No. 26-689

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

v.

CORY SPURLOCK,

DEFENDANT-APPELLANT.

On Appeal from the United States District Court
For the District of Nevada
No. 3:23-cr-00022-MMD-CLB

Hon. Miranda M. Du, District Judge

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF NEVADA, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLANT AND AFFIRMANCE IN PART AND REVERSAL IN PART

Laura Moraff
Kiran Wattamwar
Nathan Freed Wessler
Brett Max Kaufman
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
lauramoraff@aclu.org

Christopher M. Peterson
American Civil Liberties Union of Nevada
4362 W. Cheyenne Ave.
North Las Vegas, NV 89032
(702) 366-1226
peterson@aclunv.org

Andrew Crocker
Jennifer Lynch
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
andrew@eff.org

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rules 26.1 and 29(a)(4)(A) of the Federal Rules of Appellate Procedure, *amici curiae* state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

Dated: November 3, 2026

/s/ Laura Moraff
Laura Moraff

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF *AMICI CURIAE* 1

INTRODUCTION 2

ARGUMENT 5

I. Tower-Dump Warrants Are Unconstitutional General Warrants 5

A. Tower Dumps Are "Searches" Under the Fourth Amendment 5

B. Tower-Dump Warrants Inherently Violate Bedrock Fourth Amendment Requirements 7

C. Tower-Dump Warrants Infringe on the Associational Privacy of Countless Innocent Bystanders 12

II. If this Court Declines to Hold that Tower-Dump Warrants Are *Per Se* Unconstitutional, it Should Articulate Constitutional Limitations to Minimize their Harms to Suspects and Bystanders 15

III. Evidence Obtained from the Tower-Dump Warrant Must Be Suppressed 20

IV. The Court Should Decide the Underlying Fourth Amendment Issues Before Addressing the Good-Faith Exception 22

CONCLUSION 25

CERTIFICATE OF SERVICE 27

TABLE OF AUTHORITIES

Cases

Ashcroft v. al-Kidd,
563 U.S. 731 (2011) 8

Berger v. New York,
388 U.S. 41 (1967) 15, 16, 18, 19

Buckley v. Valeo,
424 U.S. 1 (1976) 13

Carpenter v. United States,
585 U.S. 296 (2018) ..... *passim*

Chatrie v. United States,
609 U.S. 605 (2026) ..... *passim*

Commonwealth v. Perry,
184 N.E. 3d 745 (Mass. 2022) 1, 17, 18

Coolidge v. New Hampshire,
403 U.S. 443 (1971) 9

First Choice Women's Resource Centers, Inc. v. Davenport,
608 U.S. 174 (2026) 13

Groh v. Ramirez,
540 U.S. 551 (2004) 21

Illinois v. Gates,
462 U.S. 213 (1983) 20, 24

In re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. 2703(c), 2703(d) Directing AT & T, Sprint/Nextel, T-Mobile, Metro PCS, Verizon Wireless,
42 F. Supp. 3d 511 (S.D.N.Y. 2014) 16, 18

In re Four Applications for Search Warrants Seeking Information Associated With Particular Cellular Towers,
No. 3:25-CR-38, 2026 WL 2260371 (S.D. Miss. Aug. 5, 2026) 9, 10, 21, 23

In re Four Applications for Search Warrants Seeking Information Associated with Particular Cellular Towers,
No. 3:25-CR-38-CWR-ASH, 2025 WL 1792841 (S.D. Miss. June 27, 2025) 10

In re Four Applications for Search Warrants Seeking Information Associated with Particular Cellular Towers,
No. 3:25-CR-38-CWR-ASH, 2025 WL 603000 (S.D. Miss. Feb. 21, 2025) 9, 10

In re Search Information that is Stored at Premises Controlled by Google,
542 F. Supp. 3d 1153 (D. Kan. 2021).....16

In re Search of Cellular Telelphone Towers,
945 F. Supp. 2d 769 (S.D. Tex. 2013)..... 18, 19

In re U.S. ex rel. Order Pursuant to 18 U.S.C. Section 2703(d),
930 F. Supp. 2d 698 (S.D. Tex. 2012).....18

In re United States for an Order Pursuant To 18 U.S.C. §2703(d),
No. 2:17-MC-51662, 2017 WL 6368665 (E.D. Mich. Dec. 12, 2017).....18

Kyllo v. United States,
533 U.S. 27 (2001).....5, 6

Marcus v. Search Warrants of Property at 104 E. Tenth St.,
367 U.S. 717 (1961).....12

Matter of Tower Dump Data for Sex Trafficking Investigation,
No. 23 M 87, 2023 WL 1779775 (N.D. Ill. Feb. 6, 2023) 19

NAACP v. State of Ala. ex rel. Patterson,
357 U.S. 449 (1958).....13

O'Connor v. Donaldson,
422 U.S. 563 (1975).....24

Olmstead v. United States,
277 U.S. 438 (1928).....5

Payton v. New York,
445 U.S. 573 (1980).....20

People v. Meza,
312 Cal. Rptr. 3d 1 (Cal. Ct. App. 2023) 2

Riley v. California,
573 U.S. 373 (2014).....21

Roberts v. U.S. Jaycees,
468 U.S. 609 (1984).....12

Stanford v. Texas,
379 U.S. 476 (1965).....8, 15

State v. Bryant,
No. A-43/44/45-25 (N.J. appeal docketed May 8, 2026).....1

United States v. Collins,
427 F.3d 688 (9th Cir. 2005).....11

United States v. Comprehensive Drug Testing, Inc.,
621 F.3d 1162 (9th Cir. 2010) 17, 19

United States v. Dahlman,
13 F.3d 1391 (10th Cir. 1993) 23

United States v. Di Re,
332 U.S. 581 (1948).....5

United States v. Huggins,
299 F.3d 1039 (9th Cir. 2002) 23

United States v. Jones,
565 U.S. 400 (2012).....6, 13

United States v. Knotts,
460 U.S. 276 (1983).....7

United States v. Koerth,
312 F.3d 862 (7th Cir. 2002) 23

United States v. Leon,
468 U.S. 897 (1984)..... 20, 22, 23

United States v. Mayer,
503 F.3d 740 (9th Cir. 2007) 15

United States v. Moalin,
973 F.3d 977 (9th Cir. 2020) 14

United States v. Smith,
110 F.4th 817 (5th Cir. 2024) 2, 8, 9, 15

United States v. Stubbs,
873 F.2d 210 (9th Cir. 1989) 21

United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div.,
407 U.S. 297 (1972) 12

United States v. Vaughan,
718 F.2d 332 (9th Cir. 1983) 11

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 23

United States v. Yang,
958 F.3d 851 (9th Cir. 2020) 2

Verdun v. City of San Diego,
51 F.4th 1033 (9th Cir. 2022) 8

Ybarra v. Illinois,
444 U.S. 85 (1979) 10, 11, 12

Other Authorities

Brian L. Owsley, *Searching A Person's Thoughts: Keyword Search Warrants and Fourth Amendment Concerns*, 28 Stan. Tech. L. Rev. 66 (2025).....3

Ex. A to Motion to Suppress, *United States v. Spurlock*, 778 F. Supp. 3d 1136 (D. Nev. 2025), ECF No. 254-2.....14

Haley Amster & Brett Diehl, Note, *Against Geofences*, 74 Stan. L. Rev. 385 (2022).....2

Matthew Tokson & Michael Gentithes, *The Reality of the Good Faith Exception*, 113 Geo. L.J. 551 (2025) 21, 23

Note, *Geofence Warrants and the Fourth Amendment*, 134 Harv. L. Rev. 2508 (2021) 8

Orin S. Kerr, *Good Faith, New Law, and the Scope of the Exclusionary Rule*, 99 Geo. L. J. 1077 (2011) 24

Potter Stewart, *The Road to Mapp v. Ohio and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 Colum. L. Rev. 1365 (1983) 24

INTEREST OF *AMICI CURIAE*[1]

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. The ACLU of Nevada is a state affiliate of the ACLU. The ACLU and its affiliates have frequently appeared before the U.S. Supreme Court and other federal and state courts in numerous cases implicating Americans' right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 585 U.S. 296 (2018), and as *amici* in *Chatrie v. United States*, 609 U.S. 605 (2026), *Commonwealth v. Perry*, 184 N.E. 3d 745 (Mass. 2022), and *State v. Bryant*, No. A-43/44/45-25 (N.J. appeal docketed May 8, 2026).

The Electronic Frontier Foundation ("EFF") is a nonprofit civil liberties organization with more than 30,000 dues-paying members. Founded in 1990, EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law to technology. EFF regularly participates both as direct counsel and as *amicus* in the Supreme Court, this Court, and other state and federal courts in cases addressing the Fourth

---

[1] Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), counsel for *Amici Curiae* certifies that no person or entity, other than *Amici Curiae*, its members, or its counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. All parties to this case have consented to the filing of this *amici curiae* brief.

Amendment and its application to new technologies. *See*, *e.g.*, *Chatrie v. United States*, 609 U.S. 605 (2026); *People v. Meza*, 312 Cal. Rptr. 3d 1 (Cal. Ct. App. 2023); *United States v. Yang*, 958 F.3d 851 (9th Cir. 2020).

INTRODUCTION

Today's general searches look different than those of the colonial era. Instead of going door to door, physically searching every house in a neighborhood for evidence, modern police departments can simply tap into an "all-encompassing database," allowing them "to undertake nearly perfect, retrospective surveillance of countless persons and places." *Chatrie v. United States*, 609 U.S. 605, 629, 634 (2026). But the evil that a general warrant authorizes remains the same as ever: arbitrary invasions into individuals' privacy without probable cause.

Like the geofence warrant at issue in *Chatrie*, the tower-dump warrant in this case was just such a general warrant.[2] These types of warrants, sometimes referred to as "reverse warrants," "effectively 'work in reverse' from traditional search warrants." *United States v. Smith*, 110 F.4th 817, 822 (5th Cir. 2024) (quoting Haley Amster & Brett Diehl, Note, *Against Geofences*, 74 Stan. L. Rev. 385, 388 (2022)). They leverage massive databases of digital information to identify potential suspects when law enforcement has identified none. In other words, they are aimed at *finding*

[2] The Supreme Court held in *Chatrie* that the geofence warrant effected a search, and remanded for decision on the validity of the warrant. 609 U.S. at 637, 641. That question is currently before the Fourth Circuit.

probable cause with respect to a particular individual rather than proceeding on the basis of a probable cause finding in order to search someone's sensitive information.

The proliferation of personal, Internet-connected devices and the expansion of government and corporate surveillance have created fertile ground for these types of warrants to proliferate. These developments have created troves of sensitive, personal information capable of revealing, for example, everyone who was in the vicinity of a certain church, medical office, protest, or crime scene weeks or months in the past, *and* they have provided police with the technology to easily sift through that information.

The availability of this information has spurred police departments to experiment with various types of reverse warrants. For example, law enforcement has used reverse keyword search warrants to compel Google to produce records of all people who searched for a victim's name in the time leading up to a crime, in order to identify potential suspects. *See, e.g.*, Brian L. Owsley, *Searching A Person's Thoughts: Keyword Search Warrants and Fourth Amendment Concerns*, 28 Stan. Tech. L. Rev. 66, 72–73 (2025). Law enforcement has used reverse location warrants or "geofence warrants" to compel companies to produce records of all people who were in the area of a crime around the time of its commission. *See Chatrie*, 609 U.S. at 610. And, as illustrated in this case, law enforcement has used "tower-dump" warrants to compel cellular service providers to produce records of all people whose

devices connected to cell towers near a crime around the time of its commission in order to identify people who were in close proximity.

These reverse search techniques are appealing to law enforcement for the same reason that they are dangerous to the public: they leverage modern technology to scour vast numbers of people's information, obviating the need to develop probable cause before treating an innocent individual as a suspect and searching their private information.

As "'[s]ubtler and more far-reaching means of invading privacy have become available to the Government,'" courts are "obligated . . . to ensure that the 'progress of science' does not erode Fourth Amendment protections." *Id.* (quoting *Carpenter v. United States*, 585 U.S. 296, 320 (2018)). Preserving Fourth Amendment protections requires courts to recognize and reject modern reincarnations of general warrants. *Amici* respectfully submit that reverse search warrants, like the tower-dump warrant at issue here, are *per se* unconstitutional. At the very least, tower-dump warrants require safeguards to minimize their constitutional harms on innocent bystanders. Therefore, *Amici* urge the Court to uphold the lower court's ruling that the tower-dump warrant in this case was an unconstitutional general warrant, and to further hold that the good-faith exception cannot apply to the warrant at issue here. Importantly, this Court should decide the merits of the Fourth Amendment question regardless of its decision on the good-faith exception, in order to prevent future

unconstitutional searches and provide magistrates and law enforcement with necessary guidance.

ARGUMENT

I. Tower-Dump Warrants Are Unconstitutional General Warrants.

While tower-dump warrants "afford[] law enforcement a powerful new tool to carry out its important responsibilities," they also "risk[] Government encroachment of the sort the Framers, 'after consulting the lessons of history,' drafted the Fourth Amendment to prevent." *Carpenter*, 585 U.S. at 320 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). To "assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted," *id.* at 305 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)), this Court should hold that tower-dump warrants are general warrants and, as such, are *per se* unconstitutional.

A. Tower Dumps Are "Searches" Under the Fourth Amendment.

"[T]he Fourth Amendment must protect against 'every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed.'" *Chatrie*, 609 U.S. at 641 (quoting *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)). Eight years ago, the Supreme Court "decline[d] to grant the state unrestricted access to a wireless carrier's database of physical location information" in light of its "deeply revealing nature, . . . depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its

collection." *Carpenter*, 585 U.S. at 320. The Court held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell-site location information]," *id.* at 310, and that the Fourth Amendment requires the government to obtain a warrant in order to access "historical cell phone records that provide a comprehensive chronicle of the user's past movements." *Id.* at 300.

Earlier this year, the Supreme Court reaffirmed that "[w]here the Fourth Amendment applies, it applies—regardless of 'the quality or quantity of information' the government obtains." *Chatrie*, 609 U.S. at 629 (quoting *Kyllo*, 533 U.S. at 37). The Court held that police intrude on an individual's "reasonable expectation of privacy in records about his cell phone's location . . . when they demand the information—even though for only a limited time, and from a third-party tech company." *Id.* at 611.

The data acquired from tower dumps, like the data acquired from geofence searches, "allows officers to target one-off events of potential interest: a gun show, say, or a political rally." *Id.* at 629. Law enforcement's newfound ability to retrospectively search the records of every person who happened to be in a given location at a given time fundamentally alters the traditional "relationship between citizen and government in a way that is inimical to democratic society." *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (citation

omitted). "What in the past was 'unknowable'"—for example, everyone who had driven on a stretch of highway a month ago, or everyone in the vicinity of a certain church, medical office, or protest—"suddenly becomes open to view, presenting formerly unimaginable 'privacy concerns.'" *Chatrie*, 609 U.S. at 624 (quoting *Carpenter*, 585 U.S. at 311–12). There is no question that, when police demand that a third-party cellular service provider turn over (or "dump") location information for all phones in an area, they invade individuals' reasonable expectation of privacy and conduct a "search" within the meaning of the Fourth Amendment.

B. Tower-Dump Warrants Inherently Violate Bedrock Fourth Amendment Requirements.

Tower-dump warrants purport to authorize "dragnet type law enforcement practices" that threaten to upend constitutional protections. *United States v. Knotts*, 460 U.S. 276, 283–84 (1983). With tower-dump warrants, as with geofence warrants, "[p]olice officers need not decide in advance . . . who they want to follow and when." *Chatrie*, 609 U.S. at 624. Instead of developing probable cause to search a particular suspect, police simply treat *everyone in the area* as a suspect, compelling cellular service providers to hand over data exposing everyone's "comings and goings in any area." *Id.* at 607. "[W]herever a location of interest turns out to be (whether a crime scene or a protest march or even a private home)," the place and everyone in it "has effectively been surveilled for . . . boundless time." *Id.* at 626.

Indiscriminate surveillance is the precise evil that general warrants and writs of assistance inflicted on the colonists. "The general warrants of the colonial era 'allowed royal officials to search and seize whatever and whomever they pleased while investigating crimes or affronts to the Crown.'" *Verdun v. City of San Diego*, 51 F.4th 1033, 1046 (9th Cir. 2022) (quoting *Ashcroft v. al-Kidd*, 563 U.S. 731, 742 (2011)). For example, "writs of assistance" gave British officers "blanket authority to search where they pleased for goods imported in violation of the British tax laws"—an authority Revolutionary advocate James Otis called "the worst instrument of arbitrary power . . . because [it] placed the liberty of every man in the hands of every petty officer." *Stanford v. Texas*, 379 U.S. 476, 481 (1965) (citation modified). Thus, courts have long recognized that "no warrant 'can authorize the search of everything or everyone in sight.'" *Smith*, 110 F.4th at 836 (quoting Note, *Geofence Warrants and the Fourth Amendment*, 134 Harv. L. Rev. 2508, 2518 (2021)).

But tower-dump warrants do just that; they sweep up the data of any person with a cell phone who happened to be near the scene of a crime around when it was committed—even if there is no reason to believe they were involved. While the Supreme Court in *Chatrie*, after holding that geofence warrants effectuate a Fourth Amendment search, did not reach the question of whether they are unconstitutional general warrants, the Fifth Circuit has correctly held that geofence warrants are

"categorically prohibited by the Fourth Amendment" because they "*never* include a specific user to be identified, only a temporal and geographic location where any given user *may* turn up post-search." *Smith*, 110 F.4th at 837, 838 (footnoted omitted). They indiscriminately sweep in scores of people when "law enforcement officials have *no idea* who they are looking for, or whether the search will even turn up a result." *Id.* at 837. In other words, "[g]eofence warrants present the exact sort of 'general, exploratory rummaging' that the Fourth Amendment was designed to prevent." *Id.* (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)).

As the court below recognized, the tower-dump warrant at issue here is "materially indistinguishable from the geofence search warrant foreclosed by *Smith*." 1-ER-245 (quoting *In re Four Applications for Search Warrants Seeking Info. Associated with Particular Cellular Towers*, No. 3:25-CR-38-CWR-ASH, 2025 WL 603000, at *8 (S.D. Miss. Feb. 21, 2025) (hereinafter "*Four Applications I*"), *review denied sub nom. In re Four Applications for Search Warrants Seeking Info. Associated With Particular Cellular Towers*, No. 3:25-CR-38, 2026 WL 2260371 (S.D. Miss. Aug. 5, 2026) (hereinafter "*Four Applications III*")). The warrant here specified no suspect and ultimately led to the seizure of 1,686 people's private data. *Id.* It was "equivalent to a request for 'access to an entire haystack because it may contain a needle,'" *id.* (quoting *Four Applications I*, 2025 WL 603000, at *8), and constitutes "too permeating police surveillance," *id.*

While police use of tower dumps predates their use of geofence warrants, courts have only recently begun to recognize the severe constitutional implications of tower-dump warrants. Judge Reeves of the Southern District of Mississippi recently held that tower-dump warrants are *per se* unconstitutional, affirming Magistrate Judge Harris's earlier decisions holding the same. *Four Applications III*, 2026 WL 2260371, at *1; *In re Four Applications for Search Warrants Seeking Info. Associated with Particular Cellular Towers*, No. 3:25-CR-38-CWR-ASH, 2025 WL 1792841, at *3 (S.D. Miss. June 27, 2025) (hereinafter "*Four Applications II*"); *Four Applications I*, 2025 WL 603000, at *8. Judge Reeves recognized that "the emergence of digital surveillance has the potential to unleash the Founders' sincere fear" of general warrants. *Four Applications III*, 2026 WL 2260371, at *9 (citation omitted). And he recognized that tower-dump warrants "could produce thousands if not tens of thousands of cellular records," giving the government "unfettered access to the locations of an unknowable number of individuals" including in "highly-sensitive areas—homes, places of worship, and political centers." *Id.* at *10 (citing *Four Applications I*, 2025 WL 603000, at *6).

Moreover, almost half a century ago, the Supreme Court in *Ybarra v. Illinois* rejected the notion that warrants could authorize a search on the basis of mere propinquity to a suspect or crime—as tower-dump warrants do. 444 U.S. 85, 91 (1979). There, officers searched all people present in a tavern despite having

probable cause only with respect to the bartender. *Id.* at 88, 90. While the officers permissibly searched the bartender, they had "no authority whatever to invade the constitutional protections possessed individually by the tavern's customers," *id.* at 92 (footnote omitted), each of whom "was clothed with constitutional protection against an unreasonable search or an unreasonable seizure" when they walked into the tavern—the scene of the alleged crime, *id.* at 91.

Individuals going about their daily lives, using cell towers to communicate, are similarly clothed in constitutional protection against unreasonable, indiscriminate searches. Officers apply for tower-dump warrants when they know "nothing in particular about" any of the individuals whose records will be searched and seized, except their spatial and temporal proximity to a crime. *Id.* at 91. But "proximity and timing" are not enough to establish probable cause. *United States v. Collins*, 427 F.3d 688, 692 (9th Cir. 2005) (footnote omitted) (defendant's presence in a public parking lot that was under surveillance because officers had reason to believe that someone carrying stolen checks would show up there did not supply probable cause to arrest him); *see also United States v. Vaughan*, 718 F.2d 332, 335 n.7 (9th Cir. 1983) ("Persons detained during a search for evidence cannot be searched . . . simply because they are there."). Tower-dump warrants thus violate the requirement that probable

cause be "particularized with respect to that person," a requirement that "cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be." *Ybarra*, 444 U.S. at 91. Searching all people in an area without probable cause to believe they were all involved in the criminal activity under investigation reproduces the evils of general warrants and is not constitutionally permitted.

C. Tower-Dump Warrants Infringe on the Associational Privacy of Countless Innocent Bystanders.

The "unrestricted power of search and seizure" that tower-dump warrants grant law enforcement "could also be an instrument for stifling liberty of expression" and association. *Marcus v. Search Warrants of Prop. at 104 E. Tenth St.*, 367 U.S. 717, 729 (1961). Indeed, "[o]fficial surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech." *United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 320 (1972).

The Supreme Court has "long understood" that "implicit in the right to engage in [protected First Amendment] activities" is "a corresponding right to associate with others in pursuit of . . . political, social, economic, educational, religious, and cultural ends." *Roberts v. U.S. Jaycees*, 468 U.S. 609, 622 (1984) (citation omitted). The freedom to associate is "a right which, like free speech, lies

at the foundation of a free society," *Buckley v. Valeo*, 424 U.S. 1, 25 (1976) (citation omitted). But an "[a]wareness that the government may be watching chills associational and expressive freedoms." *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring). Thus, without freedom "from governmental oversight and intrusion, [] the freedom to associate may become no freedom at all." *First Choice Women's Res. Ctrs., Inc. v. Davenport*, 608 U.S. 174, 185–86 (2026); *see also NAACP v. State of Ala. ex rel. Patterson*, 357 U.S. 449, 462 (1958) (recognizing "the vital relationship between freedom to associate and privacy in one's associations").

Tower dumps threaten associational freedoms by providing the government with data on individuals' physical locations, and through them, "a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations." *Chatrie*, 609 U.S. at 629 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)); *see also Carpenter*, 585 U.S. at 320 (recognizing the "deeply revealing nature, . . . depth, breadth, and comprehensive reach" of the location information in a wireless carrier's database). For instance, a tower-dump warrant seeking records from cell towers near a meeting house around the time of a political meeting could reveal the members of a disfavored political organization. *Cf. NAACP*, 357 U.S. at 462–63 (finding that compelled disclosure of NAACP's membership list "may induce members to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown

through their associations and of the consequences of this exposure."). By the same principle, a tower dump could tie someone to a short-stay motel, a gay bar, a church service, a union meeting, a protest, and countless other locations that tend to reveal private, associational information. *See Chatrie*, 609 U.S. at 631 n.10 (noting that the geofence at issue included a nearby church).

The tower-dump warrant at issue here targeted all cell towers that cover the "immediate area" surrounding two highway mile-markers—one of which was 0.6 miles from a church, a hotel, and rural homes—at opposite ends of the town of Bridgeport along the major highway running through it. Ex. A to Mot. to Suppress 3, *United States v. Spurlock*, 778 F. Supp. 3d 1136 (D. Nev. 2025), ECF No. 254-2. The warrant also sought detailed communications records of people whose devices used the cell towers identified in the warrant, including the phone numbers of others they called and texted. *See id*. (requesting "phone numbers associated with any communications" that were supported by the towers at issue). These records would show if, for example, someone called their lawyer, sponsor, suicide hotline, or ex-partner. *See United States v. Moalin*, 973 F.3d 977, 992 (9th Cir. 2020) (discussing inferences that can be drawn from call records). And the records produced in this case did indeed expose the private information of more than 1,500 people whose associations would not otherwise have been subjected to government scrutiny in this manner. *See* 1-ER-244.

Tower dumps' tendency to infringe on associational freedoms requires that their constitutionality be carefully scrutinized. *See Smith*, 110 F.4th at 837 ("[W]hen these core [associational and expressive] rights are at issue, the warrant requirement must 'be accorded the most scrupulous exactitude.'" (quoting *Stanford*, 379 U.S. at 485)); *United States v. Mayer*, 503 F.3d 740, 747–48 (9th Cir. 2007) (integrating First Amendment concerns into the Fourth Amendment analysis where an investigation allegedly violates a third party's associational privacy rights). And given that tower-dump warrants provide the government with "a virtual panopticon with which to scrutinize its citizens' activities," *Chatrie*, 609 U.S. at 630, including the private associations of people who have no connection to the crime, and no knowledge of the collection, retention, or potential uses of their information for other purposes, the Court should hold that these warrants are *per se* unconstitutional.

II. If this Court Declines to Hold that Tower-Dump Warrants Are *Per Se* Unconstitutional, it Should Articulate Constitutional Limitations to Minimize their Harms to Suspects and Bystanders.

If this Court concludes that tower-dump warrants are not categorically prohibited under the Fourth Amendment, it should recognize that the Fourth Amendment at least requires safeguards to mitigate constitutional harms going forward. Appropriate safeguards can be gleaned from the Supreme Court's landmark opinion in *Berger v. New York*, which invalidated New York's eavesdropping statute because it enabled "general searches." 388 U.S. 41, 58 (1967). The *Berger* Court

found that eavesdropping "involves an intrusion on privacy that is broad in scope," *id.* at 56, as "conversations of any and all persons coming into the area covered by the device will be seized indiscriminately and without regard to their connection with the crime under investigation," *id.* at 59. The same is true of tower dumps. In order to minimize the harms that such broad intrusions inflict on suspects and innocent bystanders alike, several "protective procedures" are necessary. *Id.* at 60.

First, tower-dump warrants must strictly limit the scope and duration of the search. The towers from which law enforcement seeks data must be clearly specified and in close proximity to the sites of the crimes under investigation, and the time periods must be no longer than necessary to identify individuals present during the alleged crimes. The affidavits in support of tower-dump warrants must provide specific justification for the scope and duration of records sought. *See In re Application of the U.S.A. for an Ord. Pursuant to 18 U.S.C. 2703(c), 2703(d) Directing AT & T, Sprint/Nextel, T-Mobile, Metro PCS, Verizon Wireless*, 42 F. Supp. 3d 511, 519 (S.D.N.Y. 2014) (requiring the government to submit an amended tower-dump application providing "specific justification for the time period for which the records will be gathered"); *In re Search Information that is Stored at Premises Controlled by Google*, 542 F. Supp. 3d 1153, 1158 (D. Kan. 2021) (rejecting a geofence warrant application in part because the warrant failed to address the geofenced area's inclusion of a business unrelated to the alleged crime).

Second, tower-dump warrants should issue only in cases involving investigations of multiple temporally and geographically distinct crimes, and only where there is probable cause to believe those crimes were committed by the same cell phone user. *See Commonwealth v. Perry*, 184 N.E.3d 745, 767 (Mass. 2022) (noting a tower-dump affidavit "outlined significant similarities amongst the offenses then under investigation, and therefore afforded a substantial basis to believe that the offenses had been committed by the same individual"). The crime scenes must be geographically distant enough that they are served by different cell towers. Either the provider or a filter team that is walled off from the primary investigators should limit the records that the investigators examine to those of individuals appearing at all crime scenes. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1180 (9th Cir. 2010) (Kozinski, J., concurring) ("Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party."). Although it may appear incongruous to permit only multiple-crime tower dumps, which may sweep up more people initially, these searches will ultimately produce datasets that are smaller in size, more particularized, and more closely tied to probable cause.

Third, a tower-dump warrant must prohibit the use and retention of seized records that are irrelevant to the crime under investigation. The statute in *Berger* impermissibly left "full discretion in the officer as to the use of seized conversations

of innocent as well as guilty parties" *Berger*, 388 U.S. at 60. In a prescient 2012 opinion, Magistrate Judge Brian Owsley denied an application for a tower-dump order, in part because the government's application failed to address "the Fourth Amendment concerns of these innocent subscribers whose information will be compromised." *In re U.S. ex rel. Ord. Pursuant to 18 U.S.C. Section 2703(d)*, 930 F. Supp. 2d 698, 702 (S.D. Tex. 2012). Judge Owsley determined that "in order to receive such data, the Government at a minimum should have a protocol to address how to handle this sensitive private information." *Id.*; *accord In re Application of the U.S.A. for an Ord. Pursuant to 18 U.S.C. 2703(c), 2703(d) Directing AT & T, Sprint/Nextel, T-Mobile, Metro PCS, Verizon Wireless*, 42 F. Supp. 3d at 519; *In re U.S. ex rel. Ord. Pursuant to 18 U.S.C. Section 2703(d)*, 930 F. Supp. 2d at 702; *In re United States for an Ord. Pursuant To 18 U.S.C. §2703(d)*, No. 2:17-MC-51662, 2017 WL 6368665, at *2 (E.D. Mich. Dec. 12, 2017).

This Court should make clear that any tower-dump warrant must "include protocols for the prompt and permanent disposal of any and all data that does not fit within the object of the search following the conclusion of the prosecution." *Perry*, 184 N.E.3d at 770; *see also See In re Search of Cellular Tel. Towers*, 945 F. Supp. 2d 769, 771 (S.D. Tex. 2013) (ordering the government to "return any and all original records and copies, whether hardcopy or in electronic format or storage, to the Provider, which are determined to be not relevant to the Investigative Agency's

investigation"). And after executing a tower-dump warrant, the government must "not use further investigative steps" concerning tower-dump data irrelevant to the crime under investigation. *See Matter of Tower Dump Data for Sex Trafficking Investigation*, No. 23 M 87, 2023 WL 1779775, at *1 (N.D. Ill. Feb. 6, 2023).

Fourth, the government must provide notice to individuals whose information was swept up in the tower dump. *See Berger*, 388 U.S. at 60 (faulting eavesdropping statute for having "no requirement for notice" to affected individuals); *In re Search of Cellular Tel. Towers*, 945 F. Supp. 2d at 771 (requiring notification to subscribers that their records were provided to the government). Notice is crucial because tower dumps, like other types of digital searches, "expose exceedingly sensitive information about countless individuals not implicated in any criminal activity, who might not even know that the information about them has been seized and thus can do nothing to protect their privacy." *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1177.

Finally, tower-dump warrant returns must detail the number of devices for which data was seized, the number of those devices that were irrelevant to the investigation, and the estimated coverage area of each cell tower included in the data. This information will provide judges, lawmakers, and the public with insight into the invasiveness of these searches and whether additional safeguards are needed.

III. Evidence Obtained from the Tower-Dump Warrant Must Be Suppressed.

Law enforcement's surveillance capabilities are rapidly advancing, fueled by leaps in artificial intelligence that make data collection and analysis cheaper and easier than ever. Data from various sources can be aggregated and mined for sensitive, personal information—and retained indefinitely. Whereas collecting more data used to mean spending more time and resources on processing, sorting, and analyzing, now, it only means more granular, sensitive, and malleable insights. The incentives for law enforcement to conduct indiscriminate mass surveillance have therefore never been higher. Consequently, the value of the exclusionary rule in "deterring official misconduct and removing inducements to unreasonable invasions of privacy," *United States v. Leon*, 468 U.S. 897, 900 (1984), has never been greater.

In crafting the good-faith exception, the Court sought to "retain[] the value of the exclusionary rule as an incentive for the law enforcement profession as a whole to conduct themselves in accord with the Fourth Amendment." *Id.* at 919 n.20 (quoting *Illinois v. Gates*, 462 U.S. 213, 261 n.15 (1983) (White, J., concurring)). The Court adopted an objective standard so that officers would still be required "to have a reasonable knowledge of what the law prohibits." *Id.*

The law has long prohibited general warrants—the "immediate evils" that motivated the Fourth Amendment in the first place. *Payton v. New York*, 445 U.S. 573, 583 (1980). Thus, when it comes to tower dumps, the "database is new, but the

principle covering it is not." *Chatrie*, 609 U.S. at 641. Any reasonable officer understands that general searches—those that allow law enforcement to arbitrarily invade the privacy of scores of individuals without probable cause—have been unlawful since this Nation's founding. *See Riley v. California*, 573 U.S. 373, 403 (2014). A general warrant is necessarily "so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law." *Groh v. Ramirez*, 540 U.S. 551, 558 (2004) (citing *Leon*, 468 U.S. at 923); *see also United States v. Stubbs*, 873 F.2d 210, 212 (9th Cir. 1989) (declining to apply the good-faith exception where a warrant "merely described broad classes of documents without specific description of the items to be seized").

Applying the exclusionary rule here is not an indictment of the magistrate or officer in this case; it is the necessary course to preserve Fourth Amendment rights and deter future general searches. Otherwise, the good-faith exception serves as a "doctrinal 'loophole[]' . . . that easily permit[s] law enforcement to utilize new technologies without inquiring about the legality of their actions." *Four Applications III*, 2026 WL 2260371, at *4 n.8; *see also* Matthew Tokson & Michael Gentithes, *The Reality of the Good Faith Exception*, 113 Geo. L.J. 551, 553 (2025) (arguing that the good-faith exception "incentivizes investigators to employ novel surveillance tactics aggressively before courts can declare them unconstitutional").

The tower dump here violated the privacy of 1,686 individuals based on mere proximity to a crime. Next time, police might use a more advanced technology, a more novel technique, or a database ten times the size of the one here to gather intelligence about everyone near a suspected crime. Law enforcement cannot be permitted to escape the ban on general searches by conducting them with new tools. *See* Appellant's Opening Br. 24–28. Suppressing evidence in this case would result in "appreciable deterrence" of unconstitutional searches, *see Leon*, 468 U.S. at 909, by signaling to officers that general warrants are prohibited, regardless of the technology used to conduct them.

IV. The Court Should Decide the Underlying Fourth Amendment Issues Before Addressing the Good-Faith Exception.

This Court should not decide whether the good-faith exception applies until it has first determined whether the tower-dump warrant violated the Fourth Amendment. Proceeding in this order will provide law enforcement officers and magistrate judges with much-needed guidance, and guard against future unconstitutional searches.

"[T]he very decision establishing [the good-faith] exception" contemplated that courts could "'resolv[e] the Fourth Amendment issue' before the good-faith issue, either to better assess good faith or 'to guide future action by law enforcement officers and magistrates.'" *Chatrie*, 609 U.S. at 619 n.4 (quoting *Leon*, 468 U.S. at 925). Indeed, "a close reading of *Leon* reveals that, while the Supreme Court

intended to vest lower courts with discretion, the preferred sequence is to address the Fourth Amendment issues before turning to the good faith issue unless there is no danger of 'freezing' Fourth Amendment jurisprudence or unless the case poses 'no important Fourth Amendment questions.'" *United States v. Dahlman*, 13 F.3d 1391, 1397 (10th Cir. 1993) (quoting *Leon*, 468 U.S. at 924–25); *see also United States v. Koerth*, 312 F.3d 862, 866 (7th Cir. 2002) ("By resolving the issue of probable cause before addressing the question of good-faith reliance, we further the *Leon* Court's goal"); *United States v. Huggins*, 299 F.3d 1039, 1052 (9th Cir. 2002) (Fletcher, J., concurring) ("the majority errs in failing to make an explicit finding that no probable cause existed to issue the first warrant that authorized a thermal imaging search.").

When the good-faith exception is invoked without deciding the underlying constitutional question, it "stymie[s] development of Fourth Amendment law, and in doing so, . . . allow[s] law enforcement and the government to violate the Fourth Amendment." *Four Applications III*, 2026 WL 2260371, at *4 n.8 (citing Tokson & Gentithes, *supra*, at 553). As the Sixth Circuit has recognized, "[i]f every court confronted with a novel Fourth Amendment question were to skip directly to good faith, the government would be given *carte blanche* to violate constitutionally protected privacy rights." *United States v. Warshak*, 631 F.3d 266, 282 n.13 (6th Cir. 2010). "[P]olice officers might shift the focus of their inquiry from 'what does the

fourth amendment require?' to 'what will the courts allow me to get away with?'" Potter Stewart, *The Road to Mapp v. Ohio and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 Colum. L. Rev. 1365, 1403 (1983) (footnote omitted).

This Court's opinion on the constitutionality of tower-dump warrants is "necessary to guide future action by law enforcement officers and magistrates" and to ensure that constitutional rights remain protected as law enforcement techniques evolve. *See Gates*, 462 U.S. at 264, 265 n.18 (White, J., concurring) (citing *O'Connor v. Donaldson*, 422 U.S. 563 (1975)). While courts typically discuss the exclusionary rule's function with respect to police practices, "[a] failure by the appellate courts to accurately assess Fourth Amendment interests in the course of announcing the law has the same impact as the failure of the police to follow the law." Orin S. Kerr, *Good Faith, New Law, and the Scope of the Exclusionary Rule*, 99 Geo. L. J. 1077, 1090 (2011). Whether a constitutional violation arises from a police officer's own misunderstanding or irreverence for constitutional rights, or insufficient guidance from the courts as to which police practices are unconstitutional, constitutional rights are left unprotected and more readily violated in the future. Thus, regardless of the Court's ruling on the good-faith exception, the Court should hold that the magistrate's issuance of the tower-dump warrant in this case was in error.

CONCLUSION

As law enforcement's surveillance capabilities increase, the foundational principles of our constitution must hold firm. *Amici* urge the Court to hold that tower dumps are modern general searches that are *per se* unconstitutional and cannot be saved by the good-faith exception.

Dated: November 3, 2026

Respectfully submitted,

/s/ Laura Moraff

Laura Moraff
Kiran Wattamwar
Nathan Freed Wessler
Brett Max Kaufman
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
lauramoraff@aclu.org

Andrew Crocker
Jennifer Lynch
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
andrew@eff.org

Christopher M. Peterson
American Civil Liberties Union of Nevada
4362 W. Cheyenne Ave.
North Las Vegas, NV 89032

(702) 366-1226
peterson@aclunv.org

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this third day of November, 2026, the foregoing brief of *Amici Curiae* American Civil Liberties Union, American Civil Liberties Union of Nevada, and the Electronic Frontier Foundation was filed electronically through the Court's ACMS system. Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system.

Dated: November 3, 2026

/s/ Laura Moraff
Laura Moraff

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 26-689

I am the attorney or self-represented party.

This brief contains 5,815 **words,** including 0 words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- ○ complies with the word limit of Cir. R. 32-1.
- ○ is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ◉ is an **amicus** brief and complies with the word limit of FRAP 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ○ is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ○ complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
  - ☐ it is a joint brief submitted by separately represented parties.
  - ☐ a party or parties are filing a single brief in response to multiple briefs.
  - ☐ a party or parties are filing a single brief in response to a longer joint brief.
- ○ complies with the length limit designated by court order dated ____.
- ○ is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/ Laura Moraff **Date** November 3, 2026

(use "s/[typed name]" to sign electronically-filed documents)