COMMONWEALTH OF MASSACHUSETTS

Supreme Judicial Court

No. SJC-13144

COMMONWEALTH,
RESPONDENT-APPELLEE,

v.

JERRON PERRY
PETITIONER-APPELLANT.

ON INTERLOCUTORY APPEAL FROM AN ORDER OF THE SUFFOLK SUPERIOR COURT

BRIEF AMICUS CURIAE OF THE AMERICAN CIVIL LIBERTIES UNION, THE AMERICAN CIVIL LIBERTIES UNION OF MASSACHUSETTS, INC., THE COMMITTEE FOR PUBLIC COUNSEL SERVICES, THE ELECTRONIC FRONTIER FOUNDATION, AND THE MASSACHUSETTS ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF THE DEFENDANT & REVERSAL OF THE DENIAL OF THE MOTION TO SUPPRESS

Matthew R. Segal (BBO 654489)
Jessie J. Rossman (BBO 670685)
Jessica J. Lewis (BBO 704229)
American Civil Liberties Union Foundation of Massachusetts, Inc.
211 Congress Street
Boston, MA 02110
(617) 482-3170
msegal@aclum.org
jrossman@aclum.org
jlewis@aclum.org

Nathan Freed Wessler (BBO 680281)
Brett Max Kaufman (on the brief)
Ashley Gorski (on the brief)
Patrick Toomey (BBO 673928*)
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
nwessler@aclu.org
bkaufman@aclu.org
agorski@aclu.org
ptoomey@aclu.org

Counsel continued on next page

Jennifer Granick (on the brief)
American Civil Liberties
Union Foundation
39 Drumm Street
San Francisco, CA 94111
(415) 343-0758
jgranick@aclu.org

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

Matthew Spurlock (BBO 601156)
Committee for Public Counsel
Services, Public Defender Division
75 Federal Street
Boston, MA 02110
(617) 482-6212
mspurlock@publiccounsel.net

Joshua M. Daniels (BBO 673034)
Law Office of Joshua M. Daniels
P.O. Box 300765
Jamaica Plain, MA 02130
(617) 942-2190
jdaniels@danielsappeals.com

* *Inactive status in Massachusetts*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Constitutional Provisions

Other Authorities

CORPORATE DISCLOSURE STATEMENT

Pursuant to Supreme Judicial Court Rule 1:21, the American Civil Liberties Union of Massachusetts, Inc. (ACLUM) and the Electronic Frontier Foundation (EFF) represent that they are a 501(c)(3) organization under the laws of the Commonwealth of Massachusetts. The American Civil Liberties Union (ACLU) is a District of Columbia non-profit membership organization and 501(c)(4) organization. The Massachusetts Association of Criminal Defense Lawyers (MACDL) represents that it is a 501(c)(6) organization under the laws of the Commonwealth of Massachusetts. ACLU, ACLUM, EFF, and MACDL do not issue any stock or have any parent corporation, and no publicly held corporation owns stock in ACLU, ACLUM, EFF, or MACDL.

The Committee for Public Counsel Services (CPCS) is a statutorily created agency established by G.L. c. 211D, § 1.

PREPARATION OF AMICUS BRIEF

Pursuant to Appellate Rule 17(c)(5), amici and their counsel declare that:

(a) no party or party's counsel authored this brief in whole or in part;

(b) no party or party's counsel contributed money to fund preparing or submitting the brief;

(c) no person or entity other than the amici curiae contributed money that was intended to fund preparing or submitting a brief; and

(d) counsel has not represented any party in this case or in proceedings involving similar issues, or any party in a case or legal transaction at issue in the present appeal.

INTRODUCTION AND SUMMARY OF ARGUMENT

To identify a single suspect, the Commonwealth obtained private information about, and the property of, tens of thousands of people. It did so by requesting historical cell site location information (CSLI) of all individuals whose phones connected to several cell-phone towers during designated periods of time, a technique known as a "tower dump." This electronic dragnet is a fundamentally new and invasive technology that evades longstanding practical barriers to sweeping police surveillance. Even data from a single cell phone tower can reveal presence inside the home or a place of worship, at a protest or political rally, or coming and going from a hospital—not just for one individual, but for *everyone* with a phone who was present within the requested period of time.

This kind of data-mining is a search that triggers constitutional protections. Tower dumps reveal retrospective, comprehensive, and invasive information that police could never have amassed before the cell-phone age. (pp. 11–16). They also intrude on tens of thousands of people's property rights in their cell-phone location records. (pp. 16–20). By collecting information otherwise unknowable through traditional surveillance techniques and interfering with people's property interests

in their digital "papers," tower dumps constitute searches and seizures under art. 14 of the Massachusetts Declaration of Rights and the Fourth Amendment to the U.S. Constitution.

The extraordinary breadth of tower dumps renders them general searches that no warrant can constitutionally sanction. Article 14 and the Fourth Amendment were adopted mainly as responses to the general warrants and writs of assistance that authorized unconstrained searches of private places, papers, and effects without probable cause and without particularly describing the place to be searched. *See, e.g.*, *Stanford v. Texas*, 379 U.S. 476, 481–85 (1965); *Commonwealth v. Rodriguez*, 430 Mass. 577, 585–86 (2000). Because a tower dump necessarily sweeps up information about troves of people with no connection to the crime under investigation, a warrant purporting to authorize such collection is void as a general warrant. (pp. 22–27).

But even assuming some tower dump requests can pass constitutional muster—which they cannot—their scope and execution must be limited. In considering another novel and intrusive surveillance technique, the U.S. Supreme Court held that wiretapping warrants must include strict minimization procedures to avoid exploiting the private information of people not suspected of committing crimes. *See Berger v. New York*, 388 U.S. 41 (1967). At a minimum, tower dumps

require similar protections in order to mitigate the risk that they become a tool of abusive government power. (pp. 27–33).

STATEMENT OF INTEREST OF AMICI

The American Civil Liberties Union of Massachusetts (ACLUM) and the American Civil Liberties Union (ACLU) are membership organizations dedicated to the principles of liberty and equality embodied in the constitutions and laws of the Commonwealth and the United States. The rights they defend through direct representation and amicus briefs include the right to be free from unreasonable searches and seizures.

The Committee for Public Counsel Services (CPCS), Massachusetts's public defender agency, is statutorily mandated to provide counsel to indigent defendants in criminal proceedings. G.L. c. 211D, § 5. The rights that CPCS defends through direct representation and amicus briefs include the right to be free from unreasonable searches and seizures. The issue addressed in this case will affect numerous indigent defendants whom CPCS attorneys are appointed to represent.

The Electronic Frontier Foundation ("EFF") is a member-supported, nonprofit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for over thirty years. EFF represents technology users' interests in court cases and broader policy debates. EFF has

served as amicus in numerous cases addressing Fourth Amendment protections for technologies that involve location tracking.

The Massachusetts Association of Criminal Defense Lawyers (MACDL), the Massachusetts affiliate of the National Association of Criminal Defense Lawyers, is an incorporated association representing more than 1,000 experienced trial and appellate lawyers of the Massachusetts Bar who focus a substantial part of their practices on criminal defense. MACDL devotes much of its energy to identifying, and seeking to avoid or correct, problems in the Commonwealth's criminal justice system, including by filing amicus briefs in cases raising questions central to the administration of justice.

ARGUMENT

Cell phones have become "such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society." *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (quotation marks and citation omitted). The ability of law enforcement to readily access sensitive digital data generated by cell phones has now ballooned. As this Court knows, historical CSLI allows police to track a known individual's past movements. *See Commonwealth v. Augustine*, 467 Mass. 230 (2014). But police can also identify every previously unknown cell-phone user in the range of a cell tower during a designated time frame by seeking

all of the cell-tower records from that period, a form of collection also known as a tower dump.

Tower dumps provide police with an unprecedented investigatory power. If police want to know who was near the scene of an alleged crime—months or even years later[1]—cell tower data can turn back the clock and allow them to surveil the past.[2] Moreover, it is not clear how long police retain the information once they receive it, or whether it is ever deleted.[3]

Each tower dump exposes thousands of people to law enforcement's eye, an impact that multiplies with the number of tower dump requests issued each year. And tower dumps are not used sparingly. T-Mobile alone, for example, received more than 12,000 requests for tower dumps during 2020.[4] This scrutiny is not equitably distributed. Members of low-income, politically disenfranchised

---

[1] Providers keep tower records for a long time—up to seven years for AT&T. Joseph Cox, *Here's the FBI's Internal Guide for Getting Data from AT&T, T-Mobile, Verizon*, Motherboard (Oct. 25, 2021), https://www.vice.com/en/article/m7vqkv/how-fbi-gets-phone-data-att-tmobile-verizon [https://perma.cc/UE82-S23R].

[2] *See* FBI Cellular Analysis Survey Team, *Cellular Analysis & Geo-Location Field Resource Guide* 4 (Mar. 2019), available at https://propertyofthepeople.org/document-detail/?doc-id=21088576 [https://perma.cc/4SSU-9GCH].

[3] *Id.* at 60.

[4] T-Mobile, Inc., *Transparency Report for 2020* 6, https://www.t-mobile.com/news/_admin/uploads/2021/07/2020-Transparency-Report.pdf [https://perma.cc/MU2D-T27C].

communities of color—who often live in densely populated areas—will bear the brunt of these mass, suspicionless examinations of their private location data. *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 348–50 (4th Cir. 2021) (Gregory, C.J., concurring) (en banc).

As explained below, such electronic dragnets are comparable to unconstitutional general searches, which can never be authorized. Alternatively, at a minimum, these searches must be subject to strict minimization procedures.

I. Tower dumps trigger art. 14 and Fourth Amendment protections.

A. A tower dump is a search because it violates an objectively reasonable expectation of privacy by providing the government access to private information that would have been unknowable prior to the cell-phone age.

To ensure that technology does not erode the "degree of privacy against government that existed when the Fourth Amendment" and art. 14 were adopted, *Carpenter*, 138 S. Ct. at 2214, both this Court and the United States Supreme Court have held that the use of technology to collect information effectively unknowable through traditional techniques triggers constitutional protections, *see id*. at 2217, 2218; *Commonwealth v. Almonor*, 482 Mass. 35, 46 (2019); *Commonwealth v. Mora*, 485 Mass. 360, 372, 374 (2020). As Justice Alito explained in *United States v. Jones*, because "[i]n the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical," technologies that allow easy evasion of those practical limits require constitutional

regulation. 565 U.S. 400, 429 (2012) (Alito, J., concurring in the judgment); *accord Mora*, 485 Mass. at 374 (requiring warrant under art. 14 when new technology "eliminated resource constraints that otherwise may have rendered this surveillance unfeasible"). In other words, art. 14 and the Fourth Amendment apply to technology that allows police to gather "a category of information that *never* would be available through the use of traditional law enforcement tools of investigation." *Augustine*, 467 Mass. at 254.

There is little question that tower dumps are such a technology. Police have never before had the capability to call up a near-perfect record of virtually *every* person who was in a particular area at a particular time, months or years earlier, including inside homes and other constitutionally protected spaces. Tower dumps therefore "grant[] police unfettered access 'to a category of information otherwise unknowable.'" *Almonor*, 485 Mass. at 46 (quoting *Carpenter*, 138 S. Ct. at 2218).

First, tower dumps allow for "continuous, tireless, effortless, and absolute surveillance," whose comprehensiveness has no precedent in traditional surveillance techniques. *See Commonwealth v. McCarthy*, 484 Mass. 493, 500 (2020); *see also Carpenter*, 138 S. Ct. at 2218, 2223 (holding that the collection of historical CSLI violated an objectively reasonable expectation of privacy in part due to the "depth, breadth, and comprehensive reach" and "the inescapable and automatic nature of its collection"). As with GPS tracking of cars, long-term

collection of an individual's cell-site location information, and long-term pole camera surveillance of the home, "it is almost impossible to think of late–18th-century situations that are analogous" to tower dumps. *Mora*, 485 Mass. at 374 (quoting *Jones*, 565 U.S. at 420 (Alito, J., concurring in the judgment)). A government could never deploy enough police officers or informants to obtain the information it can easily acquire through a tower dump. To capture every person's whereabouts within range of a cell tower would be practically impossible, prohibitively expensive, and inconsistent with basic freedoms in a democratic society. *Cf.* Hannah Arendt, *Origins of Totalitarianism* 431 (1968) (discussing corrosive effects of "a system of ubiquitous spying where everybody may be a police agent and each individual finds himself under constant surveillance"). And "this newfound tracking capacity runs against everyone," *Carpenter*, 138 S. Ct. at 2218, since people cannot reasonably avoid their CSLI being logged, *Augustine*, 467 Mass. at 250.

Second, the breadth of a tower dump's reach is amplified by "the retrospective quality" of the data, which likewise implicates objectively reasonable expectations of privacy. *Carpenter*, 138 S. Ct. at 2218. "The ability of the government to know where anyone is at any moment poses a profound threat to the right to be let alone. . . . To know that the government can find you, anywhere, at any time is—in a word—'creepy.'" *Almonor*, 482 Mass. at 55 (Lenk, J.,

concurring). This is particularly so when the government can pluck tens of thousands of people's whereabouts *from the past*.

Third, tower dumps are deeply revealing because even a small number of location data points facilitates inferences about individuals' habits of life. The data can disclose the location of individuals (including, necessarily, non-suspects) in non-public and constitutionally sensitive places, such as the home, doctor's office, protest, or place of worship. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2218 ("A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."); *United States v. Karo*, 468 U.S. 705, 715 (1984) (Fourth Amendment protects against warrantless electronic tracking that locates a person in their home, especially when such presence "could not have been visually verified" by police). *Contra* Motion Judge's Order at 8 (Def. Br. Add. at 64) (stating, without support in the record, that tower dumps in this case "did not involve intruding into any non-public space"). Police can also use tower-dump data to identify relationships between people where, as here, the call detail records include "source and destination numbers" associated with any communication that occurred in the vicinity. Com. Br. at 39 (citing ICA at 23–24). As a result, tower dumps can identify the friends, family, and other intimate associates of the thousands of people caught up in the sweep. *Cf. Mora*, 485 Mass. at 372 (noting that whether a

surveillance technique triggers art. 14 protections depends on whether it reveals, "by easy inference," "a highly detailed profile . . . of our associations" (quotation marks and citation omitted)). And contrary to the suggestion of the trial court, *see* Motion Judge's Order at 9 (Def. Br. Add. at 65), the anonymization of the records obtained here offers no real privacy protection. Law enforcement can easily identify people in the records by issuing an administrative subpoena to the service provider seeking names and other subscriber data, *see* 18 U.S.C. § 2703(c)(2), or by querying databases that already contain that information.

Despite the many ways in which tower dumps provide information traditionally unknowable to police, the Commonwealth argues that no search occurred here under this Court's *Estabrook* decision. *See* Com. Br. at 20–26 (citing *Commonwealth v. Estabrook*, 472 Mass. 852, 854 (2015)). But *Estabrook* did not address tower dumps, and its holding does not govern here. *Estabrook* held that police need not obtain a warrant when they seek six or fewer hours of historical telephone-call CSLI for a *single, identified number*. 472 Mass. at 858 & n.12. A tower dump, by contrast, is a mass intrusion that, as here, may well affect *tens of thousands of people* not suspected of any wrongdoing. This fundamental difference between the technology and scope of the search at issue in *Estabrook* and tower dumps is constitutionally significant.

Tower dumps can identify virtually *all* people near an identified point of interest—something law enforcement could never achieve through visual surveillance—with nothing more than a request to the cell-service provider from the officer's desk. And since tower dumps are a mass-surveillance technique, to accurately capture the invasion of privacy, the duration of the surveillance must be multiplied by the number of people impacted. This Court has already highlighted concerns about "the duration of digital surveillance drastically exceed[ing] what would have been possible with traditional law enforcement methods." *McCarthy*, 484 Mass. at 500. Even if collecting a few data points about one person's location when making or receiving calls is not a search, *see Estabrook*, 472 Mass. at 858, collecting the same amount of data about hundreds, thousands, or tens of thousands of people is a different category of privacy harm that triggers constitutional protections.

B. Tower dumps are searches and seizures because they implicate cell-phone users' property rights.

Tower dumps separately trigger constitutional protections because they invade cell-phone users' property rights.[5] Although searches are often properly analyzed under the reasonable-expectation-of-privacy framework, the "reasonable-

[5] If this Court properly holds that a search occurred under the reasonable-expectation-of-privacy framework, it need not address whether a search independently occurred under the property framework.

expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test" for searches and seizures. *Jones*, 565 U.S. at 409. Under that test, when the government interferes with a person's possessory rights in order to obtain information, a search has occurred. *Id.* at 404–05; *accord Florida v. Jardines*, 569 U.S. 1, 5 (2013). Likewise, a seizure occurs when one's property rights are violated, even if the property is never searched. *Soldal v. Cook Cty.*, 506 U.S. 56, 62–64, 68 (1992); *see also Commonwealth v. Connolly*, 454 Mass. 808, 822–23 (2009) (installation of tracking device on vehicle and monitoring that device without consent "constituted a seizure under art. 14").

Digital records can be a person's "papers" no less than physical documents. *E.g.*, *Commonwealth v. Fulgiam*, 477 Mass. 20, 33 (2017) (warrant required for digital text messages); *United States v. Wurie*, 728 F.3d 1, 14 (1st Cir. 2013), *aff'd sub nom. Riley v. California*, 573 U.S. 373 (2014). And a person can retain constitutional protection of their papers or effects even when those items are in another's possession, as is often true of electronic communications. *See, e.g.*, *Ex parte Jackson*, 96 U.S. 727, 733 (1878) (sealed letters in possession of postal service); *Fulgiam*, 477 Mass. at 33 (text messages in possession of service provider). The relevant question, then, is whether people hold enough of a property interest in their CSLI that it remains at least in part their "papers" under art. 14 and the Fourth Amendment, even though held by the cell-phone company.

They do. Possessory interest is defined as the "right to control property, *including the right to exclude others*." Black's Law Dictionary (11th ed. 2019) (emphasis added); *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435 (1982) ("The power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights."). Property rights need not be exclusive to be effective, and a person can retain significant property rights in an item or location even if another entity holds equivalent or additional rights. *E.g.*, *Jones*, 565 U.S. at 404 n.2 (recognizing that a bailee of property has sufficient property rights for Fourth Amendment purposes).

Determining whether the government has interfered with the security of one's papers or effects within the meaning of the art. 14 or the Fourth Amendment requires assessing a person's property rights in those items, including by reference to common-law trespass and property principles, *see id.* at 404–05 & n.2, or positive law (i.e., statutes, regulations, and similar enactments), *see Carpenter*, 138 S. Ct. at 2270 (Gorsuch, J., dissenting); *State v. Wright*, 961 N.W.2d 396, 415–17 (Iowa 2021) (relying on municipal ordinance to hold that police seizing and examining garbage is a trespassory search that requires a warrant under the state constitution).[6] When the law protects against access by the public without consent,

[6] *See also* William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv. L. Rev. 1821 (2016).

unreasonable access by the government is prohibited as well. *Carpenter*, 138 S. Ct. at 2270–71 (Gorsuch, J., dissenting); *Wright*, 961 N.W.2d at 417.

Positive law establishes the relevant property interests in the CSLI at issue here. The federal Telecommunications Act requires "express prior authorization of the customer" before a service provider can "use or disclos[e] . . . call location information," 47 U.S.C. § 222(f), and provides "customers a private cause of action for damages against carriers who violate the Act's terms," *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting) (citing 47 U.S.C. § 207). The Act also designates location information as "customer proprietary network information" ("CPNI")—a category of records that the service provider cannot disclose without "approval of the customer." 47 U.S.C. § 222(c)(1)–(2), (h)(1)(A). As the Federal Communications Commission explains, location information "clearly qualifies as CPNI," and therefore subjects service providers to "a duty to protect [its] confidentiality." *In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 28 FCC Rcd. 9609, 9616 ¶ 22, 9619 ¶ 29 (2013). And "to the extent CPNI is property, . . . it is better understood as belonging to the customer, not the carrier." *Second Report & Order and Further Notice of Proposed Rulemaking, In re Implementation of the Telecommunications Act of 1996*, 13 FCC Rcd. 8061 ¶ 43 (1998), *vacated on other grounds by U.S. West, Inc. v. F.C.C.*, 182

F.3d 1224 (10th Cir. 1999). When carriers have violated these provisions by denying customers the right to control others' access to their location information, they have been subject to aggressive enforcement actions by the FCC and to private suits.[7]

Given these protections, "customers have substantial legal interests in this information, including at least some right to include, exclude, and control its use." *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting). In other words, individuals have a property right in their cell phone location records, making those records "their" papers for purposes of art. 14 and the Fourth Amendment. Where, as here, the government seeks access to those papers, it effects both a search and seizure requiring a warrant.[8]

---

[7] *See, e.g.*, Jennifer Valentino-DeVries, *Cellphone Carriers Face $200 Million Fine for Not Protecting Location Data*, N.Y. Times (Feb. 28, 2020), https://www.nytimes.com/2020/02/28/technology/fcc-cellphones-location-data-fines.html [https://perma.cc/R6LP-YY8T]. In addition, the federal Communications Assistance for Law Enforcement Act, which otherwise requires phone companies to build lawful interception and surveillance capabilities into their networks, prohibits use of the federal pen register statute to "obtain any information that may disclose the physical location of the subscriber['s cell phone]." 47 U.S.C. § 1002(a)(2).

[8] Under the property-based approach, a request for even one data point in which a person has a property interest is a search and seizure. Thus, finding a search under the property-based approach does not hinge on the duration or breadth of the data requested.

C. Tower dumps implicate concerns at the very core of art. 14 and the Fourth Amendment.

Tower dumps expand police power in the manner prohibited by the federal and state constitutions. The ability of government "to target any home, at any time, for any reason" is what "spurred John Adams to draft art. 14 more than two hundred years ago, and raises the spectre of the Orwellian state today." *Mora*, 485 Mass. at 372 (internal quotation marks omitted). To prevent such abuse, the federal and state constitutions secure "the privacies of life" against "arbitrary power" and "place obstacles in the way of a too permeating police surveillance." *Carpenter*, 138 S. Ct. at 2214.

The Commonwealth's bid to exclude altogether this powerful surveillance technique from constitutional protection, *see* Com. Br. at 17–26, would leave the people's privacy interests "at the mercy of advancing technology." *Kyllo v. United States*, 533 U.S. 27, 35 (2001). That approach is directly contrary to this Court's and the U.S. Supreme Court's decisions in the digital age. As Justice Gorsuch recognized in his *Carpenter* dissent, tower dumps are the "*paradigmatic* example of 'too permeating police surveillance' and a dangerous tool of 'arbitrary' authority . . . On what possible basis could such mass data collection survive the Court's test while collecting a single person's data does not?" 138 S. Ct. at 2267 (Gorsuch, J., dissenting).

What is more, art. 14 and the Fourth Amendment have long been held to regulate technologies that enable dragnet, bulk surveillance. *E.g.*, *United States v. Knotts*, 460 U.S. 276, 283–84 (1983) (If "dragnet type law enforcement practices . . . should eventually occur," then "different constitutional principles may be applicable."). Tower dumps trigger these exact concerns. Although the police obtained warrants here, the Commonwealth now claims that police do *not* need a warrant to obtain tower-dump data. Under that approach, police could identify congregants at a place of worship, immigrant students attending a know-your-rights training, or activists at a protest, all without any judicial oversight or probable-cause requirement.[9] To protect against these privacy invasions and arbitrary abuses, this Court should hold, as the Superior Court did, that tower dumps are searches and/or seizures under art. 14 and the Fourth Amendment.

II. Tower dumps are unconstitutional general searches.

This Court's review of the case should be informed by the similarities between tower dumps and general warrants. This Court has previously found police practices to be unconstitutional when they sweep up information that is

[9] For example, into 2014, the Ukrainian government reportedly used tower dumps to figure out who attended an anti-government protest. Andrea Peterson, *Ukraine's 1984 Moment: Government Using Cellphones to Track Protesters*, Wash. Post (Jan. 21, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/01/21/ukraines-1984-moment-government-using-cellphones-to-track-protesters/ [https://perma.cc/34VU-8LHV].

overbroad and lacks particularity. *See, e.g.*, *Commonwealth v. Yusuf*, 488 Mass. 379, 394 (2021) (permitting police to "trawl through [body-worn camera] footage to look for evidence of crimes unrelated to the officers' lawful presence in the home when they are responding to a call for assistance is the virtual equivalent of a general warrant"). Tower dumps are likewise inherently unreasonable because they constitute bulk surveillance of many people without probable cause to believe that most of those affected have committed, or have evidence related to, a crime. Tower-dump warrants also leave to the officers' discretion how to manage the vast trove of private (but irrelevant) information that the government obtains. No valid warrant can issue to authorize such electronic dragnets. *See* Def. Br. at 22–49.

Article 14 and the Fourth Amendment "were enacted, in large part, in response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Mora*, 485 Mass. at 370 (some internal quotation marks omitted). These instruments allowed officials to look everywhere without requiring any showing of a close connection to the crime. For centuries before the U.S. founding, English jurists and legal scholars rejected writs of assistance and general warrants as the worst exercise of tyrannical power. *See id.* at 370 n.11.

Although at the time of the founding it would have been inconceivable that police could trawl through databases revealing the locations of nearly every person to identify a suspect, the Founders were well aware of—and rejected—the ability of law enforcement to search every house, or examine all goods, to look for evidence. *See id.* "Article 14, like the Fourth Amendment, was intended by its drafters not merely to protect the citizen against the breaking of his doors, and the rummaging of his drawers, . . . but also to protect Americans in their beliefs, their thoughts, their emotions and their sensations by conferring, as against the government, the right to be let alone." *Id.* at 371 (quoting *Commonwealth v. Blood*, 400 Mass. 61, 69 (1987)). By infringing on these interests en masse, tower dumps run head-on into constitutional prohibitions on general warrants.

To begin, tower-dump warrants are overbroad because they necessarily compel disclosure of the location information for hundreds or thousands of phone numbers, allowing police to track a myriad of individuals with no connection to the crime under investigation. For example, in one of the earliest known tower-dump cases, the FBI sought four tower dumps that reportedly returned the location information for *150,000 people*.[10] The two tower-dump warrants in this case

[10] Ellen Nakashima, *Agencies Collected Data on Americans' Cellphone Use in Thousands of 'Tower Dumps'*, Wash. Post (Dec. 9, 2013) https://www.washingtonpost.com/world/national-security/agencies-collected-data-

sought the unique identities of all cell phones communicating with the closest cell sites to seven different incidents, over an aggregated three hours, and ultimately revealed the location of tens of thousands of cell phone users.

Even tower dumps that sweep in far fewer innocent people are irremediably overbroad. The government knows that most people swept up in a tower dump are uninvolved in any crime under investigation. Law enforcement can therefore never establish a sufficient nexus between hundreds or thousands of people's private information and the alleged offense. The pre-digital analog, a government agent examining documents or searching houses based on mere proximity to a crime scene, would never have been accepted at the time art. 14 or the Fourth Amendment were adopted. As this Court has made clear, a warrant authorizing the search of any person present "can only be valid where the underlying circumstances presented to the issuing judge or clerk clearly demonstrate probable cause . . . to believe that *all* persons present are involved in the criminal activity afoot." *Commonwealth v. Smith*, 370 Mass. 335, 344 (1976) (emphasis added); *see also Commonwealth v. Brown*, 68 Mass. App. Ct. 261 (2007) (same).[11]

---

on-americans-cellphone-use-in-thousands-of-tower-dumps/2013/12/08/20549190-5e80-11e3-be07-006c776266ed_story.html [https://perma.cc/Q5WL-6NB7].

[11] *Accord Ybarra v. Illinois*, 444 U.S. 85, 86 (1979) ("[A] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person."); *Berger*, 388 U.S. at 59 (decrying wiretapping of "conversations of any and all persons coming into

Tower-dump warrants cannot meet this standard. The Commonwealth argues that it has probable cause to believe that the comparison of records from multiple towers will reveal the perpetrator's identity if there is evidence that the same individual committed each crime. Com. Br. at 32. That may be a reason to believe that the suspect's data will be included in the CSLI records. But it does not supply probable cause for the thousands of innocent people whose information is also caught in the dragnet.

Nor are tower-dump warrants sufficiently particularized. Warrants must "both define[] and limit[] the scope of the search and seizure." *Commonwealth v. Balicki*, 436 Mass. 1, 8 (2002). "Just as police are not permitted to rummage unrestrained through one's home, so too constitutional safeguards prevent warrantless rummaging through the complex digital trails and location records created merely by participating in modem society." *McCarthy*, 484 Mass. at 499. Tower-dump warrants leave it to the officers' discretion how to search, use, share, and store this sensitive information.

The Commonwealth argues that the tower-dump warrants in this case specifically described what authorities sought to search (multiple cell towers), and what they sought to seize (call detail records from defined windows of time). Com.

---

the area covered by the [eavesdropping] device . . . without regard to their connection with the crime under investigation").

Br. at 39. But the warrants were insufficiently particular in describing the *specific* records sought, namely, those of the specific suspect. As a result, law enforcement obtained *all* of the tens of the thousands of records, and left officers to make their own discretionary decisions about how to analyze and retain them.

Finally, the Commonwealth argues that there was no less invasive means to obtain this information. But that is not, and cannot, be a justification for a general search. Even "if the government can identify th[e] wrongdoer only by sifting through the identities of unknown innocent persons without probable cause and in a manner that allows officials to 'rummage where they please in order to see what turns up,'" courts cannot constitutionally permit such a practice. *In re Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 757 (N.D. Ill. 2020).

III. Even assuming that tower-dump warrants are sometimes permissible, they must be subject to strict minimization requirements as a constitutional safeguard against abuse.

If this Court concludes that tower-dump warrants do not categorically violate the prohibition on general warrants, it should limit its holding to the tower dumps at issue here, and it should look to the overbreadth and particularity requirements of art. 14 and the Fourth Amendment to guide the adoption of safeguards to mitigate constitutional violations going forward.

A. This Court should limit its holding to tower dumps.

Although this Court's amicus solicitation references "cell tower dump or geofence warrants," the decision in this case should be limited to tower dumps. While tower dumps rely on location data and other call detail records generated by phones registering with cellular towers, "geofencing" most often refers to Google's ability to locate its subscribers' and users' phones based on a combination of cell-site, Wi-Fi, and GPS-connection data. *See generally, e.g.*, *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345 (N.D. Ill. 2020). Because these differences are potentially relevant,[12] this Court should not address the constitutionality of geofence warrants in this case.

B. This Court should articulate constitutional limitations on tower-dump warrants sufficient to ensure they are particular and not overbroad.

Because tower dumps necessarily sweep in information about people who have no connection to the crime under investigation, tower-dump warrants must at least include minimization requirements and related protections. The U.S. Supreme Court's landmark opinion in *Berger v. New York*, 388 U.S. 41, required such

[12] For example, GPS coordinates currently can pinpoint a person's location with more precision than the CSLI provided in tower dumps. *Id.* at 360. And geofence coordinates may be generated (and retained) regardless of whether the cell-phone user is actively using the phone.

protections in order to ensure that eavesdropping and wiretaps were constitutional. Similar safeguards must apply to the extraordinarily invasive technology at issue here.

The *Berger* Court addressed wiretapping and eavesdropping warrants, which, like tower dumps, "involve[] an intrusion on privacy that is broad in scope" because such surveillance can sweep in the "conversations of any and all persons coming into the area covered by the device . . . without regard to their connection with the crime under investigation." *Id.* at 56, 59. The Court invalidated New York's eavesdropping statute because it enabled "general searches." *Id.* at 58. To prevent those intrusions, the Court identified safeguards such as limitations on the duration and scope of the collection, requirements to first exhaust "conventional" investigative methods, procedures to avoid "use of seized conversations of innocent as well as guilty parties," and notice to affected parties. *Id.* at 59–60.

As this Court has recognized, the "purpose of including the minimization directive is to . . . avoid any improper intrusion on rights of privacy." *Commonwealth v. Vitello*, 367 Mass. 224, 265–66 (1975). Following *Berger*, both the U.S. Congress and the Massachusetts legislature enacted wiretapping and eavesdropping statutes including such protections. *Blood*, 400 Mass. at 75 n.15. Notably, these requirements are not unique to the wiretapping context. Courts have frequently recognized the need for *ex ante* protections when police seize large

caches of private digital data without probable cause or particularity, to prevent them from exploiting this information. *See, e.g.*, *In re Search Warrant*, 71 A.3d 1158 (Vt. 2012); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) (per curiam) (en banc); *id.* at 1180 (Kozinski, C.J., concurring); *State v. Mansor*, 421 P.3d 323 (Or. 2018).

Here, the probable cause and particularity requirements of art. 14 and the Fourth Amendment require *ex ante* protections like those required for wiretapping.

First, the government must aver in its warrant application that it has exhausted less invasive means of identifying the suspect. This is a familiar requirement for police in the Commonwealth. *See, e.g.*, G.L. c. 272, § 99(E)(3) (wiretapping warrant may issue only "[u]pon a showing by the applicant that normal investigative procedures have been tried and have failed or reasonably appear unlikely to succeed if tried").

Second, tower-dump warrants should be issued only in cases involving investigation of multiple temporally and geographically distinct crimes, and only where there is probable cause to believe those crimes were committed by the same individual. The crime scenes should be geographically distant enough that they are served by different cell towers. Only these searches—when combined with strict

filter and discard requirements, *see infra*—will return results that are limited to individuals appearing at multiple scenes.[13]

Third, tower-dump warrants should mitigate the intrusion into the private lives of proximate individuals by:

- Requiring "justification for the time period for which the records will be gathered";[14]
- Requiring that the time period be no longer than necessary to identify individuals present at the alleged crime;
- Requiring that the area to be searched be closely circumscribed to the site of the incident under investigation;
- Prohibiting the return of phone numbers engaged in communication with phones at the site in question;
- Requiring that law enforcement adopt and follow a protocol for the acquisition, use, and retention of the information obtained to limit to the fullest extent possible invasions into the privacy of people lacking any

[13] 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.

[14] *In re Application of the U.S. 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, 519 (S.D.N.Y. 2014) [hereinafter *S.D.N.Y. Tower Dump Order*].

role in the purported criminal offense.[15] This would include protocols to prevent disclosure of phone numbers present only at one scene, either by requiring the service provider to compare tower-dump data from different crime scenes to determine if any phone was present at the sites of multiple offenses, or through the use of a filter team walled off from the primary investigators to conduct such matching.[16] The investigative team would receive only information about individuals present at the scenes of multiple offenses.

- Requiring prompt deletion of information about people not suspected of the crime under investigation, except as necessary to satisfy *Brady* and similar defense-disclosure obligations.[17] If not immediately deleted, the data should be segregated and stored securely in a manner off-limits to investigative queries.

---

[15] *See In re Application of the U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 930 F. Supp. 2d 698, 702 (S.D. Tex. 2012) (imposing this requirement); *S.D.N.Y. Tower Dump Order*, 42 F. Supp. 3d at 519 (same).

[16] *See Comprehensive Drug Testing, Inc*., 621 F.3d at 1180 (Kozinski, C.J., concurring) ("Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party.").

[17] *Cf. In re Application of the U.S. for an Order Relating to Telephones Used by Suppressed*, No. 15 M 0021, 2015 WL 6871289, at *4 (N.D. Ill. Nov. 9, 2015) (in granting warrant to use cell site simulator to locate suspect's phone, requiring that "law enforcement officers must immediately destroy all data other than the data identifying the cell phone used by the target").

Fourth, the individuals whose personal information was swept up in the tower dump during the course of the criminal investigation must be notified by either the telecommunications provider or the government as soon as the notification would not jeopardize the ongoing criminal investigation.[18]

Fifth, the warrant return should detail the number of devices or individuals with data returned in the tower dump, the number of individuals not suspected of the crime under investigation, and the estimated coverage area of each cell tower or cell site included in the data. This information will provide judges, lawmakers, and the public insight into how invasive these searches are in practice and whether additional safeguards are needed.

CONCLUSION

For the reasons above, this Court should hold that tower dumps constitute a search and seizure. The Court should further hold that the unprecedented, indiscriminate, and dragnet nature of tower dumps means they are unconstitutional general searches. Even if the Court disagrees, it should rule narrowly on the permissibility of tower dumps and impose minimization requirements and other safeguards to address the invasive nature of this technique.

[18] *See In re Search of Cellular Tel. Towers*, 945 F. Supp. 2d 769, 771 (S.D. Tex. 2013).

Dated: November 17, 2021

Respectfully submitted,

/s/ Matthew R. Segal

Matthew R. Segal (BBO 654489)
Jessie J. Rossman (BBO 670685)
Jessica J. Lewis (BBO 704229)
American Civil Liberties Union
Foundation of Massachusetts, Inc.
211 Congress Street
Boston, MA 02110
(617) 482-3170
msegal@aclum.org
jrossman@aclum.org
jlewis@aclum.org

Counsel for ACLU of Massachusetts

Nathan Freed Wessler (BBO 680281)
Brett Max Kaufman (on the brief)
Ashley Gorski (on the brief)
Patrick Toomey (BBO 673928*)
American Civil Liberties
Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
nwessler@aclu.org
bkaufman@aclu.org
agorski@aclu.org
ptoomey@aclu.org

Jennifer Granick (on the brief)
American Civil Liberties
Union Foundation
39 Drumm Street
San Francisco, CA 94111
(415) 343-0758

jgranick@aclu.org

Counsel for ACLU

Matthew Spurlock (BBO 601156)
Committee for Public Counsel
Services, Public Defender Division
75 Federal Street
Boston, MA 02110
(617) 482-6212
mspurlock@publiccounsel.net

Counsel for CPCS

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

Counsel for EFF

Joshua M. Daniels (BBO 673034)
Law Office of Joshua M. Daniels
P.O. Box 300765
Jamaica Plain, MA 02130
(617) 942-2190
jdaniels@danielsappeals.com

Counsel for MACDL

* *Inactive status in Massachusetts*

CERTIFICATE OF COMPLIANCE

I, Matthew R. Segal, do hereby certify that this brief complies with the rules of court that pertain to the filing of amicus briefs, including, but not limited to Rules 16, 17, and 20. This brief complies with the length limit because it is set in 14-point Times New Roman font, and contains 6,540 non-excluded words, as determined through the use of the "word count" feature in Microsoft Word Version 16.54.

/s/ Matthew R. Segal
Matthew R. Segal

CERTIFICATE OF SERVICE

I, Matthew R. Segal, do hereby certify that on November 17, 2021, I served this brief on the Commonwealth and the defendants by directing an electronic copy of the foregoing brief to the following counsel.

Eric Tennen (BBO 650542)
Swomley & Tennen, LLP
50 Congress Street, Suite 600
Boston, MA 02190
(617) 227-9443
etennen@swomleyandtennen.com

Cailin M. Campbell (BBO 676342)
Assistant District Attorney
One Bulfinch Place
Boston, MA 02114
(617) 619-4070
cailin.campbell@state.ma.us

/s/ Matthew R. Segal
Matthew R. Segal