*Appeal No. 24-1025*

**IN THE**

**UNITED STATES COURT OF APPEALS**

**FOR THE NINTH CIRCUIT**

JOSHUA SIMON, ET AL.,

PLAINTIFFS-APPELLEES,

v.

CITY AND COUNTY OF SAN FRANCISCO, ET AL.,

DEFENDANTS-APPELLANTS.

On Appeal from the United States District Court
for the Northern District of California
Case No. 4:22-cv-05541 JST
The Honorable Jon S. Tigar

# *AMICUS BRIEF* OF NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF PLAINTIFFS-APPELLEES

**MORRISON & FOERSTER LLP**
GALIA Z. AMRAM
LAURA LIVELY BABASHOFF
LARA MCDONOUGH
CHLOE CONNOLLY
425 Market Street,
San Francisco, California 94105-2482
Telephone: 415.268.7000
Facsimile: 415.268.7522
GAmram@mofo.com
LLively@mofo.com
LMcDonough@mofo.com
CConnolly@mofo.com

*Counsel for National Association of Criminal Defense Lawyers*

# TABLE OF CONTENTS

**Page**

# TABLE OF AUTHORITIES

**Page(s)**

## Cases

**Other Authorities**

## CORPORATE DISCLOSURE STATEMENT

### Federal Rules of Appellate Procedure 29(a)(4)(A), 26.1

*Amicus Curiae* is a non-profit corporation or organization. *Amicus* has no parent corporation, and no publicly held corporation owns 10% or more of its stock.

DATED: May 17, 2024

Respectfully submitted,

By: */s/ Galia Z. Amram*

Galia Z. Amram
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, CA 94105-2482
Telephone: 415.268.7000
Facsimile: 415.268.7522
GAmram@mofo.com

*Counsel for National Association of Criminal Defense Lawyers*

## STATEMENT OF CONSENT

PURSUANT TO FEDERAL RULE OF Appellate Procedure 29(a), *Amicus Curiae* hereby state that this brief is being filed based on the consent of all parties.

DATED: May 17, 2024

Respectfully submitted,

By: */s/ Galia Z. Amram*

Galia Z. Amram
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, CA 94105-2482
Telephone: 415.268.7000
Facsimile: 415.268.7522
GAmram@mofo.com

*Counsel for National Association of Criminal Defense Lawyers*

## STATEMENT REGARDING AUTHORING OF BRIEF

### Federal Rules of Appellate Procedure 29(a)(4)(e), Rule 32

*Amicus* certifies that no counsel for any party authored this brief in whole or in part, no party or party's counsel contributed money that was intended to fund preparation of submission of the brief, and no persons other than *Amicus* contributed money that was intended to fund preparation or submissions of the brief.

DATED: May 17, 2024

Respectfully submitted,

By: */s/ Galia Z. Amram*

Galia Z. Amram
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, CA 94105-2482
Telephone: 415.268.7000
Facsimile: 415.268.7522
GAmram@mofo.com

*Counsel for National Association of Criminal Defense Lawyers*

## IDENTITY AND INTEREST OF *AMICUS CURIAE*

**The National Association of Criminal Defense Lawyers (NACDL)** is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers, with tens of thousands of members and affiliates throughout the country. NACDL is particularly interested in cases arising from surveillance technologies and programs that pose new challenges to personal privacy. It operates a dedicated initiative that trains and directly assists defense lawyers handling such cases to help safeguard privacy rights in the digital age. NACDL has also filed numerous amicus briefs in this Court and the Supreme Court on issues involving digital privacy rights, including: *Carpenter v. United States*, 585 U.S. 296 (2018); *Riley v. California*, 573 U.S. 373 (2014); *United States v. Jones*, 565 U.S. 400 (2012); *State v. Aranda*, 370 Or. 214 (2022); *In re J. C. N.-V.*, 359 Or. 559 (2016).

## I. INTRODUCTION

The San Francisco Sheriff's Office's ("Sheriff" or "SFSO") policy of sharing pretrial releasees' location data with other law enforcement agencies and officers on an ongoing basis as part of the pretrial Electronic Monitoring ("EM") program is not necessary to achieve the program's stated goals of ensuring public safety and appearance in court. For decades, law enforcement agencies in California have used EM as a *less* restrictive alternative to pretrial detention without sharing the private and constitutionally protected information of pretrial releasees. Pretrial releasees' location data also is not shared on an ongoing, warrantless basis in the federal EM system, further demonstrating that effective monitoring can be achieved without compromising a pretrial releasee's privacy and due process rights. Ultimately, if SFSO determines that sharing a pretrial releasee's location data is necessary for public safety, there is a simple solution: they can obtain a warrant. But the warrantless, ongoing sharing of location data belonging to presumptively innocent pretrial releasees is a plainly unnecessary violation of the constitutional rights to privacy and due process.

## II. CALIFORNIA'S EM PROGRAM IS NOT INTENDED TO GRANT LAW ENFORCEMENT AGENCIES LIMITLESS POWER TO SURVEIL INDIVIDUALS.

California's EM program is not intended to give law enforcement a limitless license to surveil San Francisco's presumptively innocent residents. It is intended

to be a less restrictive alternative to pretrial detention. Judges may require an individual awaiting trial to participate in the program "for the *limited purposes* of ensuring future court appearances and protecting public safety." 1-ER-10 (emphasis added)); *see also In re Humphrey*, 11 Cal. 5th 135, 142 (2021) (noting that pretrial detention should be reserved for those who otherwise cannot be relied upon to make court appearances or who pose a risk to public or victim safety).[1] SFSO's use of EM to conduct invasive, warrantless sharing of a pretrial releasee's location data is unnecessary for achieving either purpose.

### A. SFSO's Policy of Sharing Pretrial Releasee's Location Data Is A Gross Misuse Of The EM Program.

SFSO administers the electronic monitoring of individuals on pretrial release via its EM Program Rules for Pre-Sentenced Participants ("Program Rules"). Under the Program Rules, the Sheriff and its private contractor, Sentinel Offender Services LLC ("Sentinel"), enroll individuals by outfitting them with an ankle monitor providing continuous GPS location coordinates, which is monitored twenty-four hours a day, seven days a week by SFSO and Sentinel. The data is also stored historically on Sentinel's servers. Under the current program, law

[1] Sara Zampierin, *Mass E-Carceration: Electronic Monitoring As A Bail Condition*, 2023 Utah L. Rev. 589 (2023) ("Pretrial electronic monitoring should be severely limited if decisionmakers follow the inquiries required by the Eighth Amendment, Due Process Clause, and state law and require the government to prove that the bail condition is the least restrictive condition that could mitigate the risks of flight and to public safety.")

enforcement agencies other than SFSO can request a releasee's historical or current location data at any time for any law enforcement purpose without any judicial oversight.

The rules set forth in the Program Rules and the "San Francisco Sheriff's Dept. Electronic Monitoring Program Participant Contract: Pre-Sentenced Individuals" ("Participant Contract") impose no limitation on which agencies may request this location data. Rule 13 (later changed to Rule 11) of the Program Rules provides, "I acknowledge that my EM data may be shared with other criminal justice partners." 2-ER-116. Similarly, Paragraph 9 of the Participant Contract states, "I acknowledge that my electronic monitoring data may be shared with other criminal justice partners." 2-ER-151. In both documents, "criminal justice partners" is not defined. 2-ER115-116, 2-ER-149-153.

The hurdle for a requesting agency or officer to obtain a pretrial releasee's location data from SFSO is quite low. The requestor does not need a warrant or even articulable suspicion. They need only submit a form titled "Electronic Monitoring Location Request" to the Sheriff and represent that they are requesting this information as part of a current criminal investigation. Upon doing so, the requestor can receive either the GPS location data of a specific individual on EM across a particular period or the GPS location data of anyone on GPS tracking in a

specific location. *See* 5-ER-797, *People v. Robinson*, MCN 21000279 (San Francisco Sup. Ct. Feb. 19, 2021).

There is simply no applicable precedent to justify this broad overreach by law enforcement agencies in sharing sensitive location data. Reliance on *United States v. Hensley*, for example, is misplaced. 469 U.S. 221, 232 (1985). *Hensley* involved a minimally intrusive investigatory stop based on a "wanted flyer" posted by another police department. The court held that an investigatory stop in reliance on that flyer, which was issued on basis of articulable facts supporting a reasonable suspicion that the person wanted had committed an offense, was constitutionally reasonable. *Id*. at 233. That situation is not comparable to the issue presented here. The highly intrusive 24/7 location data provided by SFSO to other law enforcement agencies is not shared on the basis of any particularized suspicion or exigent circumstances.

Moreover, the practice of sharing EM location data has grown only in recent years and is used in only a limited number of cases, which also calls into question its necessity. The number of location data requests has increased dramatically, but only recently. In 2019, the Sheriff shared the GPS location data of four individuals with other agencies. 1-ER-13. In 2020, that number increased to 41, and in 2021, it grew to 179. *Id*. This growth has not matched the overall growth of the EM program itself. In 2018, the EM program averaged an annual caseload of 75; in

2021, it reached an annual caseload of 1,650.[2] In 2021, SFSO received data requests for only 10% of its cases. That SFSO managed to administer the EM program without providing access to this highly private data to other agencies prior to 2018 and that it shares this location data for only a small percentage of individuals supports that it is not actually necessary.

### B. Sharing Location Data Is Not Necessary to Promote Public Safety or Ensure Court Attendance.

SFSO claims that sharing location data with other law enforcement agencies is necessary to protect the public. But infringing upon the constitutional rights of the public is not protection. Unlimited and warrantless sharing of location data violates both the United States and California constitutions by subjecting pretrial detainees to unjustified invasions of privacy. *See United States v. Jones*, 565 U.S. 400 (2012) (installing a GPS tracking device to monitor a vehicle's movements constitutes a search under the Fourth Amendment); *Grady v. North Carolina*, 575 U.S. 306 (2015) (wearing a GPS monitor constitutes a search under the Fourth Amendment); *see also Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35–37 (1994) (analyzing whether a drug testing program furthered its stated purpose, the utility of the program manifestly outweighed any resulting impairment of the

[2] *See* Alissa Skog, et al., Pretrial Electronic Monitoring in San Francisco, California Policy Lab (2022), https://www.capolicylab.org/wp-content/uploads/2022/11/Pretrial-Electronic-Monitoring-in-San-Francisco.pdf.

privacy right, and whether there are alternatives to drug testing less offensive to privacy interests); *Carpenter v. United States*, 585 U.S. 296, 309-310(2018) (warrantless seizure of cell-site records violates Fourth Amendment right); *United States v. Freeman*, 635 F. Supp. 2d 1205, 1208 (D. Or. 2009) ("Warrantless search of house is per se unreasonable.").

This practice also is not justified under either a "totality of the circumstances" or "special needs" analysis, because the invasion of privacy does more to harm the public than protect it. *United States v. Knights*, 534 U.S. 112, 118–119 (2001) ("the degree to which [this data sharing policy] intrudes upon an individual's privacy" is not justified by "legitimate governmental interests."); *see also In re York*, 9 Cal. 4th 1133, 1149 (1995) (holding that "a court must balance 'the nature and quality of the intrusion . . . [against] the governmental interests'").

The public safety risk posed by pretrial releasees is not the same as that of someone post-conviction. "[P]retrial releasees are ordinary people who have been accused of a crime but are presumed innocent." *United States v. Scott*, 450 F.3d 863, 871–74 (9th Cir. 2006). As such, the government cannot assume that pretrial releasees are "more likely to commit crimes than other members of the public, without an individualized determination to that effect." *Scott,* 450 F.3d at 874. This assumption would be "contradicted by the presumption of innocence" to which every person is entitled. *Id.*

Participation in the EM program also does not reduce reasonable expectations of privacy of those who have been detained pretrial. *Id.* at 873–74 (A pre-trial releasee's "privacy and liberty interests [a]re far greater than a probationer's."). "Any condition imposed on a criminal defendant must be '*the least restrictive*' way to 'reasonably assure the appearance of the person as required and the safety of any other person and the community.'" *United States v. Perez-Garcia*, 96 F.4th 1166, 1175 (9th Cir. 2024) (quoting 18 U.S.C. § 3142(c)(2)(B)) (emphasis added); *In re Humphrey*, 11 Cal. 5th 135, 146, 482 (2021).) Conditions of pretrial release cannot be justified as punishment, rehabilitation, or deterrence. U.S. Const. amends. V, VI.; *United States v. Salerno*, 481 U.S. 739, 747 (1987) (noting certain restrictions on liberty for pretrial releasees may constitute impermissible punishment); *Bell v. Wolfish*, 441 U.S. 520, 539 n.20 (1979) ("Retribution and deterrence are not legitimate non-punitive governmental objectives."). Thus, applying a *per se* rule that exigent circumstances necessarily exist to justify warrantless sharing of location data merely because someone has been placed into the EM program is inappropriate. *See Missouri v. McNeely*, 569 U.S. 141, 156 (2013) (finding that a *per se* rule for nonconsensual blood testing cannot be applied because exigency must be determined case-by-case based on the totality of the circumstances).

Moreover, there are no "special needs" that justify the warrantless sharing of a pretrial releasee's location data. Ensuring attendance at hearings, assuring compliance with court-ordered restrictions, and addressing violations of the Program Rules does not require sharing location data with agencies outside of SFSO. The Superior Court entrusted SFSO with monitoring the releasee's attendance at court appearances and their adherence to court-ordered rules—not any other law enforcement agency. Cases that permit warrantless searches are generally decided based on individualized, exigent circumstances or apply to individuals already convicted of a crime. *See*, *e.g.*, *Griffin v. Wisconsin*, 483 U.S. 868, 873–74 (1987) (permitting a warrantless search of a probationer's home because "special needs" of Wisconsin's probation system made the warrant requirement impracticable and justified replacement of probable cause standard by 'reasonable grounds' standard). Again, a *per se* rule permitting SFSO's location sharing policy is inappropriate under this analysis because a pre-trial releasee's "privacy and liberty interests [a]re far greater than a probationer's" and therefore require a case-by-case analysis to satisfy the demands of the Fourth Amendment. *Scott*, 450 F.3d at 873–74; *McNeely*, 569 U.S. at 156.

### C. The Warrant System Is Sufficient to Promote Public Safety.

Sharing sensitive location data with other law enforcement agencies is unnecessary because law enforcement agencies can and should obtain a warrant,

ensuring compliance with constitutional protections and promoting targeted and limited investigations. Requiring law enforcement agencies to obtain a warrant to receive this data upholds the constitutional rights of pretrial releasees by ensuring that data requests are supported by a judge's determination of necessity. *Carpenter*, 585 U.S. at 298 (finding that individuals have a reasonable expectation of privacy in cell-site location data and noting "[a] warrant is required...where the suspect has a legitimate privacy interest in records held by a third party."); *Riley v. California*, 573 U.S. 373, 382 (2014) (citation omitted) ("[A] warrant ensures that the inferences to support a search are 'drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.'") Further, requiring a warrant protects due process. It provides a safeguard for pretrial releasees who are presumed innocent and who deserve the same protections against undue surveillance or data sharing. *Scott*, 450 F.3d at 873–74.

Law enforcement agencies and officers should not be permitted to short-circuit the warrant process by taking advantage of individuals participating in the EM program. The only time a warrantless search should be permitted against a pretrial releasee is where the judge has ordered that submission to warrantless searches is a specific condition of release, which is based on individualized findings. 1-ER-10.

Finally, the lack of judicial oversight in SFSO's current system poses additional risks to the public. It may lead to increased scrutiny or enforcement measures, which undermines the less restrictive intent of electronic monitoring. Unrestricted data sharing may encourage fishing expeditions by law enforcement or inappropriate profiling and bias. *See*, *e.g.*, *United States v. Mumphrey*, 193 F. Supp. 3d 1040, 1042, 1069 (N.D. Cal. 2016) (finding "substantial evidence suggestive of racially selective enforcement by the San Francisco Police Department."). Law enforcement agencies may inappropriately rely on location data to profile individuals based on frequenting certain areas or interacting with certain groups. *See*, *e.g.*, *Raza v. City of New York*, No. 1:13CV03448, 2013 WL 3079393 (E.D.N.Y.) (complaint ultimately resulting in settlement with Muslim community groups following NYPD's "Muslim Surveillance Program"). The lack of oversight may also erode the public's trust in law enforcement. On the contrary, a warrant process fosters public trust by demonstrating that law enforcement agencies respect constitutional rights to privacy and adhere to established legal procedures. Requiring a warrant also aligns with precedent emphasizing that judicial oversight is important when handling sensitive personal information, such as location data. *Riley*, 373 U.S. at 382-83.

### D. The Federal System for Electronic Monitoring Proves That Sharing Location Data is Unnecessary.

The federal EM system further demonstrates that the sharing of location data collected from pretrial releasees with other law enforcement agencies is not necessary to promote public safety and ensure court appearances.

Under the federal EM system, only half of participants are placed in a GPS tracker system in which the participant's location is detected 24/7 via GPS satellites, cellular towers, and/or Wi-Fi. Most of the remaining EM participants are tracked by wearing a transmitter that emits radio frequency units, which send a signal to the receiver in the participants' resident to verify that wearer is at home.[3] However, authorities will not know the location of the participants when they leave their home.[4] Thus, nearly half of the individuals in the federal EM system are already subject to much less intensive monitoring than what is administered by SFSO.

For participants that wear the GPS tracker, federal law enforcement officers receive electronic notification when an individual moves into or out of approved or prohibited areas, or if the device is tampered with or removed. But these officers

---

[3] *See* U.S. Courts, *Federal Location Monitoring*, https://www.uscourts.gov/services-forms/probation-and-pretrial-services/supervision/federal-location-monitoring.

[4] *See* U.S. Gov't Accountability Off., GAO-16-10, *Federal Real Property: DHS and GSA Need to Strengthen the Management of DHS Headquarters Consolidation* (2015), https://www.gao.gov/assets/gao-16-10.pdf.

do not track a person's movement in the community in real time, 24 hours a day, seven days a week. Instead, they rely on activity reports and emergency alerts to intercede if conditions ordered by the judge are violated.[5] There is no policy in the federal system of sharing location data with other law enforcement agencies. Therefore, the federal EM system provides a key exemplar that less invasive monitoring policies can still effectively protect the public and ensure compliance with pretrial conditions and court appearances.

## III. CONCLUSION

The District Court's order properly found that invasive and warrantless sharing of location data with other law enforcement agencies is unnecessary and should be enjoined. Requiring agencies and officers to obtain a warrant maintains the integrity of the justice system by ensuring that constitutional rights are respected without compromising public safety.

[5] *See* U.S. Courts, Federal Location Monitoring, https://www.uscourts.gov/services-forms/probation-and-pretrial-services/supervision/federal-location-monitoring.

DATED: May 17, 2024

Respectfully submitted,

By: */s/ Galia Z. Amram*

Galia Z. Amram
Laura Lively Babashoff
Lara M. McDonough
Chloe Connolly
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, CA 94105-2482
Telephone: 415.268.7000
Facsimile: 415.268.7522
GAmram@mofo.com

*Counsel for National Association of Criminal Defense Lawyers*

## CERTIFICATE OF COMPLIANCE

This brief complies with all typeface and type-volume requirements of the Federal Rules of Appellate Procedure because it has been prepared using Microsoft Word's 14-point, proportionally spaced, Times New Roman font and contains 2,618 words.

DATED: May 17, 2024

Respectfully submitted,

By: */s/ Galia Z. Amram*

Galia Z. Amram
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, CA 94105-2482
Telephone: 415.268.7000
Facsimile: 415.268.7522
GAmram@mofo.com

*Counsel for National Association of Criminal Defense Lawyers*

## CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on May 17, 2024.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

DATED: May 17, 2024

*/s/ Galia Z. Amram*

Galia Z. Amram
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, CA 94105-2482
Telephone: 415.268.7000
Facsimile: 415.268.7522
GAmram@mofo.com

*Counsel for National Association of Criminal Defense Lawyers*