities as to whether or not a person is at home.

GPS-tracking monitors, on the other hand, are meant to record a person's every movement by connecting directly with the GPS satellite infrastructure. Companies that sell GPS tracking services monitor and keep a record of a person's historical location 24/7. These devices can be configured to trigger alerts when a person leaves home or another designated place, or if a person enters a prohibited "exclusion zone." The systems can also be set up with a pre-determined movement schedule, for example triggering an alert if the person remains at a workplace longer than pre-scheduled hours.

Movement restrictions for people on ankle monitors can be extremely onerous and specific. In some places, people are categorically forbidden from leaving home altogether without specific, express permission from a court or supervising authority.[61]

Some ankle monitors are equipped with a microphone and speaker such that supervising agents can announce themselves to people on monitors at any time and demand a response.[62] Supervising agents can begin such communications at any time, for example while the monitored person is sleeping, working, or in church. When the monitor triggers an alert in public, it is audible to anyone in the vicinity. People on monitors must respond immediately to alerts or else risk being tagged with a violation and being taken into physical custody.

Ankle monitors are equipped with batteries that must be charged by the monitored person by plugging the device into the wall, typically for at least two continuous hours per day. [63] Authorities also often impose rules about the hours during which

---

vazquez-scram-monitor/; Maya Dukmasova, *Her crime was driving without a license; a judge forced her to choose between months in jail or a year of alcohol monitoring*, INJUSTICE WATCH (Aug. 5, 2022), https://www.injusticewatch.org/news/judicial-conduct/2022/alcohol-monitor-or-jail-judge-vazquez/.

[61] Kate Weisburd, et al., *Electronic Prisons: The Operation of Ankle Monitoring in the Criminal Legal System*, George Washington University Law School Public Law Research Paper No. 2021-41 (September 27, 2021), at 6–8, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3930296.

[62] *Id.* at 2; Nila Balad & Lars Trautman, *A Wearable Wiretap: A new generation of ankle monitors offers a range of advanced features—and raises a host of thorny questions*, SLATE (Nov. 8, 2019), https://slate.com/technology/2019/11/enhanced-ankle-monitors-community-supervision-privacy.html.

[63] Panjwani, *ICE's Digital Prisons*, *supra* note 57, at 9–11.

charging must occur.[64] During these times, the person on EM is physically attached to the electrical outlet. One person on electronic monitoring estimated that, with two hours of charging per day, he effectively "spent one month of every year leashed to a wall."[65]

Recently, a number of private companies have begun to market location monitoring systems that do not rely on an ankle monitor but instead leverage smartphone devices that most of us now carry in our pockets.[66] These apps access sensor data and, frequently, a range of other data found on people's phones and transmit it to the vendor. Typically, such apps require people to "check in" regularly, often by taking a picture of themselves that is sent to the monitoring company along with a timestamp, location information, and other data. Some vendors advertise using facial recognition software to "verify" that such pictures match the monitored person's photo.[67]

The companies that sell electronic monitoring to law enforcement agencies typically offer the devices themselves together with monitoring services staffed by employees of the private company. It is typically supervising agents employed by these private companies who first contact monitored people to enforce supposed violations.[68]

The location (and other) data generated by GPS-based ankle monitors is kept in databases maintained by the private companies who sell these systems to law enforcement. An individual's location information can be searched and filtered so that supervising agents and law enforcement officials can, in effect, go back in time and determine whether the monitored person was in a particular location at a

---

[64] *Id.* 8–9.

[65] Samuel Nesbit, *Tracking the Recent Decisions in North Carolina's Satellite-Based Monitoring Jurisprudence*, CAMPBELL LAW OBSERVER (May 4, 2020), http://campbelllawobserver.com/tracking-the-recent-decisions-in-north-carolinas-satellite-based-monitoring-jurisprudence/.

[66] *See generally* Kentrell Owens, Anita Alem, Franziska Roesner & Tadayoshi Kohno, *Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, Human-Centered, and Legal Perspectives*, PROCEEDINGS OF THE 31ST USENIX SECURITY SYMPOSIUM (Aug. 2022), https://www.usenix.org/system/files/sec22-owens.pdf.

[67] *See, e.g.*, BI Smartlink, BI INCORPORATED (Oct., 2022) https://bi.com/wp-content/uploads/2022/10/2210_FS_SmartLINK.pdf.

[68] *See* Johanna Bhuiyan, *Poor tech, opaque rules, exhausted staff: inside the private company surveilling US immigrants*, THE GUARDIAN (Mar. 7, 2022), https://www.theguardian.com/us-news/2022/mar/07/us-immigration-surveillance-ice-bi-isap.

particular time.[69] In Cook County, Illinois, it appears that data about location of people on electronic monitors is regularly being cross-matched with other sources of data—including the location of ShotSpotter alerts reporting supposed gunfire—in order to identify individuals to law enforcement officials as investigatory targets.[70]

It is unclear in what other ways electronic monitoring vendors might make use of the data they collect about people subject to monitoring. The contracts and privacy policies of electronic monitoring vendors are typically extremely permissive.[71] There are indications that some electronic monitoring vendors may sell or otherwise monetize the location data they collect about people who are forced to use their devices.[72]

There are upwards of 50 companies selling ankle monitoring devices to law enforcement agencies.[73] The market for these technologies is estimated to be larger than $1 billion per year.[74] The largest company selling electronic monitoring devices and services is BI Incorporated, which is now a wholly-owned subsidiary of GEO Group, one of the largest operators of private prison and mental health facilities in the world.[75] The smallest companies are startups selling new devices or apps into the marketplace.[76]

So far as we are aware, there are no testing, auditing, validation, or accreditation programs that apply to electronic monitoring devices. Companies enter contracts directly with law enforcement agencies and local governments to provide their products and services. There is no specific regulatory oversight of these products or transactions.

---

[69] *Id.* 19–20; *Panjwani*, ICE's Digital Prisons*, supra* note 57, at 8.

[70] Documents obtained through FOIA requests by advocates in Chicago show that this work has been undertaken by the University of Chicago Center for Radical Innovation for Social Change ("RISC") in partnership with the Cook County Sheriff's Office. Documents on file with the author.

[71] Weisburd, *Electronic Prisons*, *supra* note 61, 10–11; Panjwani, *ICE's Digital Prisons*, *supra* note 57, at 10; Owens et al., *Electronic Monitoring Smartphone Apps*, *supra* note 66, at 4085–86.

[72] Owens et al., *Electronic Monitoring Smartphone Apps, supra* note 66, at 4081–82.

[73] James, *Cages Without Bars*, *supra* note 56, at 12.

[74] *Id*.

[75] *Id*.

[76] *See* Owens, et al., *Electronic Monitoring Smartphone Apps, supra* note 66, at 4094 (listing electronic monitoring apps tested by the authors and their relative usage).

There is significant evidence that electronic monitors may trigger a very high number of false alarms where the device falsely reports to supervising officials that a person has left their home or other authorized location. A report prepared by a center affiliated with the University of Chicago for the Cook County Sheriff's Office indicated that around 80% of alerts were false alarms or "non-actionable alerts" triggered by "such factors as: low quality-signals, GPS drift, cell-based tracking, and inadequate grace period."[77]

False alerts result in the electronic monitoring device setting off an alarm that requires the monitored person immediately to explain themselves to supervising officials. On devices equipped with speakers and microphones, supervising agents may immediately contact the person and accuse them of violating the terms of EM. At minimum, false alarms are a major intrusion—a person is forced to stop everything and answer to the supervising agent. If treated as actual violations, false alarms can result in law enforcement officials immediately arriving at the person's home to take them back into custody for a supposed violation. False alarms can also later be used as retroactive "evidence" of a supposed program violation in order to justify increasing or revoking bond, revoking parole, or otherwise reincarcerating a person.[78]

In one notable case, a man subject to electronic monitoring in Cook County, Illinois documented dozens of false alarms where his ankle-monitor triggered an alert and supervising officials contacted him through the device about a supposed violation. He has recorded and posted 150 videos to YouTube showing false alerts and violations, documenting that he was in fact at home or at some other authorized location when he received the alerts.[79] In other cases, electronic monitors have sounded false alarms while the monitored person is in court standing in front of a judge or jury.[80]

---

[77] Matt Chapman & Natalie Frazier, *False Alarms: Ankle-monitor alerts garner phone calls and visits from sheriffs* [sic] *officers—but more than 80 percent are bogus, according to a University of Chicago analysis*, CHICAGO READER (June 9, 2022), https://chicagoreader.com/news-politics/false-alarms/.

[78] *Id.*

[79] *Id.*; Leor Galil, *22 Months: Jeremy Johnson has chronicled nearly two years of pretrial house arrest*, CHICAGO READER (June 9, 2022), https://chicagoreader.com/news-politics/news/22-months/; Monitored by Cook, YOUTUBE.COM, https://www.youtube.com/channel/UCTvnhaiUl1AVetrH-UEmQ8g.

[80] Matt Chapman & Natalie Frazier, *False Alarms*, *supra* note 77.

In many instances the person subject to monitoring must themselves pay for the device and the monitoring service.[81] Monitoring fees can exceed $5,000 per year.[82] In at least one jurisdiction, judges have ordered people to wear (and pay for) a particular company's electronic monitoring device even though the local supervising agency's contract with the company had expired.[83] Vendors have sued people subject to electronic monitoring to recover unpaid fees in amounts that sometimes exceed $10,000.[84] In other instances, failure to pay fees can lead to people being taken into physical custody.[85]

There is significant evidence that electronic monitoring is being imposed on people of color at vastly disproportionate rates. In Cook County, for example, 74% of people on electronic monitoring are Black even though only 23% of residents are Black.[86] The disparities in other jurisdictions are even worse: In San Francisco, for example, where just 6 percent of the population is Black, nearly half of the people on electronic monitors are Black.[87] As of May 2021, nearly 100,000 immigrants were subject to electronic monitoring at the direction of Immigration and Customs Enforcement.[88] Electronic monitoring and e-carceration threaten to become the newest frontier in the mass criminalization and control of marginalized people in America.[89]

---

[81] Weisburd, *Electronic Prisons*, *supra* note 61, 15–17; *Electronic Monitoring Fees: A 50-State Survey of the Costs Assessed to People on E-Supervision*, FINES & FEES JUSTICE CENTER (Sep. 2022), https://finesandfeesjusticecenter.org/content/uploads/2022/09/FFJC-Electronic-Monitoring-Fees-Survey-2022.pdf

[82] Weisburd, *Electronic Prisons*, *supra* note 61, 3.

[83] Maya Dukmasova, *SCRAM vendor continues to operate despite lapsed contract with Cook County*, INJUSTICE WATCH, (Aug. 5, 2022), https://www.injusticewatch.org/news/courts/2022/scram-cook-county-lapsed-contract/.

[84] *Id.*; Dukmasova, *Cook County judge Vazquez's heavy use of sobriety monitor highlights oversight gaps*, *supra* note 60; Dukmasova, *Her crime was driving without a license; a judge forced her to choose between months in jail or a year of alcohol monitoring*, *supra* note 60.

[85] *Electronic Monitoring Fees, supra* note 81, at 9

[86] James, *Cages Without Bars*, *supra* note 56, at 13.

[87] JAMES KILGORE, UNDERSTANDING E-CARCERATION: ELECTRONIC MONITORING, THE SURVEILLANCE STATE, AND THE FUTURE OF MASS INCARCERATION, 89 (The New Press 2022).

[88] Panjwani, *ICE's Digital Prisons*, *supra* note 57, at 4.

[89] Michelle Alexander, *The Newest Jim Crow*, N.Y. TIMES (Nov. 8, 2018), https://www.nytimes.com/2018/11/08/opinion/sunday/criminal-justice-reforms-race-technology.html.

Harms that flow from electronic monitoring

Electronic monitoring imposes a range of harms on both the people forced to wear the devices and their families and household members. At the most basic level, false alarms or minor violations from electronic monitoring devices can lead directly to a person being handcuffed, taken into custody, and reincarcerated. People on ankle monitors and their families thus live under the constant specter of law enforcement upending their lives.

Electronic monitoring also imposes a range of economic and social costs. Depending on the stringency of the movement restrictions imposed by the supervising authority, the person on EM might not be able to take care of even the most basic necessities of life, like buying groceries, doing laundry, or even taking out the trash.[90]

Electronic monitoring also severely impairs a person's ability to secure and maintain employment. Even if the supervising agency allows a person to travel outside their home to work, the limitations and reliability problems of the device itself prevent many kinds of employment. For instance, a person on EM must be able to charge the device for lengthy, often fixed periods that preclude unpredictable work schedules.[91] The devices often fail to work inside metal or concrete structures like warehouses—a workplace traditionally open to previously-incarcerated people. People on ankle monitors who work in such facilities are forced to leave work at random intervals to pick up a signal or call their monitoring agency, creating tension with employers.[92] Frequent interruptions due to alerts from the device make it very difficult to maintain a job in general.[93] The mere presence of a monitor

---

[90] Jonathan Manes, *Cook County judges are violating the SAFE-T Act's electronic monitoring reforms*, INJUSTICE WATCH (Nov. 16, 2022), https://www.injusticewatch.org/commentary/2022/electronic-monitoring-reforms-judges-violations/.

[91] Weisburd et al., *Electronic Prisons*, *supra* note 61, at 8-9.; Jennifer McKim, *'Electronic Shackles': Use of GPS Monitors Skyrockets in Massachusetts Justice System,* WGBH (Aug. 10, 2020) https://www.wgbh.org/news/local-news/2020/08/10/electronic-shackles-use-of-gps-monitors-skyrockets-in-massachusetts-justice-system; Olivia Solon*, 'Digital Shackles': The Unexpected Cruelty of Ankle Monitors*, THE GUARDIAN (Aug. 28, 2018) https://www.theguardian.com/technology/2018/aug/28/digital-shackles-the-unexpected-cruelty-of-ankle-monitors.

[92] James Kilgore, Emmett Sanders & Myaisha Hayes, No More Shackles: Why We Must End the Use of Electronic Monitors for People on Parole, THE CENTER FOR MEDIA JUSTICE (Sept. 16, 2018) at 7.

[93] *Commonwealth v. Norman*, 142 N.E.3d 1, 9-10 (Mass. 2020) (observing that the litany of "frequent interruptions" can "endanger an individual's livelihood").

strapped to a person's ankle carries a stigma that often makes employers reluctant to hire the person in the first place, particularly in positions that interact with the public.[94]

Ankle monitors can also cause physical injuries to the wearer. One survey found that a majority of monitored people experience a "constant negative impact" on their health, including electrical shocks, cuts and bleeding, inflammation, scarring, numbness, aches and pains, and excessive heat.[95] Ankle monitors also impair access to medical care. Medical procedures including MRIs, X-rays, CT scans, and mammograms cannot be performed while a patient wears an ankle monitor. The process by which a person can try to get approval to temporarily remove the device to receive such medical care is often unclear or non-existent.[96]

Electronic monitoring also exacts an enormous cost to the privacy of the wearer and anyone who lives with them or frequently accompanies them. At a basic level, an electronic monitor effectively turns the person's home into an extension of the jail or prison system's jurisdiction, allowing law enforcement officials to monitor constantly and arrive at any time to enter and verify compliance. All cohabitants of a person on EM can be subject to impromptu home searches or other intrusions whenever an ankle monitor registers a violation or officials demand access to the device.[97] The devices also intrude upon people's data privacy rights: the granular location information and other data gathered by the monitor is shared not just with law enforcement but is held by a private company that can analyze, share, or perhaps even sell or monetize it without meaningful notice or obvious limits.

People on EM also lose the ability to speak and assemble freely or anonymously because they know that the government is keeping a constant record of their movements. As Justice Sotomayor has observed: "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth

---

[94] Kilgore, Sanders & Hayes, *supra* note 92, at 7; Kilgore, UNDERSTANDING E-CARCERATION, *supra* note 86, at 81–83; Ava Kofman, *Digital Jail: How Electronic Monitoring Drives Defendants Into Debt*, PROPUBLICA (July 3, 2019), https://www.propublica.org/article/digital-jail-how-electronic-monitoring-drives-defendants-into-debt.

[95] Tosca Giustini et al., *Immigration Cyber Prisons: Ending the Use of Electronic Ankle Shackles*, CARDOZO LAW SCHOOL 13 (July 2021), https://larc.cardozo.yu.edu/cgi/viewcontent.cgi?article=1002&context=faculty-online-pubs.

[96] James Kilgore & Emmett Sanders, *Ankle Monitors Aren't Humane. They're Another Kind of Jail*, WIRED (Aug. 4, 2018) https://www.wired.com/story/opinion-ankle-monitors-are-another-kind-of-jail/; Kilgore, UNDERSTANDING E-CARCERATION, *supra* note 87, at 83–86.

[97] Weisburd et al., *Electronic Prisons*, *supra* note 61, at 12

of detail about her familial, political, professional, religious, and sexual associations."[98] The mere accumulation of that information chills protected expression and activity, presenting First Amendment concerns.[99]

Finally, electronic monitoring imposes significant dignitary harms. Because of the stigma surrounding involvement with the criminal legal system, the visibility of the monitoring device is one of its most salient burdens.[100] The presence of a monitoring device is expressive, signaling to its wearer that society does not forgive or trust him, and to the public that he is deviant, dangerous, and someone who has committed a serious enough crime that the state must keep him under surveillance.[101] Many describe EM as a deeply dehumanizing experience and reported feelings of anxiety, stigma, humiliation, a constant worry about concealing the ankle monitor, concern about the consequences of a potential device malfunction, feelings of being surveilled, and the fear of being arrested or detained.[102]

Despite these harms, the market for electronic monitoring devices remains almost entirely unregulated, without any oversight of their reliability, marketing, or even their utility as a public safety tool. Companies are free to devise ever more intrusive forms of monitoring and to sell them directly to law enforcement agencies who will force people to wear and often pay for the devices.

3. The Commission can and should enact regulations that would reduce harm in this sector of the surveillance industry.

The Commission has an opportunity to address the regulatory void within which companies now operate when they sell surveillance products to law enforcement. As illustrated in the examples described earlier, the lack of proper oversight has meant

---

[98] *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

[99] Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013), https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_richards.pdf; Alex Abdo, *Why Rely on the Fourth Amendment to Do the Work of the First?*, 127 YALE L.J. FORUM 444, 447–49 (2017), https://www.yalelawjournal.org/pdf/Abdo_5czbvbj9.pdf.

[100] Ben A. McJunkin & J.J. Prescott, *Fourth Amendment Constraints on the Technological Monitoring of Convicted Sex Offenders*, 21 NEW CRIM. L. REV. 379, 413 (2018); *See also* Brian Payne & Randy R. Gainey, *A Qualitative Assessment of the Pains Experienced on Electronic Monitoring*, 42 INT'L J. OFFENDER THERAPY & COMP. CRIMINOLOGY 149, 153–56 (1998).

[101] *See* McJunkin & Prescott, *supra* note 100, at 416; James Baimbridge, *My GPS-Tracked Life on Parole*, THE MARSHALL PROJECT (Oct. 28, 2019), https://www.themarshallproject.org/2019/10/28/my-gps-tracked-life-on-parole.

[102] Giustini, et al., *supra* note 95, at 15-16.

that there are no regulations about how well such products must work; there are no specific regulations of the marketing claims that vendors can make when pitching their products to far-flung police departments; there are no regulations that would surface the harms that flow to consumers as a result of the use and predictable failures of these products; and there are no regulations requiring even basic transparency about the surveillance products on the market, even though such products are increasingly shaping how law enforcement operates and interacts with the public.

We make four specific recommendations about measures the Commission should take to regulate this industry:

First, we urge the Commission to ensure that any proposed rule and regulations adopted encompass law enforcement surveillance technologies. Any new rules that apply to private companies that sell surveillance products into the private sector should apply equally to private companies that supply surveillance products to law enforcement agencies.

Second, we encourage the Commission to adopt regulations that would require companies selling surveillance products to law enforcement agencies to submit to independent auditing, testing, and validation of their products before they can be marketed to law enforcement customers. Given the grave risks of harm when faulty technologies are used in the criminal legal system—and given the absence of other effective regulatory constraints—it is essential to have independent, pre-marketing testing and validation of surveillance products.

Third, we encourage the Commission to adopt rules that flesh out the obligation of companies not to engage in deceptive or misleading claims when marketing surveillance technology to law enforcement agencies. One regulatory intervention could require companies to disclose all of the evidence, studies, and data that support any marketing claims that they make about the reliability, efficacy, or utility of their surveillance products. Such a rule could also reaffirm that the familiar legal prohibitions against misleading claims or "deceptive acts or practices in or affecting commerce"[103] apply with respect to products that are sold to law enforcement agencies.

Fourth, we encourage the Commission to adopt rules that require certain baseline levels of transparency with respect to surveillance products sold to law enforcement. Public, democratic oversight of law enforcement decisions to acquire surveillance technologies is impossible without meaningful transparency. In the interest of ensuring a fair and transparent marketplace for these products, the Commission

---

[103] 15 U.S.C. § 45(a)(1).

could mandate disclosure of the results of testing, validation and efficacy studies; data privacy rules and practices; privacy impact assessments; and an assessment of the risks with respect to civil rights and race disparity.

* * *

We are grateful for the opportunity to submit these comments and hope that they will be of use to the Commission as it pursues this important rulemaking. We stand ready to provide further information or assistance with respect to any of the matters discussed in this comment.

Respectfully submitted,

Jonathan Manes
Attorney, Illinois Office
Roderick & Solange MacArthur Justice Center