COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT

No. SJC-13144

COMMONWEALTH OF MASSACHUSETTS,

Appellee,

v.

JERRON PERRY,

Appellant.

On Interlocutory Appeal from an Order of the Suffolk Superior Court

---

BRIEF OF AMICUS CURIAE THE SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT IN SUPPORT OF APPELLANT AND REVERSAL

Dated: November 17, 2021

Mason A. Kortz, BBO #691257
Cyberlaw Clinic
Harvard Law School
1585 Massachusetts Ave., Suite 5018
Cambridge, MA 02138
Tel: (617) 495-2895
Fax: (617) 495-7641
mkortz@law.harvard.edu

Counsel for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 17(c)(1) of the Massachusetts Rules of Appellate Procedure, amicus curiae the Surveillance Technology Oversight Project states that it has no parent corporation. It has no stock, and therefore, no publicly held company owns 10% or more of its stock.

Dated: November 17, 2021

Respectfully Submitted,

/s/ Mason A. Kortz

Mason A. Kortz, BBO #691257

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST OF AMICUS CURIAE

The Surveillance Technology Oversight Project ("S.T.O.P.") is a non-profit advocacy organization and legal services provider based in New York City, NY. S.T.O.P. advocates for the protection of civil rights in light of technological advancements, with a particular focus on the discriminatory impact of surveillance on marginalized communities. S.T.O.P. pursues its goals through a combination of litigation, legislative reform, civil rights advocacy, and public education. S.T.O.P. envisions a world in which the United States and its constituent governments harness novel technologies without sacrificing age-old rights.

The question on which the Supreme Judicial Court solicited amicus briefs—namely, whether suppression of evidence is required due to the breadth of the cell tower dump warrants used in this case—is directly relevant to S.T.O.P.'s interests and experience. In 2020, S.T.O.P. worked with New York State legislators to propose a ban on geolocation searches, including cell tower dumps and geofence searches. The law would ban all cell tower dumps, whether done pursuant to a judicial warrant or with the affirmative consent of the cell tower operator.

DECLARATION OF AMICUS CURIAE

Pursuant to Rule 17(c)(5) of the Massachusetts Rules of Appellate Procedure, amicus certifies that no party's counsel authored this brief in whole or in part; no party or party's counsel contributed money that was intended to fund preparing or submitting this brief; and no person—other than amicus, its members, or its counsel—contributed money that was intended to fund preparing or submitting this brief. Amicus and its counsel have not represented any party to the present appeal in another proceeding involving similar issues, or been a party or represented a party in a proceeding or legal transaction that is at issue in the present appeal.

SUMMARY OF ARGUMENT

Cell tower dumps are a ticking time bomb—an error-prone, biased, and invasive tactic—that if left unchecked, will fuel a wave of false arrests and convictions. American Police departments are conducting exponentially increasing numbers of cell tower dumps every year, now tens of thousands of tower dumps annually, with each dump collecting thousands of individuals' cell site location information ("CSLI"). By casting such a broad digital dragnet for even low-level offenses, officers are taking in huge amounts of data, but not always helpful data. All of this information primes police to falsely suspect bystanders based on incomplete data. When offenders turn off their phone prior to committing a crime, tower dumps will lead officers on a wild goose chase, a mirage of nearby "suspects" whose only offense was walking with their phone. The risk of false arrest will not be borne evenly. Variation in cellular network topography—cell tower density, environmental conditions, and other factors—will radically skew the precision of cell tower data for low-income communities. These errors and biases will likely accelerate surveillance and over policing of marginalized and multi-marginalized communities. Cell tower dumps are not just a panopticon, but a policing quagmire.

While those who are committing crimes might be on notice to turn off their phones, those of us going about our lives rarely do. The resulting pool of intimate

information is ripe for abuse. Police departments lack the internal safeguard to prevent misuse of such a powerful tool for improper personal purposes. Access to such a high supply of information will only lead to more frequent and severe misuse of information. But misuse by the government is not the only concern. The growing threat of cyberattacks against law enforcement agencies means it is increasingly probable that outside parties can get access to the private, revealing data collected through tower dumps. Cell tower dumps undermine, rather than improve, Massachusetts residents' safety, especially for members of marginalized communities.

Cell tower dumps are not only dangerous and bad for policing—they are also flatly unconstitutional. Both the federal and state Constitutions prohibit general warrants that lack particularity. A warrant that authorizes the collection of 50,950 individuals' information, with no individualized suspicion, lacks particularity by any definition of the term. Finally, the Commonwealth's argument that it did not need a warrant in the first place is not only irrelevant, considering both federal and local law enforcement used warrants in this case, it is also inaccurate, as the Supreme Court itself has recognized the privacy interest in CSLI data. Accordingly, amicus respectfully urges the Court to reverse the decision below and order suppression of all evidence obtained from the cell tower dumps at issue in this case.

ARGUMENT

The use of "cell tower dumps" to collect of mass quantities of CSLI poses a singular threat to the public safety, civil rights, and privacy of the residents of the Commonwealth. As with other uses of data-driven policing, cell tower dumps will be a high-tech destruction, leading police to arrest innocent bystanders. Courts cannot address these harms through procedural safeguards or better software—cell tower dump data is inherently imperfect because of the uneven distribution and variable coverage of cellular networks. These flaws reinforce existing biases in policing, directing police attention to low-income neighborhoods and Black, Indigenous, and people of color ("BIPOC") communities. On top of this, a history of intentional misuse of surveillance data and the ever-present risk of cybersecurity attacks mean that police should not even be permitted to collect such massive amounts CSLI data.

Similar concerns led both this Court and the United States Supreme Court to prohibit police from collecting an individual's historical CSLI without a warrant. But whereas police can seek a warrant to search an individual's CSLI history, no officer can satisfy the showing of particularity needed to authorize a cell tower dump. This is because, unlike individuals CSLI searches, each cell tower serves thousands of customers, the vast majority of whom will have no connection to the investigation. A cell tower dump's inherent lack of particularity makes any

authorizing warrant—including those issued in this case—an unconstitutional general warrant.

I. CELL TOWER DUMPS ARE HARMFUL TO SOCIETY AND ULTIMATELY UNDERMINE PUBLIC SAFETY.

Cell tower dumps are an unreliable and uniquely invasive law enforcement tool. The scope of even a single cell tower dump far exceeds that of many other investigatory techniques, not merely crossing but leaping over the line into dragnet surveillance. Police investigative techniques are historically prone to errors and bias, often leading to false arrests, faulty convictions, and other injustices. Cell tower dumps significantly magnify these concerns, where each request discloses the information of tens if not hundreds of thousands of people. Attempts to use large-scale data analysis for law enforcement purposes have led to false positives, bias amplification, and a vicious cycle of over policing in minority neighborhoods. Nothing ensures that police have the training to utilize this dangerous tool in a responsible manner.

In addition to undermining public safety, cell tower dumps threaten personal freedoms. Whether through accidental disclosure or intentional abuse, government surveillance tools often lead to the misuse of personal information, putting subjects at risk of stalking, harassment, or worse. Moreover, when police obtain data through cell tower dumps, they are tasked with keeping that information safe. Some of the best trained and most sophisticated data management companies

struggle to keep their data secure. Law enforcement agencies often lack even basic training in data security and are frequently the targets of malicious attacks, further exposing private information.

All told, cell tower dumps are less reliable and more damaging than the Commonwealth asserts. See Kolender v. Lawson, 461 U.S. 352, 367 (1983) (Brennan, J., concurring) (explaining that government assertion of interest in "general facilitation of police investigation and preservation of public order" is not sufficient to justify an unconstitutional search). Amicus respectfully urges the Court to consider the threats to fundamental concepts of public safety and privacy posed by cell tower dumps.

A. Data obtained from cell tower dumps can contain errors and biases, undermining public safety and leading to unjust outcomes.

As with any surveillance technology, CSLI is neither error- nor bias-free. The potential for errors in police technology means that, inevitably, innocent people are investigated, arrested, and even convicted due to faulty analysis. The presence of bias means that the burden of these mistakes will fall predominantly on marginalized communities. The Court should be especially wary of the potential for errors and biases in cell tower dumps given the massive scale and indiscriminate data collection and processing.

As an initial matter, it is important to understand just how much location information cell tower dumps produce. In the 2010 High Lands Bandits case, the

FBI obtained data to identify the location of over 150,000 people by requesting all registered phone numbers near the banks where three robberies took place. Nate Anderson, How "Cell Tower Dumps" Caught the High Country Bandits—And Why It Matters, Ars Technica (Aug. 29, 2013).[1] In the Appellant's case, police searched six locations, revealing the information of over 50,000 unique registered phone numbers. Perry Brief at 12. Such searches are far from uncommon. While law enforcement agencies rarely disclose their practices, provider transparency reports show that law enforcement agents request CSLI at an alarming rate. T-Mobile, one of the providers involved in this case, received 70,938 CSLI demands and 6,542 requests for tower dumps in 2019. Transparency Report for 2019, T-Mobile (July 2020).[2] In 2020, the number of CSLI requests rose to 109,534, while the number of tower dump requests increased 84% to 12,019. Transparency Report for 2020, T-Mobile (July 2021).[3] AT&T and Verizon, two more providers searched in this case, have already reported thousands of cell tower dump requests in 2021.

[1] https://arstechnica.com/tech-policy/2013/08/how-cell-tower-dumps-caught-the-high-country-bandits-and-why-it-matters/
[2] https://www.t-mobile.com/news/_admin/uploads/2020/07/2019-Transparency-Report-3.pdf
[3] https://www.t-mobile.com/news/_admin/uploads/2021/07/2020-Transparency-Report.pdf

Transparency Report, AT&T (Aug. 2021);[4] US Transparency Report, Verizon (Aug. 2021).[5]

With this much information in their possession, law enforcement agencies will increasingly make mistakes and investigate, arrest, and punish innocent individuals. This is due, in part, to the fact that mass surveillance takes the focus off traditional processes of developing leads and investigating individuals and puts it on automated pattern recognition. See generally Elizabeth E. Joh, The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing, 10 Harv. L. & Pol'y Rev. 15 (2016).[6] However, these tools make mistakes, like the automated license plate reader error that led to police holding a Black woman at gunpoint, id. at 31 (citing Greene v. San Francisco, 751 F.3d 1039, 1042-43 (9th Cir. 2014)), or a facial recognition false positive causing police to wrongly arrest a Black man for shoplifting, Drew Harrell, Wrongfully Arrested Man Sues Detroit Police Over False Facial Recognition Match, Washington Post (Apr. 13, 2021).[7] Even when correctly functioning, data-based surveillance can detect patterns that have nothing to do with criminal activity. See Joh, supra, at 27; see also Leila Barghouty, What

[4] https://about.att.com/content/dam/csr/2019/transparency/2021/2021-August-Report.pdf
[5] https://www.verizon.com/about/sites/default/files/us-transparency-report-1h-2021.pdf
[6] https://harvardlpr.com/wp-content/uploads/sites/20/2016/02/10.1_3_Joh.pdf
[7] https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/

Are Geofence Warrants?, The Markup (Sept. 1, 2020)[8] (reporting on a biker whose exercise routine flagged him as a suspect in a robbery). Cellular data is no exception; private vendors are already selling surveillance analytics tools that allow police to process cellular data at scale, "convert[ing] information collected by cellular providers into maps of people's locations, movements, and relationships." Sam Richards, Powerful Mobile Phone Surveillance Tool Operates in Obscurity Across the Country, The Intercept (Dec. 23, 2020).[9]

Cellular data collection can also be biased. For example, the density of cellular networks varies geographically. CSLI is more abundant and more precise in denser networks, meaning cell tower dumps will result in greater capture of innocent individuals' information in densely populated areas. In other areas, the lack of cell towers may give a biased view of an individual's movements. In the High Country Bandits case, the FBI demanded dumps for Verizon towers near the locations of four bank robberies, but Verizon only had towers in range of three of them. Anderson, supra. As a result, the data obtained could have missed potentially exculpatory evidence from the fourth location in question. This no small problem: missing or biased data leads to incorrect conclusions about criminal activity. Will Douglas Heaven, Predictive Policing Is Still Racist—Whatever Data It Uses, MIT

[8] https://themarkup.org/ask-the-markup/2020/09/01/geofence-police-warrants-smartphone-location-data
[9] https://theintercept.com/2020/12/23/police-phone-surveillance-dragnet-cellhawk/

Technology Review (Feb. 5, 2021)[10] (reporting that "predictive policing" analysis underestimated crime rate in areas with low reporting and overestimated crime rate in areas with high reporting). Then there is the fact that criminals can, and likely will, turn off their phones during the commission of a crime while innocent people will not—meaning that cell tower dumps are prone to both false negatives and false positives. With cell tower dumps, police risk letting guilty parties go undetected while falsely arresting innocent people, all depending on the vagaries of a cellular network.

Third, preexisting assumptions about criminal activity lead to increased surveillance of marginalized communities. It is well documented that low-income communities and communities of color are already overpoliced. See generally Colleen Walsh, Solving Racial Disparities in Policing, The Harvard Gazette (Feb. 23, 2021).[11] When police rely on purportedly "neutral" data sources like cell tower dumps, the technologies themselves embed biases that amplify existing disparities. See Andrew Selbst, Disparate Impact in Big Data Policing, 52 Ga. L. Rev. 109, 126-140 (2017).[12] Location-based surveillance may be particularly pernicious in reinforcing existing regional disparities in investigations. See Heaven, supra

[10] https://www.technologyreview.com/2021/02/05/1017560/predictive-policing-racist-algorithmic-bias-data-crime-predpol/
[11] https://news.harvard.edu/gazette/story/2021/02/solving-racial-disparities-in-policing/
[12] https://par.nsf.gov/servlets/purl/10074337

(explaining that poor or Black people are more likely to be reported for crimes than rich or white people, leading to overestimation of crime in poor, Black neighborhoods). Conclusions drawn from location-based surveillance, which includes cell tower dumps, are therefore unreliable—given that many cities in the United States have been socially and legally segregated by race and class, the data resulting is inherently biased. Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement, 75 (2017). The same feedback loops that lead to overpolicing, Selbst, supra, at 121, may well lead to oversurveillance.

B. Cell tower dumps and the data they produce are ripe for misuse and abuse.

The accumulation of personal information is not merely a passive harm. Whether intentionally or otherwise, police departments have historically mishandled and misused evidence. A 2016 audit of the Braintree Police Department's evidence room showed that police lost firearms, money, and evidence ranging from drugs to sexual assault kits due to improper handling. Evan Allen, Drugs, Guns, and $400,000 Missing from Braintree Police, Boston Globe (Sept. 14, 2016).[13] Similar mishandling can and has occurred with electronic surveillance records as well. See Zack Whittaker, Police License Plate Readers are

[13] https://www.bostonglobe.com/metro/2016/09/14/audit-details-evidence-missing-from-braintree-police-department/oj1mvfCDTh1OSCx3K0XkEN/story.html

Still Exposed on the Internet, TechCrunch (Jan. 22, 2019).[14] Even more damaging is the intentional abuse and falsification of evidence. The Commonwealth is still reeling from the Annie Dookhan and Sonja Farak drug lab scandals, which revealed egregious abuse of authority by lab technicians and led courts to vacate over 30,000 drug convictions. Tom Jackman, Prosecutors Who Covered Up Mass. Drug Lab Scandal Now Face Bar Discipline, Civil Rights Lawsuit, Washington Post, (July 30, 2019).[15] Even now, the Massachusetts Board of Bar Overseers is determining the punishment for three assistant attorneys general who withheld potentially exculpatory evidence in cases tainted by Farak's misconduct. Deborah Becker, Lawyers on Both Sides Recommend Sanctions for 3 Ex-Assistant AGs in Drug Lab Scandal, WBUR News (Aug. 23, 2021).[16]

Surveillance technologies are particularly ripe for abuse of police power. Many law enforcement agents use unfettered access to personal information for improper personal purposes. "Police officers across the country misuse confidential law enforcement databases to get information on romantic partners, business associates, neighbors, journalists and others for reasons that have nothing

[14] https://techcrunch.com/2019/01/22/police-alpr-license-plate-readers-accessible-internet/
[15] https://www.washingtonpost.com/crime-law/2019/07/30/prosecutors-who-covered-up-mass-drug-lab-scandal-now-face-bar-discipline-civil-rights-suit/
[16] https://www.wbur.org/news/2021/08/23/kaczmarek-verner-foster-massachusetts-farak-drug-scandal-punishments

to do with daily police work." Associated Press, Police Sometimes Misuse Confidential Work Databases for Personal Gain, CBS News (Sept. 30, 2016);[17] see also Avis Thomas-Lester and Toni Locy, Chief's Friend Accused of Extortion, Washington Post (Nov. 26, 1997)[18] (reporting on police officer who abused surveillance to extort patrons of gay bar). Cell tower dump information, which can reveal where people were and even who they were calling, is ripe for even more invasive abuse.

Moreover, police abuse of surveillance power has a greater impact on certain populations. Location tracking enables intimate partner violence, and location data held by police is no exception. See CBS Local Media, Ex-Cop Uses GPS to Track His Date, CBS Los Angeles (Mar. 14, 2011).[19] Demographic differences can further exacerbate these harms. As stated above, CSLI is more accurate and abundant in densely populated areas such as large cities—the same areas where low-income people and LGBTQ communities tend to reside. Low income is correlated with intimate partner violence, and LGBTQ people who experience intimate partner violence face additional challenges in accessing resources. This

[17] https://www.cbsnews.com/news/police-sometimes-misuse-confidential-work-databases-for-personal-gain-ap/
[18] https://www.washingtonpost.com/wp-srv/local/longterm/library/dc/dcpolice/stories/stowe25.htm
[19] https://losangeles.cbslocal.com/2011/03/14/ex-cop-uses-gps-to-track-his-date/

confluence of factors dramatically increases risk posed by location tracking for these marginalized populations.

Finally, law enforcement may use tower dumps to get around existing procedural safeguards. In Commonwealth v. Estabrook, 472 Mass. 852 (2015), this Court ruled that CSLI tracking over a period that exceeds six hours implicates an individual's constitutional privacy interest and attaches a warrant requirement to the search. Id. at 858. This six-hour limit is meaningless if police can build up a database of location information one tower dump at a time. Police should not be allowed to obtain tens of thousands of CSLI records whenever a crime occurs near a cell tower—especially given that no law dictates how long police are permitted to store CSLI, with whom they are permitted to share it, or whether they are permitted to access it for unrelated investigations. See Richards, supra (reporting on Minnesota police department's five-year retention period for "criminal intelligence information").

C. Collecting location information raises data privacy and security concerns that law enforcement agencies are unequipped to address.

Cell tower dumps produce huge amounts of highly revealing data—data that law enforcement agencies are ill-prepared to protect. When a law enforcement agency inevitably suffers a cybersecurity attack and loses control of cell tower data, malicious actors will gain access to the personal information and movement patterns of tens or hundreds of thousands of individuals.

The Commonwealth downplays the invasiveness of cell tower dumps by initially claiming they reveal only phone numbers, Appellant's Brief at 24, although it later concedes in a footnote that they also show "the other phone number associated with the call, identifying information associated with the phone, and whether the communication was a voice or text communication," id. at 25 n.11. The Commonwealth argues that this additional information is not worth considering, because it could have been obtained with an administrative subpoena. Id. However, a subpoena for records on more than 50,000 subscribers, none of whom were yet connected with criminal activity, would certainly raise questions—and likely provoke a motion to quash. See M.G.L.ch. 271, § 17B (providing that administrative subpoenas for subscriber information require "reasonable grounds to believe that records in the possession of [a service provider] are relevant and material to an ongoing criminal investigation).

Even on their own, the location and number of an individual's phone are revealing. Location information reveals "an individual's habits, beliefs, and social proclivities." See Mana Azarmi, Location Data: The More They Know, Center for Democracy & Technology (Nov. 27, 2017).[20] An individual's phone number is linked to many essential life activities, including financial and medical records, email and social media accounts, and business contacts, to name a few. Nancy

[20] https://cdt.org/insights/location-data-the-more-they-know/

Lloyd, Why Giving Up Your Phone Number Can Mean Giving Up Your Privacy, Los Angeles Times (Nov. 26, 2016).[21] Inferences drawn by combining data from multiple tower dumps could reveal information about an individual's movement patterns and habits. See Richards, supra. Combined with the fact that police can stash cell tower information indefinitely, the public is subject to precisely the "mosaic of surveillance" this Court has recognized as a risk to privacy. See Commonwealth v. McCarthy, 484 Mass. 493, 503 (2020).

With the steep rise in cyberattacks globally and in the United States, it seems inevitable that this revealing information will fall into the wrong hands. According to the World Economic Forum, cyberattacks were among the top ten most likely and most damaging global risks in 2020. World Economic Forum, The Global Risks Report 2020, fig. 2 (Jan. 15, 2020)(.[22] Government agencies are particularly vulnerable to cyberattacks due to their outdated computer systems, and the sensitive nature of the data they store. See generally IBM Newsroom, IBM Survey: Only 38% of State and Local Government Employees Trained on Ransomware Prevention, IBM (Feb. 27, 2020).[23] A 2020 report by the Department of Homeland Security highlighted this vulnerability, revealing that the United States Customs

[21] https://www.latimes.com/business/la-fi-tn-phone-number-security-20161125-story.html
[22] https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
[23] https://newsroom.ibm.com/2020-02-27-IBM-Survey-Only-38-of-State-and-Local-Government-Employees-Trained-on-Ransomware-Prevention

and Border Protection exposed 184,000 facial images of cross-border travelers in a recent data breach. Department of Homeland Security, Office of the Inspector General, Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot, OIG-20-71 (Sept. 21, 2020).[24] The problem has arrived in Masschusetts as well—just this summer, the Brockton Police Department faced a ransomware attack. Wale Aliyu, Brockton PD Under Cyberattack, Police and Fire Forced to Go Old School, Boston 25 News (July 20, 2021);[25] see also Ryan Kath and Jim Haddadin, 1 In 6 Massachusetts Communities Hit by "Ransomware" Attacks, NBC Boston (Feb. 14, 2020).[26] Cyberattacks are not a theoretical risk to Massachusetts police departments; they are an active threat that has materialized in the past and will continue in the future.

If police are permitted to obtain and store cell tower dump information, a single successful cyberattack would compromise hundreds of thousands of individuals' location and subscriber information. Furthermore, because law enforcement agencies generally do not provide data inventories or articulate their method for disposing of evidence, there is no way for members of the public to know if their information is implicated in such a breach. This cloak of secrecy is

[24] https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf
[25] https://www.boston25news.com/news/brockton-pd-under-cyberattack-police-fire-forced-go-old-school/ZAK2D73VNJDHFMJS6RPDIM755U/
[26] https://www.nbcboston.com/investigations/1-in-6-massachusetts-communities-hit-by-ransomware-attacks/2076600/

yet another reason why law enforcement agencies should not be permitted to obtain such vast amounts of unnecessary data in the first place.

II. CELL TOWER DUMP SEARCHES VIOLATE THE FOURTH AMENDMENT AND ARTICLE 14 OF THE MASSACHUSETTS DECLARATION OF RIGHTS.

Both the Fourth Amendment and art. 14 of the Massachusetts Declaration of Rights require that all warrants are supported by probable cause and describe with sufficient particularity the places, persons, and items to be searched and seized. See Commonwealth v. Valerio, 449 Mass. 562, 566-67 (2007). As Appellant argues in depth, the warrant here fails to clear the first hurdle because it lacked probable cause. Appellant's Brief at 43-49. Perhaps more alarming, though, is the lack of particularity. Definitionally, no cell tower dump warrant can pass constitutional muster; cell tower dumps are exactly the kind of "all-person" search the federal and Commonwealth Constitutions prohibit. Because the constitutional requirement for a valid warrant was not met, the evidence obtained from the cell tower dump must be suppressed.

A. Cell tower dump warrants are precisely the type of general warrant that the particularity requirement seeks to eliminate.

A "general warrant" is one that "specifie[s] only an offense", leaving it "to the discretion of executing officials the decision as to which persons should be arrested and which places should be searched." Steagald v. United States, 451 U.S. 204, 220 (1981). Such warrants are not merely unconstitutional; it is precisely their

"'intolerab[ility]'" and "'abhorrence" that "'gave birth to the Fourth Amendment.'" Commonwealth v. Wilkerson, 486 Mass. 159, 169 (2020) (quoting Commonwealth v. Lett, 393 Mass. 141, 146 (1984)). The canonical general warrants were the British writs of assistance that gave custom officials "blanket authority" to sift through goods at their own discretion and search for contraband, placing "the liberty of every man in the hands of every petty officer." Stanford v. Texas, 379 U.S. 476, 510 (1965). Particularly protects against such arbitrary government intrusions, Commonwealth v. Snow, 486 Mass. 582, 590 (2021), and gives defendants a basis to challenge overbroad searches. Valerio, 449 Mass. at 567 (citing Commonwealth v. Sheppard, 394 Mass. 381, 391 (1985)).

However, the prohibition on generalized searches is not only meant to protect those who are ultimately charged with a crime; it also ensures that "an innocent person [is not] swept up in a dragnet and searched." Commonwealth v. Smith, 370 Mass 335, 346 (1976). One type of warrant that this Court and others have consistently warranted against is the "all-person" warrant, which authorizes the search of everyone present in a certain location on the theory that *someone* will be carrying evidence of a crime. See, e.g., People v. Nieves, 36 N.Y.2d 396, 402-04 (1975) (invalidating a warrant that authorized the search of a restaurant, a cocktail lounge, and all persons occupying them because one person on the premises was suspected of illegal activity); Smith, 370 Mass. at 342 (approving of

Nieves). In keeping with the particularly requirement, such "all-person" warrants are only permitted where there is "probable cause to . . . believe that *all* persons present are involved in the criminal activity afoot." Smith, 370 Mass. at 344 (emphasis added).

Cell tower dump warrants are the modern manifestation of British writs of assistance—21st century "all-person" warrants that can search not just everyone in a location at one time, but in the past as well. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (explaining that with historical CSLI, "police need not even know in advance whether they want to follow a particular individual, or when"). Such warrants authorize law enforcement to go on an exploratory search of a location—or multiple locations—without an identified suspect in mind, sweep up the information of tens of thousands of innocent individuals in a dragnet, and sift through that data at their discretion in the aim of hopefully identifying one or two people connected to the crime.

Tower dumps are even less time- and person-specific than "all-person" warrants; they authorize police to simultaneously search tens of thousands of individuals across time and space and fish for patterns that could potentially allude to criminal—or innocent—activity. By way of illustration, imagine a police officer suspects evidence of a crime can be found somewhere in the city of Cambridge, Massachusetts. If the officer wants to search for this evidence, they can obtain a

warrant by identifying, with precision, the location to be searched. See Commonwealth v. Erickson, 14 Mass. App. Ct. 501, 504-07 (1982). The officer cannot, however, obtain a warrant to peer into 50,000 residences[27] in the hopes of finding evidence in one of them. See id. (invalidating warrant that authorized search of multi-dwelling unit containing six apartments). Add to this the fact that the officer would execute this warrant instantaneously, with little cost, and with no notice to the people residing in those residences. Now make the officer a time-traveler as well, able to go back and obtain a warrant not just for today, but any time in the past. This is what the Commonwealth seeks to do with location data through cell tower dumps. Such a search would not only violate the Fourth Amendment, it would be a paradigmatic example the "arbitrary [police] power" and "unbridled authority" that the Fourth Amendment broadly, and particularity specifically, sought to eliminate. See Stanford, 379 U.S. at 510.

B. The warrant at issue in this case violates the particularity requirement.

Because cell tower dumps are general searches, amicus urges the Court to adopt a bright line rule prohibiting the issuance of cell tower dump warrants. See Smith, 370 Mass. at 344 (noting that "in the overwhelming majority of cases" an

[27] As of 2019, Cambridge, Massachusetts contained 51,621 housing units, as estimated by the U.S. Census Bureau's 2019 American Communities Survey, available online at https://data.census.gov/cedsci/.

all-person warrant is "a clear violation of the proscription against unreasonable searches"). At the very least, the Court should hold that the warrant at issue here lacked particularity.

Applications for narrower location-based searches, called "geofence warrants," have been rejected by other courts. The United States District Court in the North District of Illinois recently addressed this issue in In the Matter of the Search of Information Stored at Premises Controlled by Google, 481 F.Supp.3d 730 (2021). In that case, the government suspected that an unknown suspect had entered two locations to receive and ship stolen medication. Id. at 742-43. The government applied for a warrant that authorized the collection of anonymized location information from Google for devices within two "geofences" during three 45-minute periods on a single day. Id. at 745. Each geofence consisted of a set of coordinates that covered a single, commercial building. Id. at 743. The warrant application provided that if the government identified devices of interest, it would follow up with Google to obtain identifying information. Id. at 747-48.

Despite the limiting language in the application, the court held that the warrant violated the particularity requirement because it granted the executing officer "unbridled discretion as to what device IDs would be used to yield . . . persons' location histories." Id. at 755. In particular, the court noted that the warrant "[did] not identify any of the persons whose location information the

government will obtain." Id. The court contrasted this with other, more targeted forms of location tracking and concluded that "where a warrant allows the tracking of a phone (and thus of a person) *not identified* in the warrant, not to mention such tracking of an unknown number of such persons, the warrant does not comply with the Fourth Amendment' particularity requirement." Id. (emphasis in the original).

The cell tower dump warrant in this case is far, far broader than the geofence warrant at issue in Google. Like the Google warrant, the instant warrant enables the tracking of an unknown number of persons, none of whom were identified in the warrant, based solely on the locations where an alleged crime occurred. However, while the Google warrant would only have obtained information from Google users with location services enabled, id. at 733-34, the cell tower dump here targeted anyone carrying an AT&T, Sprint, T-Mobile, or Verizon cellphone—a combination that covers 98% of the cellular service market.[28] Moreover, the Google warrant would have covered two commercial buildings. With cell tower dumps, the coverage is impossible to predict before the search is executed, as coverage varies with the location of the tower, the specific technology used, and

[28] As of 2018, Verizon controlled 35% of the cell service market, AT&T controlled 34%, T-Mobile 17%, and Sprint 12%. America's Concentration Crisis - Cell Phone Providers, Open Markets Institute (June 2019), https://concentrationcrisis.openmarketsinstitute.org/industry/cell-phone-providers/.

even the weather. Harry Guinness, No Bars? Here's Everything That Can Affect Your Cellular Signal Strength, How-To Geek (Sept. 4, 2017).[29]

This Court has said on multiple occasions that particularity questions are "to be approached…with a view toward common sense." Smith, 370 Mass. at 342. Here, common sense counsels that a warrant that allows law enforcement to treat 50,950 innocent and otherwise unrelated individuals as suspects to a crime, gather their data, and track their movements, all in order to identify one potential suspect, is overbroad by any reasonable definition of the word. The collection of such massive amounts of data exceeds the point at which any warrant could conceivably be labeled "particular."

C. The Commonwealth's argument that no warrant is required to obtain a cell tower dump conflicts with both law and practice.

"A warrantless search is presumptively unreasonable under both the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights . . . ." Commonwealth v. Johnson, 461 Mass. 44, 48 (2011). This foundational principle applies to cell tower dumps with such obvious force that the federal and local law enforcement agents who obtained the warrants in this case applied it by default. The Commonwealth's arguments to the contrary, Commonwealth Brief at 17-26, are half-hearted at best. To make this argument is

[29] https://www.howtogeek.com/324525/everything-that-can-affect-your-cellular-signal-strength/.

to be willfully ignorant of both the jurisprudence regarding the use of CSLI and the police practices that have emerged in response.

This Court was among the first to recognize that an individual has a constitutionally protected privacy interest in their CSLI in Commonwealth v. Augustine, 467 Mass. 230 (2014) . Four years later, this became the law of the land when the Supreme Court reached the same conclusion in Carpenter v. United States, 138 S. Ct. 2206 (2018). Both landmark decisions held that CSLI tracking requires a warrant because location monitoring invades an expectation of privacy that "society is willing to recognize . . . as reasonable." Augustine, 467 Mass. at 241-42. The logic of these cases makes clear that warrantless cell tower dumps are just as unreasonable as warrantless tracking of an individual's CSLI over time. In particular, both Courts recognized two key features of CSLI that led them to find a reasonable expectation of privacy, both of which hold true with cell tower dumps.

First, CSLI provides "near perfect surveillance" at essentially no cost to the government. Carpenter, 138 S. Ct. at 2218. CLSI combines a high degree of accuracy, virtual omnipresence, and incredible ease, speed, and cost effectiveness—a mix that few other surveillance technologies can boast. Id. at 2217-18. Both the Augustine and Carpenter courts recognized that the wide-spread adoption of cell phones enabled tracking that would have previously been impossible, or at least highly impractical. Augustine, 467 Mass. at 245; Carpenter,

138 S. Ct. at 2218. However, the mere fact that technological changes make a search *possible* does not necessarily mean that it makes the search *permissible*. See Katz v. United States, 389 U.S. 347, 352-53 (1967) (holding that use electronic recording device was a search under the Fourth Amendment); Kyllo v. United States, 533 U.S. 27, 34 (2001) (warning that advances in surveillance technology should not be permitted to "erode the privacy guaranteed by the Fourth Amendment"); see also Olmstead v. United States, 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting) ("Clauses [of the Constitution] guaranteeing to the individual protection against specific abuses of power, must have [the] capacity of adaptation to a changing world.").

Second, CSLI can provide historical location data, a feature that is not shared by other tracking technology such as GPS. Augustine, 467 Mass. at 254 ("[W]hen the government obtains historical CSLI from a cellular service provider, the government is able to track and reconstruct a person's past movements, a category of information that *never* would be available through the use of traditional law enforcement tools of investigation." (emphasis in original)). Historical location tracking presents even more grave concerns when considering that individuals often bring their phones with them into private spaces which they might "'seek to preserve as private,'" places such as "residences doctor's offices, political

headquarters, and other potentially revealing locales." Carpenter, 138 S. Ct. at 2217-18 (quoting Katz, 389 U.S. at 351-52); Augustine, 467 Mass. at 252-53.

These two features are not only present, but amplified, in the tower dump context. The Commonwealth downplays these concerns by focusing on each point of data in isolation. Commonwealth Brief at 22-26. This Court should reject this simplistic view, as it has in other cases where the amplifying effect of technology allows a search that is more than the sum of the individual observations. See Commonwealth v. Yusuf, 488 Mass. 379, 390 (2021) (declining to extend plain view doctrine to review of body camera footage because footage can be "preserved indefinitely, accessed without restriction, and reviewed at will for reasons unrelated to the purposes of the police visit"). Moreover, the Court should give ample weight to that both federal and local investigators in this very case apparently assumed a warrant was required—at least until they were faced with justifying it in court.

In arguing against a warrant requirement, the Commonwealth willfully ignores Chief Justice Roberts' admonition that the unchecked use of CSLI data collection "runs against everyone," Carpenter, 138 S. Ct. at 2218, and attempts to steamroll a path that would provide for massive and unchecked collection and reconstruction of location data through cell tower dumps. This Court should reject the Commonwealth's too little, too late arguments and clarify that society is well-

prepared to recognize a reasonable expectation that individuals will not be subject to dragnet surveillance simply for participating in modern communication. Id.

CONCLUSION

Because the search warrants at issue in this case were overbroad general warrants, all evidence obtained pursuant to those warrants must be suppressed. See Wilkerson, 486 Mass. at 169. For this reason, and the reasons stated above, amicus curiae respectfully requests that the Court grant Appellant's appeal and reverse the judgment of the lower court.

Dated: November 17, 2021

Respectfully Submitted,

/s/ Mason A. Kortz

Mason A. Kortz, BBO #691257
Cyberlaw Clinic
Harvard Law School[30]
1585 Massachusetts Ave., Suite 5018
Cambridge, MA 02138
Tel: (617) 495-2895
Fax: (617) 495-7641
mkortz@law.harvard.edu

Counsel for Amicus Curiae

[30] Amicus curiae thanks Fall 2021 Harvard Cyberlaw Clinic students Reem Hussein, Jack Shaffery, and Jess Valenzuela Ramirez for their invaluable contributions to this brief.

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 17(c)(9) of the Massachusetts Rules of Civil Procedure, I, Mason A. Kortz, hereby certify that the foregoing **Brief of Amicus Curiae the Surveillance Technology Oversight Project in Support of Appellant and Reversal** complies with the rules of court that pertain to the filing of amicus briefs, including, but not limited to:

Mass. R. A. P. 16(e) (references to the record);
Mass. R. A. P. 17(c) (cover, length, and content);
Mass. R. A. P. 20 (form and length of brief); and
Mass. R. A. P. 21 (redaction).

I further certify that the foregoing brief complies with the applicable length limitation in Mass. R. A. P. 20 because it is produced in the proportional font Times New Roman at size 14 points and contains 6,034 total non-excluded words as counted using the word count feature of Microsoft Word 365.

Dated: November 17, 2021

Respectfully Submitted,

/s/ Mason A. Kortz

Mason A. Kortz, BBO #691257

COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT

No. SJC-13144

COMMONWEALTH OF MASSACHUSETTS,

Appellee,

v.

JERRON PERRY,

Appellant.

CERTIFICATE OF SERVICE

Pursuant to Mass. R. A. P. 13(e), I hereby certify, under the penalties of perjury, that on this date of November 17, 2021, I have made service of a copy of the foregoing **Brief of Amicus Curiae the Surveillance Technology Oversight Project in Support of Appellant and Reversal** in the above captioned case upon all attorneys of record by electronic service through eFileMA.

Dated: November 17, 2021

Respectfully Submitted,

/s/ Mason A. Kortz

Mason A. Kortz, BBO #691257
Cyberlaw Clinic
Harvard Law School
1585 Massachusetts Ave., Suite 5018
Cambridge, MA 02138
Tel: (617) 495-2895
Fax: (617) 495-7641
mkortz@law.harvard.edu