Case No. 20-1495

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

LEADERS OF A BEAUTIFUL STRUGGLE, *et al.*,

Plaintiffs-Appellants,

v.

BALTIMORE POLICE DEPARTMENT, *et al.*,

Defendants-Appellees.

On Appeal from the U.S. District Court
for the District of Maryland at Baltimore
Case No. 1:16-cv-00929-RDB

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, BRENNAN CENTER FOR JUSTICE, ELECTRONIC PRIVACY INFORMATION CENTER, FREEDOMWORKS FOUNDATION, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, AND RUTHERFORD INSTITUTE IN SUPPORT OF PLAINTIFFS-APPELLANTS' PETITION FOR REHEARING EN BANC

Rachel Levinson-Waldman
Laura Hecht-Felella
BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW
1140 Connecticut Ave. NW, Suite 1150
Washington, DC 20036

Elizabeth Franklin-Best
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
Elizabeth Franklin-Best, P.C.
2925 Devine Street
Columbia, South Carolina 29205

John W. Whitehead
Douglas R. McKusick
RUTHERFORD INSTITUTE
109 Deerwood Road
Charlottesville, VA 22906

Sophia Cope
Counsel of record
Mark Rumold
Adam Schwartz
Saira Hussain
Hannah Zhao
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
sophia@eff.org
Counsel for Amici Curiae

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, amici curiae Electronic Frontier Foundation, Brennan Center for Justice, Electronic Privacy Information Center, FreedomWorks Foundation, National Association of Criminal Defense Lawyers, and Rutherford Institute state that they do not have a parent corporation, and that no publicly held corporation owns 10% or more of the stock of any amici.

Dated: November 25, 2020

Respectfully submitted,

/s/ Sophia Cope
Sophia Cope

ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Counsel of Record for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

Statement of Interest[1]

Amici curiae Electronic Frontier Foundation, Brennan Center for Justice at NYU School of Law, Electronic Privacy Information Center, FreedomWorks Foundation, National Association of Criminal Defense Lawyers, and Rutherford Institute are all nonprofit, public interest organizations representing a range of ideological and organizational interests. *See* Addendum at A1-A5.

Notwithstanding these differences, amici share a common interest: ensuring the Fourth Amendment's vital protection for individual privacy is undiminished by new and intrusive surveillance technology.

[1] No party's counsel authored this brief in whole or in part. Neither any party nor any party's counsel contributed money that was intended to fund preparing or submitting this brief. No person other than amici, its members, or its counsel contributed money that was intended to fund the preparing or submitting of this brief. All parties consent to the filing of this brief.

Introduction

Rehearing en banc is necessary because the panel's opinion contradicts two controlling Fourth Amendment principles. First, surveillance technologies that collect detailed records about people's movements, like Baltimore's Aerial Investigative Research (AIR) program, infringe on individuals' reasonable expectations of privacy. *Carpenter v. United States*, 138 S. Ct. 2206 (2018). *Infra* Part I. Second, the "special needs" exception to the warrant requirement does not apply where, as here, a police surveillance program serves only as a law enforcement investigatory tool. *Infra* Part II.

Rehearing is also warranted by the important technological and social aspects of this case. Baltimore's AIR program comprehensively tracks the movements of a half-million people as they travel throughout the city, and it is integrated into the city's vast surveillance camera and automated license plate reader (ALPR) networks. Other vendors are following AIR's maker, Persistent Surveillance Systems (PSS), into this new market for advanced police aerial surveillance technologies.[2] These police "eyes in the sky" chill free speech and assembly in public places, raising serious First Amendment concerns.

[2] Patrick Tucker, *Look for military drones to begin replacing police helicopters by 2025*, Defense One (Aug. 28, 2017), https://www.defenseone.com/technology/2017/08/look-military-drones-replace-police-helicopters-2025/140588/.

This case also exemplifies the disparate burden of government surveillance borne by communities of color—a problem described as "the color of surveillance." *See* Alvaro Bedoya, *Privacy as Civil Right*, 50 N.M. Law Rev. 301, 301 (2020). Police experiment with, and eventually deploy, intrusive technologies like the AIR program in cities with large communities of color. Before Baltimore, PSS operated surveillance flights above Compton, California; Philadelphia, Pennsylvania; and Dayton, Ohio.[3] The company also seeks to conduct surveillance of St. Louis, Missouri.[4] Further, authorities have routinely deployed aerial surveillance technologies against individuals participating in racial justice movements, like those protesting against the police killings of George Floyd in Minneapolis,[5] Michael Brown in Ferguson,[6] and Freddie Gray in Baltimore.[7]

---

[3] Conor Friedersdorf, *Eyes over Compton: How police spied on a whole city*, The Atlantic (Apr. 21, 2014), https://www.theatlantic.com/national/archive/2014/04/sheriffs-deputy-compares-drone-surveillance-of-compton-to-big-brother/360954/; Denver Nicks, *New surveillance cameras can see for miles and hours*, Time (Feb. 5, 2014), https://time.com/5307/surveillance-cameras/.

[4] Jim Salter, *St. Louis considers surveillance planes in crime battle*, Associated Press (July 10, 2020), https://apnews.com/article/f77a1101849a13c1f9023ebf854939c3.

[5] Zolan Kanno-Youngs, *U.S. watched George Floyd protests in 15 cities using aerial surveillance*, N.Y. Times (June 19, 2020), https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html.

[6] Eric Tucker, *Comey: FBI used aerial surveillance above Ferguson*, Associated Press (Oct. 23, 2015), https://apnews.com/article/f1a797c9b286412ca72eb85b3cc35a4b.

[7] Andrea Peterson, *FBI spy planes used thermal imaging tech in flights over Baltimore after Freddie Gray unrest*, Wash. Post (Oct. 30, 2015),

The combination of these racial disparities and the novel surveillance technique at issue here thus justifies rehearing this case en banc. *See* L.R. 35(b)(1)(B). And the legal errors in the panel's opinion require it. *See* L.R. 35(b)(1)(A).

I. The panel's decision conflicts with *Carpenter*.

The panel's decision must be reconsidered en banc because it conflicts with *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

Carpenter recognized that a detailed history of a person's location reveals profoundly sensitive information. 138 S. Ct. at 2214-21. Location information, the Supreme Court held, "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familiar, political, professional, religious, and sexual associations." *Id.* at 2217 (internal quotations omitted). Cell site location information (CSLI)—the particular type of location information at issue in *Carpenter*—is "detailed, encyclopedic, and effortlessly compiled," *id.* at 2216; it is "tireless and absolute," *id.* at 2218; and its "retrospective quality" gives police access to information "otherwise unknowable," *id*. For these reasons, the Supreme Court ruled that collection of CSLI for a seven-day period invaded Carpenter's reasonable expectation of privacy. *Id*. at 2219.

---

https://www.washingtonpost.com/news/the-switch/wp/2015/10/30/fbi-spy-planes-used-thermal-imaging-tech-in-flights-over-baltimore-after-freddie-gray-unrest/.

The same features that make CSLI collection so invasive are present in equal, if not greater, measure in the AIR program. The AIR program—both on its own, and in conjunction with other surveillance techniques—creates a "detailed, encyclopedic" record of the movements of Baltimore residents. *See Carpenter*, 138 S. Ct. at 2216, 2218. Its "retrospective quality" allows law enforcement to "travel back in time" to track those residents—12 hours a day, for 45 or more days.[8] *Id*. at 2218. And the AIR program "runs against everyone" in Baltimore; no one can "escape this tireless and absolute surveillance." *Id*.

Yet the panel majority nevertheless concluded that the program—which automatically creates a detailed, daily, historical record of the location information for the population of an entire American city—somehow does not contravene *Carpenter*. Op. at 13-15. This error flows from the majority's mistaken conclusion that the AIR program is "unable to capture identifying characteristics of people or automobiles." Op. at 3; *see also id*. at 13 (AIR cannot be used to observe a "person's identifying characteristics"); *id.* at 15 (the program can "tell the police very little about an identified person").

[8] It bears emphasis that the 45-day retention period is based solely on the current policy judgments of the city. So too is the limitation that surveillance is only conducted 12 hours per day. These policy judgments could change at any time. *See* Op. at 29 n. 3 (Gregory, C.J., dissenting).

That is incorrect. The majority's error conflates two separate concepts: the revealing nature of the *images* captured through the AIR program, and the revealing nature of the *identifying information*, like location information, that the AIR program collects about Baltimore's residents.

As the Supreme Court explained in *Carpenter,* a detailed chronicle of someone's location, itself, reveals "identifying information." *Carpenter*, 138 S. Ct. 2219-20; *see also United States v. Jones*, 565 U.S. 400, 430-31 (Alito, J., concurring). By continuously monitoring 90% of the City of Baltimore, the AIR program comprehensively chronicles the movements of almost everyone within the city during daylight hours. And collection of that location information is revealing, even if no individually identifiable *images* are recorded. One study, led by researchers at MIT (and relied on by Plaintiffs here), estimated that as few as *four* points of location data were enough to uniquely identify 95% of cellphone users; with just two datapoints, half of all people could be individually characterized. JA89-93.

The majority incorrectly suggested that representing individuals as "dots" in the AIR program's images preserves individual privacy. *See, e.g.*, Op. at 3, 6. Representing an individual as a "dot" is a crude attempt at anonymization that does little to guard against identification: it does not eliminate the quality, quantity, or sensitivity of the location information otherwise captured by the program. Indeed,

computer scientists have repeatedly shown that it is possible to "reidentify" or "deanonymize" individuals from ostensibly anonymous data. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1716 (2010). And as the *New York Times* recently demonstrated,[9] "precise, longitudinal geolocation information is absolutely impossible to anonymize." Thompson & Warzel, *Twelve Million Phones*; *see also United States v. Chatrie*, Order, Case No. 3:19-cr-00130 (E.D. Va. Jan. 7, 2020) (ECF 69) (granting motion to seal "anonymized" Google location data because redaction was insufficient to prevent re-identification).

Likewise, "limiting" the program's surveillance to 12 hours per day does not preclude monitoring an individual from day-to-day, and thus does not materially lessen the invasion of privacy. Consider a simple example: A single "dot" travels to a specific building in the evening, and a single dot reemerges from the building the next morning. This repeats, day-after-day, likely revealing a pattern: an individual returning to their residence at night and leaving in the morning. *See id*. at 34 (Gregory, C.J., dissenting). This pattern can be tied to an individual with just

[9] The *Times* obtained a large dataset of mobile geolocation information and was able to identify and track celebrities, law enforcement officers, "high-powered lawyers (and their guests)," and even a Secret Service agent assigned to President Trump. *See* Stuart Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

a few simple steps: first, identifying the address of the residence through widely available online tools (like Google Maps); and second, searching that address in law enforcement databases like a driver's license database, or any number of commonly available public or commercial databases.

Location information collected through the AIR program is likely sufficient on its own to uniquely identify almost any individual. But when AIR program surveillance is combined with other surveillance techniques, or other datasets available to Baltimore police, individual identification is practically guaranteed.

Indeed, the AIR program was designed with the layering of surveillance tools specifically in mind. The program's contract calls for combining aerial surveillance with Baltimore's existing surveillance capabilities, like surveillance cameras and automated license plate readers. *See, e.g.*, JA71 (AIR program contract noting analysts "will track individuals and vehicles" passing CCTV cameras and will "access or request" that video to "provide more detailed descriptions").

There is no shortage of such surveillance tools: the Baltimore Police Department's existing infrastructure is vast. Its CitiWatch program operates over 800[10] "state-of-the-art CCTV cameras" throughout the city that are "monitored 24

[10] BPD, Aerial Investigation Research Pilot Program (AIR) at 28:28, Facebook (Mar. 30, 2020), https://www.facebook.com/58771761955/videos/212014970074066.

hours a day and 365 days a year."[11] Baltimore also manages a "public-private" network of surveillance cameras—private cameras operated from an individual's home or small business—that Baltimore Police can access when a "public safety" event occurs.[12] And, using facial recognition technology, Baltimore Police can compare images obtained through these cameras against a database of 7 million drivers' license photos, 3 million state mug shots, and 24.9 million FBI mug shots.[13]

Further, the police department deploys both fixed and mobile automated license plate readers (ALPRs) throughout the city. In 2018, Baltimore's ALPRs scanned over 17,000,000 license plates.[14] A single ALPR scan associates a vehicle with a time and a place; and searching a license plate number in a state registration database then links that car with an individual registrant.

---

[11] Mayor's Office of Information Technology, *CitiWatch Services*, https://moit.baltimorecity.gov/community-services/citiwatch-services.

[12] City of Baltimore, *Our Community Values Public Safety*, https://citiwatch.baltimorecity.gov; Baltimore Police Department, *CitiWatch Community Partnership Overview*, https://www.baltimorepolice.org/community/citiwatch-community-partnership-overview.

[13] Clare Garvie *et al*., Georgetown Law Ctr. On Privacy & Tech., *The Perpetual Line- Up, Unregulated Police Face Recognition in America* (Oct. 18, 2016), https://www.perpetuallineup.org/sites/default/files/2016-10/12_MD.pdf.

[14] Maryland Coordination and Analysis Center, ALPR Reporting for 2018 (Feb. 22, 2019), https://www.documentcloud.org/documents/6146047-Maryland-State-Police-PS3-509-E-2019.html

Whether considered on its own or in conjunction with Baltimore's other surveillance tools, the AIR program's persistent, expansive reach is more invasive than the collection of CSLI deemed unconstitutional in *Carpenter*. *Compare* 138 S. Ct. at 2217 n.3 (holding seven days of Carpenter's historical CSLI constituted a search), *with* Op. at 35 (Gregory, C.J., dissenting) (AIR program provides "45 daytimes' worth of retroactive locational data" for a half-million Baltimore residents). And the AIR program is fundamentally unlike traditional surveillance cameras, which typically focus on a single location, or the more limited aerial surveillance or physical tracking techniques upheld by prior Supreme Court decisions. *See* Op. at 38-40 (Gregory, C.J., dissenting) (distinguishing cases).

A "central aim" of the Fourth Amendment is "to place obstacles in the way" of surveillance that is "too permeating" and to "assure [] preservation of that degree of privacy against government that existed" when the Amendment was adopted. *Carpenter*, 138 S. Ct. at 2214 (internal citations and quotations omitted). The AIR program is too permeating, and it dramatically reduces the degree of privacy afforded every resident of Baltimore.

II. The panel's decision conflicts with existing Fourth Amendment precedent on the "special needs" doctrine and other suspicionless searches.

The panel's alternative holding, that the AIR program satisfies Fourth Amendment scrutiny under "the balancing test used for programmatic searches," Op. at 10, is also erroneous.

Under the Fourth Amendment, no "balancing test" exists for programmatic searches undertaken for ordinary law enforcement purposes, like criminal investigations or prosecutions. *See United States v. Curry*, 965 F.3d 313, 318 (4th Cir. 2020) (en banc) (Diaz, J., concurring). Supreme Court precedent is clear that "warrantless searches are typically unreasonable where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing." *Carpenter*, 138 S. Ct. at 2221 (citations omitted). Exceptions to that rule are "jealously and carefully drawn." *Jones v. United States*, 357 U.S. 493, 499 (1958).

As the Chief Judge's dissent explained, any "'special need' justifying [a] suspicionless search must be beyond the normal need for law enforcement." Op. at 43 (Gregory, C.J., dissenting) (internal quotations omitted); *see also Delaware v. Prouse*, 440 U.S. 648, 659 n.18 (1979) (observing that a "special need" must be justified by something beyond "the general interest in crime control").

In *City of Indianapolis v. Edmond*, the Supreme Court struck down a municipal vehicle checkpoint program that was directed at interdicting illegal

drugs. 531 U.S. 32, 48 (2000). As the Court explained, "programs undertaken to 'detect evidence of ordinary criminal wrongdoing, even where the 'gravity of the threat' is high, cannot be justified as a special need." Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 Emory L. J. 527, 591 (2017) (quoting *Edmond*, 531 U.S. at 41-42). Thus, crime control—even where crime rates are high—cannot justify a program of warrantless, suspicionless searches.

There is only one possible understanding of the AIR program: it is a law enforcement investigative and crime-control tool. *See* Op. at 18 (describing program as an "important," "additional tool" to augment "law enforcement's best efforts"), 3 (describing AIR program as a "step taken by the BPD to strengthen its hand against violent crime"). The "special needs" cases, therefore, simply do not apply.

Equally problematic is the panel's reliance on inapposite precedents in which the Court upheld a suspicionless search of a person with a diminished expectation of privacy. For example, the majority's reliance on *Samson v. California*, 547 U.S. 843 (2006), is misplaced. In *Samson*, the "petitioner's status as a parolee," which the Court considered "an established variation on imprisonment," rendered, in the Court's view, the petitioner without "an expectation of privacy that society would recognize as legitimate." *Id.* at 852

(citations omitted). Likewise, in *Maryland v. King*, 133 U.S. 1958 (2013), the Court upheld government-mandated DNA collection from certain classes of arrestees, holding that a DNA swab did not violate the arrestee's expectation of privacy in "the context of a valid arrest supported by probable cause." *Id.* at 465. In a case, like this one, where the subject of a search has an undiminished expectation of privacy, the Court has never countenanced this approach.

Expanding the "special needs" doctrine to encompass a program like this—one directed only at solving crimes—represents a dramatic and dangerous expansion. The Court should reconsider the panel's decision en banc to guard against such an expansion and to secure "the privacies of life" from this "tireless" surveillance. *Carpenter*, 138 S. Ct. at 2214, 2218.

Conclusion

Amici respectfully support Plaintiffs' petition for rehearing en banc.

Dated: November 25, 2020

Respectfully submitted,

/s/ Sophia Cope
Sophia Cope
Counsel of Record

Mark Rumold
Adam Schwartz
Saira Hussain
Hannah Zhao
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street

San Francisco, CA 94109
(415) 436-9333
sophia@eff.org

Rachel Levinson-Waldman
Laura Hecht-Felella
BRENNAN CENTER FOR JUSTICE AT
NYU SCHOOL OF LAW
1140 Connecticut Ave. NW, Suite 1150
Washington, DC 20036

Elizabeth Franklin-Best
NATIONAL ASSOCIATION OF CRIMINAL
DEFENSE LAWYERS
Elizabeth Franklin-Best, P.C.
2925 Devine Street
Columbia, South Carolina 29205

John W. Whitehead
Douglas R. McKusick
RUTHERFORD INSTITUTE
109 Deerwood Road
Charlottesville, VA 22906

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(4) because this brief contains 2,592 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2016, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: November 25, 2020

/s/ Sophia Cope
Sophia Cope

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system on November 25, 2020.

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

Dated: November 25, 2020

/s/ Sophia Cope
Sophia Cope

Counsel of Record for Amici Curiae

ADDENDUM - LIST OF AMICI CURIAE

The **Electronic Frontier Foundation** ("EFF") is a member-supported, non-profit organization that has worked for 30 years to ensure that technology supports freedom, justice, and innovation for all people of the world. Through direct advocacy, impact litigation, and technological innovation, EFF's team of attorneys, activists, and technologists encourage and challenge industry, government, and the courts to support free expression, privacy, and transparency in the information society. EFF has over 37,000 dues-paying members, and represents the interests of technology users in court cases and policy debates concerning the application of law in the digital age. EFF regularly participates as amicus, in this Court and other federal courts, in cases concerning Fourth Amendment rights in the digital age, including *Carpenter v. United States,* 138 S. Ct. 2206 (2018); *United States v. Jones*, 565 U.S. 400 (2012); *United States v. Bosyk*, 933 F.3d 319 (4th Cir. 2019); *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018); and *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2016).

The **Brennan Center for Justice at NYU School of Law** is a nonpartisan public policy and law institute focused on fundamental issues of democracy and justice. The Center's Liberty and National Security ("LNS") Program uses innovative policy recommendations, litigation, and public advocacy to advance effective national security policies that respect the rule of law and constitutional

values. The LNS Program is particularly concerned with domestic intelligence gathering policies, including the dragnet collection of Americans' communications and personal data, and the concomitant effects on First and Fourth Amendment freedoms. As part of its work in this area, the Center has filed numerous amicus briefs on behalf of itself and others in cases involving electronic surveillance and privacy issues, including in *Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); and *Carpenter v. United States*, 138 S. Ct. 2206 (2018). The Brennan Center also publishes scholarship on the privacy of personal data. *See* Angel Diaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, Brennan Center (Sept. 10, 2020);[1] Rachel Levinson-Waldman, *Cellphones, Law Enforcement, and the Right to Privacy*, Brennan Center (Dec. 20, 2018);[2] Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 Emory L.J. 537 (2017).

The **Electronic Privacy Information Center** ("EPIC") is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public

[1] https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations

[2] https://www.brennancenter.org/our-work/research-reports/cellphones-law-enforcement-and-right-privacy

attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC routinely participates as amicus curiae in cases concerning the impact of emerging technologies on constitutional rights. In particular, EPIC seeks to prevent new surveillance tools and police practices from eroding the privacy protections of the First and Fourth Amendments.

FreedomWorks Foundation is a non-profit, non-partisan grassroots organization dedicated to upholding free markets and constitutionally limited government. Founded in 2004, FreedomWorks Foundation is among the largest and most active right-leaning grassroots organizations, amplifying the voices of millions of activists both online and on the ground. FreedomWorks Foundation has been actively involved since 2013 in education about the dangers to due process, free speech, and dissent posed by warrantless mass surveillance, including the burgeoning use of wide-area video surveillance and facial recognition.

The **National Association of Criminal Defense Lawyers** ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of many thousands of direct members, and more than 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders,

military defense counsel, law professors, and judges. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers. NACDL is dedicated to advancing the proper, efficient, and just administration of justice. NACDL files numerous amicus briefs each year in the U.S. Supreme Court and other federal and state courts, seeking to provide amicus assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole. NACDL has a particular interest in cases that involve surveillance technologies and programs that pose new challenges to personal privacy. The NACDL Fourth Amendment Center offers training and direct assistance to defense lawyers handling such cases in order to help safeguard privacy rights in the digital age. NACDL has also filed numerous amicus briefs in this Court and the Supreme Court on issues involving digital privacy rights, including: *Carpenter v. United States,* 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014); and *United States v. Jones*, 565 U.S. 400 (2012).

The **Rutherford Institute** is an international nonprofit organization headquartered in Charlottesville, Virginia. Founded in 1982 by its President, John W. Whitehead, the Institute specializes in providing legal representation without charge to individuals whose civil liberties are threatened or infringed and in educating the public about constitutional and human rights issues. The Rutherford

Institute works tirelessly to resist tyranny and threats to freedom, ensuring that the government abides by the rule of law and is held accountable when it infringes on the rights guaranteed to persons by Constitution and laws of the United States.