

No. 20-1495

**UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT**

LEADERS OF A BEAUTIFUL STRUGGLE; ERRICKA BRIDGEFORD;
KEVIN JAMES,

Plaintiffs-Appellants,

v.

BALTIMORE POLICE DEPARTMENT; MICHAEL S. HARRISON, in his
official capacity as Baltimore Police Commissioner,

Defendants-Appellees.

On Appeal from the United States District Court for the District of Maryland, at
Baltimore. Richard D. Bennett, District Judge. (1:20-cv-00929-RDB)

**BRIEF OF AMICUS CURIAE CENTER ON PRIVACY & TECHNOLOGY
AT GEORGETOWN LAW IN SUPPORT OF APPELLANTS' PETITION
FOR REHEARING EN BANC**

Laura Moy
Counsel of Record
Michael Rosenbloom
Communications & Technology Law
Clinic, Georgetown Law
600 New Jersey Avenue NW
Washington, DC 20001
(202) 662-9547
Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES	ii
INTERESTS OF AMICUS CURIAE	1
SUMMARY OF ARGUMENT.....	2
ARGUMENT	4
I. This is a case of exceptional importance because if left undisturbed, it could be seen to green light massive programmatic surveillance of low-income communities of color.....	4
II. The panel majority’s assessment of the intrusiveness of the AIR program rests on a fundamental misunderstanding of the facts.	5
III. The majority departs from <i>Carpenter v. U.S.</i>	9
IV. The majority departs from precedent outlining limited exceptions to the warrant requirement.	12
CONCLUSION	15
CERTIFICATE OF COMPLIANCE	16
CERTIFICATE OF SERVICE.....	17

TABLE OF AUTHORITIES

Cases

<i>Carpenter v. U.S.</i> , 138 S. Ct. 2206 (2018)	passim
<i>Delaware v. Prouse</i> , 440 U.S. 648, 649 (1979).....	13
<i>Ferguson v. City of Charleston</i> , 532 U.S. 67, 68 (2001).....	13, 14
<i>Katz v. United States</i> , 389 U.S. 347, 357 (1967)	12
<i>Leaders of a Beautiful Struggle v. Baltimore Police Department</i> , No. 20-1495	passim
<i>Michigan Dept. of State Police v. Sitz</i> , 496 U.S. 444, 451 (1990)	13
<i>National Treasury Employees Union v. Von Raab</i> , 489 U.S. 656 (1989).....	14
<i>U.S. v. Jones</i> , 565 U.S. 400 (2012).....	11
<i>United States v. Graham</i> , 824 F.3d 421 (4th Cir. 2015).....	3, 11

Other Authorities

Adam Tanner, <i>Harvard Professor Re-Identifies Anonymous Volunteers In DNA Study</i> , Forbes (Apr. 25, 2013),	7
Civil Rights Privacy and Technology Table, <i>Principles</i> , https://www.civilrightstable.org/principles/	5
Clare Garvie, et al., <i>America Under Watch: Face Surveillance in the United States</i> , https://www.americaunderwatch.com/	5
Clare Garvie, et al., <i>The Perpetual Line-Up: Unregulated Police Face Recognition in America at E: Racial Bias</i> , https://www.perpetuallineup.org/findings/racial-bias	4

Electronic Frontier Foundation, <i>Street-Level Surveillance: Surveillance Cameras</i> , https://www.eff.org/pages/surveillance-cameras	9
James Vincent, <i>AI Researchers Tell Amazon to Stop Selling 'Flawed' Facial Recognition to the Police</i> (Apr. 3 2019), <i>The Verge</i> , https://www.theverge.com/2019/4/3/18291995/amazon-facial-recognition-technology-rekognition-police-ai-researchers-ban-flawed	5
Karl Bode, <i>Anonymized Data Really Isn't Anonymous: Vehicle Data Can Easily Be Used To Identify You</i> , <i>Techdirt</i> (May 31, 2016), https://www.techdirt.com/articles/20160526/06352934550/anonymized-data-really-isnt-anonymous-vehicle-data-can-easily-be-used-to-identify-you.shtml	8
Karl Bode, <i>Once More With Feeling: 'Anonymized' Data Is Not Really Anonymous</i> , <i>Techdirt</i> (July 30, 2019), https://www.techdirt.com/articles/20190723/08540542637/once-more-with-feeling-anonymized-data-is-not-really-anonymous.shtml	6
Kevin Strom, <i>Research on the Impact of Technology on Policing Strategy in the 21st Century, Final Report</i> , https://www.ncjrs.gov/pdffiles1/nij/grants/251140.pdf	4
Philippe Golle and Kurt Partridge, <i>On the Anonymity of Home/Work Location Pairs</i> , Springer Link (2009), https://link.springer.com/chapter/10.1007/978-3-642-01516-8_26	8
Sébastien Gambs, et al., <i>De-anonymization attack on geolocated data</i> , ScienceDirect (Dec. 2014),.....	8
Simone Brown, <u><i>Dark Matters: On the Surveillance of Blackness</i></u> (2015)	4
Virginia Eubanks, <u><i>Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor</i></u> (2018)	4

- Wei-han Lee, et al., *Blind Deanonimization Attacks Using Social Networks*,
Arxiv (Oct. 30, 2017), <https://arxiv.org/pdf/1801.05534.pdf>..... 7
- Yves-Alexandre de Montjoye, et al., *Unique in the Crowd: The privacy bounds
of human mobility*, *Nature* (Mar. 25, 2013),
<https://www.nature.com/articles/srep01376> 7
- Yves-Alexandre de Montjoye, et al., *Unique in the shopping mall: On the
reidentifiability of credit card metadata*, *Science* (Jan 30, 2015),
[https://science.sciencemag.org/content/347/6221/536.full?ijkey=4rZ2e
FPUrlLGw&keytype=ref&siteid=sci](https://science.sciencemag.org/content/347/6221/536.full?ijkey=4rZ2eFPUrlLGw&keytype=ref&siteid=sci)..... 7

INTERESTS OF AMICUS CURIAE¹

The Center on Privacy & Technology at Georgetown Law is a think tank focused on privacy and surveillance law and policy. The Center has an interest in protecting the privacy of historically marginalized communities, who often are disparately impacted by surveillance programs while simultaneously neglected in privacy debates. The Center has done extensive research and advocacy concerning police surveillance technology, including a series of groundbreaking reports on police use of facial recognition technology.

¹ Amicus confirms that no party or counsel for any party authored this brief in whole or in part, and that no person other than amici or their counsel made any monetary contribution intended to fund the preparation or submission of this brief.

SUMMARY OF ARGUMENT

The Center files this brief supporting *en banc* review to highlight both an issue of exceptional importance and a conflict with Supreme Court precedent.² First, programmatic surveillance programs like Aerial Investigation Research (AIR) enable privacy invasions disproportionately in low-income and non-white communities. Second, the majority opinion departs from precedent set in *Carpenter v. U.S.*, 138 S. Ct. 2206 (2018).

If allowed to stand, the panel majority's decision would clear the way for similar surveillance in other cities, subjecting low-income communities of color to further disproportionate surveillance.

The majority opinion appears to rest on a fundamental misunderstanding about how AIR operates. Although AIR photographs display people as dots, these photographs are then cross-referenced with other data to identify individuals. The Baltimore Police Department (BPD) can combine AIR data with security cameras or license-plate readers to track down specific persons. Research demonstrates that it is possible to

² This brief was prepared with the substantial research and drafting assistance of Victoria Tang, Teaching Fellow at the Georgetown Communications & Technology Law Clinic, as well as clinic students Samuel Hanks and Mariestela Somarriba.

uncover the identity of a previously anonymous person by combining just a few datasets.

The majority's opinion also is inconsistent with precedent and key facts established in *Carpenter v. U.S.*, a case involving information that is in many ways less precise than AIR's photography. Additionally, this is an opportunity to rectify the Fourth Circuit's earlier holding in *United States v. Graham*, 824 F.3d 421 (4th Cir. 2015), which deemed cell site location information unprotected under the Fourth Amendment.

The majority gives law enforcement excessive power to conduct unfettered aerial surveillance; it attempts to justify AIR as a programmatic search using the language of a special needs exception, but cites no special need. In fact, the AIR program is explicitly justified as routine crime control.

ARGUMENT

I. This is a case of exceptional importance because if left undisturbed, it could be seen to green light massive programmatic surveillance of low-income communities of color.

The panel majority's holding would green light a proliferation of suspicionless surveillance programs. Police agencies across the country have and continue to adopt high-tech surveillance programs that, like AIR, are invasive in novel ways, including through use of body cameras, drones, and always-on face surveillance.³

These initiatives significantly harm low-income communities of color. Research shows that when advanced surveillance technologies are instituted programmatically, these programs disproportionately impact low-income communities of color.⁴ In addition to violating important civil rights principles,⁵ these technologies often are less accurate when used on non-white populations.⁶ The panel holding would encourage police to

³ See Kevin Strom, *Research on the Impact of Technology on Policing Strategy in the 21st Century, Final Report*, <https://www.ncjrs.gov/pdffiles1/nij/grants/251140.pdf>.

⁴ Clare Garvie, et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America* at E: Racial Bias, <https://www.perpetuallineup.org/findings/racial-bias>. See generally Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (2018); Simone Brown, *Dark Matters: On the Surveillance of Blackness* (2015).

⁵ Civil Rights Privacy and Technology Table, *Principles*, <https://www.civilrightstable.org/principles/>.

⁶ James Vincent, *AI Researchers Tell Amazon to Stop Selling 'Flawed' Facial Recognition to the Police* (Apr. 3 2019), *The Verge*,

implement more biased and flawed surveillance programs, exacerbating existing problems with police use of technology.

II. The panel majority's assessment of the intrusiveness of the AIR program rests on a fundamental misunderstanding of the facts.

The panel majority does not recognize just how invasive AIR is because it misunderstands the increasing ease with which individual people can be identified from seemingly anonymous data. BPD uses AIR in concert with other tools like security cameras and license-plate readers. Data from all these sources can easily be combined to identify an individual. Indeed, the program was designed to help pinpoint specific people. *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 at 3–4. The majority thus misses the point when it contends AIR is only “used to track non-identified individuals.” *Leaders* at 17. People do appear as dots in AIR photographs. *Id.* But a simple cross-reference of the AIR dataset to other data *in BPD's possession* can reveal race, gender, or other identifying characteristics of each dot – or each individual.

<https://www.theverge.com/2019/4/3/18291995/amazon-facial-recognition-technology-rekognition-police-ai-researchers-ban-flawed>. See also Clare Garvie, et al., *America Under Watch: Face Surveillance in the United States*, <https://www.americaunderwatch.com/>.

Numerous experiments have demonstrated how seemingly “anonymous” data can be used to ascertain an individual’s identity. For example, researchers correctly “de-anonymized” supposedly anonymous people with 99.98% accuracy using datasets like age, gender, and marital status.⁷ In another study, people anonymously shared their DNA, but a researcher uncovered their names using datasets like ZIP code, date of birth, and medical conditions.⁸ Social media researchers have de-anonymized users solely through their connections.⁹ And 90% of 1.1 million people’s credit card records were de-anonymized using only four pieces of information.¹⁰

Location data is particularly identifiable. In studies, researchers successfully identified 95% of individuals using only four smartphone

⁷ Karl Bode, *Once More With Feeling: ‘Anonymized’ Data Is Not Really Anonymous*, Techdirt (July 30, 2019), <https://www.techdirt.com/articles/20190723/08540542637/once-more-with-feeling-anonymized-data-is-not-really-anonymous.shtml>.

⁸ Adam Tanner, *Harvard Professor Re-Identifies Anonymous Volunteers In DNA Study*, Forbes (Apr. 25, 2013), <https://www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/?sh=20f21c1392c9>.

⁹ Wei-han Lee, et al., *Blind Deanonymization Attacks Using Social Networks*, Arxiv (Oct. 30, 2017), <https://arxiv.org/pdf/1801.05534.pdf>.

¹⁰ Yves-Alexandre de Montjoye, et al., *Unique in the shopping mall: On the reidentifiability of credit card metadata*, Science (Jan 30, 2015), <https://science.sciencemag.org/content/347/6221/536.full?ijkey=4rZ2eFPUrlLGw&keytype=ref&siteid=sci>.

locations,¹¹ or identified drivers by something as small as their recorded brake pedal usage.¹² In a study of data analogous to that collected by AIR, researchers showed that specific people can be identified from nameless geolocation data by tracing visits to certain points of interest.¹³ A mere two locations of interest – that of a person’s presumed home and that of their presumed work – are typically sufficient to identify a specific individual.¹⁴

In the case at hand, the potential de-anonymization of the “dots” is not mere theory – BPD already possesses the information it needs to identify specific individuals in its AIR data and track their detailed movements over time. In addition to employing a team of analysts to examine AIR photographs, BPD combines AIR data with other databases such as automated license-plate readers and the “CitiWatch” network of more than 800 cameras. Petition for Rehearing En Banc at 4. When the

¹¹ Yves-Alexandre de Montjoye, et al., *Unique in the Crowd: The privacy bounds of human mobility*, *Nature* (Mar. 25, 2013), <https://www.nature.com/articles/srep01376>.

¹² Karl Bode, *Anonymized Data Really Isn't Anonymous: Vehicle Data Can Easily Be Used To Identify You*, *Techdirt* (May 31, 2016), <https://www.techdirt.com/articles/20160526/06352934550/anonymized-data-really-isnt-anonymous-vehicle-data-can-easily-be-used-to-identify-you.shtml>.

¹³ Sébastien Gambs, et al., *De-anonymization attack on geolocated data*, *ScienceDirect* (Dec. 2014), <https://www.sciencedirect.com/science/article/pii/S0022000014000683>.

¹⁴ Philippe Golle and Kurt Partridge, *On the Anonymity of Home/Work Location Pairs*, Springer Link (2009), https://link.springer.com/chapter/10.1007/978-3-642-01516-8_26.

panel majority admitted that “BPD can take advantage of existing networks of cameras and license plate readers,” it highlighted this precise issue.

Leaders at 18. More concerningly, these are only the datasets to which we already know the BPD has easy access.

The majority points out that in *Carpenter* the Supreme Court stated that traditional surveillance tools, “specifically security cameras,” remain lawful to operate without a warrant. But AIR is not a traditional surveillance tool. *Leaders*, No. 20-1495 at 12. Affixed security cameras capture a person’s presence only within a locally limited zone.¹⁵ In contrast, AIR oversees 90% of Baltimore at any given time. Petition for Rehearing En Banc at 1. The average Baltimorean who routinely goes outside would likely be unable to escape from AIR’s panopticon.

As the Supreme Court noted in *Carpenter v. U.S.*, the fact that an inference must be made from collected data does not mean it was not a search. 138 S. Ct. at 2218 (citing *Kyllo*, 533 U.S. at 36, 121). When the *Carpenter* Court held that law enforcement’s use of CSLI to track down a suspect constituted a search under the Fourth Amendment, it explained

¹⁵ Electronic Frontier Foundation, *Street-Level Surveillance: Surveillance Cameras*, <https://www.eff.org/pages/surveillance-cameras>.

that “the Government could, *in combination with other information*, deduce a detailed log of Carpenter’s movements, including when he was at the site of the robberies.” *Id.* (emphasis added). *Carpenter* accounted for the reality of living in 2020, when it is difficult to avoid not only constant data collection but also the linking of datasets to re-identify individuals. In addition, the *Carpenter* Court warned, “Courts should be wary of ‘a too permeating police surveillance.’” *Id.* at 2214 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). By itself, AIR is already overly pervasive and invasive. Petition for Rehearing En Banc at 3–6. Applying the Fourth Amendment to modern surveillance practices requires understanding how a tool that tracks “dots” superficially can actually show defining characteristics of individuals in reality.

III. The majority departs from *Carpenter v. U.S.*

The court should also rehear this case because the majority’s opinion departs from Supreme Court precedent set in *Carpenter v. U.S.* In *Carpenter*, the Court considered privacy based not only on the information directly collected by the government, but also on the details of Carpenter’s movements that could be inferred from that information. *See* 138 S. Ct. at 2218. Here, the majority failed to focus on this fuller scope. As shown

above, advances in computing have made it easier than ever to gain a comprehensive insight into a person's private life from smaller and smaller collections of data.

Indeed, in many ways the AIR program is more precise and intrusive than the cell-site location information (CSLI) at issue in *Carpenter*. There, each CSLI datapoint only showed a subject's location within the range of a cell site, typically "one-eighth to four square miles." *Id.* Here, when AIR captures a person or vehicle, it can detect with far greater precision where in space the subject is. The majority admits that AIR is capable of determining positions of subjects at crime scenes, which is far more precise than mere presence within the range of a particular cell tower. *Leaders* at 3.

Additionally, the AIR program is more factually intrusive than CSLI because it fills in gaps in BPD's other, preexisting surveillance programs. AIR surpasses prior programs because it scans almost the entirety of the public space in Baltimore, and AIR's continuous daytime tracking covers most outside human movement. AIR's 45-day retention period, while shorter than the period at issue in *Carpenter*, is more than enough to form a comprehensive record of a person's movements. The GPS tracking

program at issue in *U.S. v. Jones*, 565 U.S. 400 (2012), featured only a 28-day duration.

The Fourth Circuit makes the same mistake here as it did in *United States v. Graham*: focusing too heavily on the specific mechanisms of the surveillance without also examining the total scope of information gleaned from that surveillance. See 824 F.3d at 435-36 (4th Cir. 2015). In *Graham*, the Court admitted that, were it “writing from a clean slate” it may have ruled that individuals held a reasonable expectation of privacy to “large quantities of location information, even if they have shared that information with a phone company,” but the Court felt constrained by its own analysis of the third-party doctrine. *Id.* at 436. *Carpenter* has created exactly that clean slate. In finding that a person has a reasonable expectation of privacy in “the whole of their physical movements,” 138 S. Ct. at 2219, the Supreme Court paved the way for this Court to analyze the AIR program similarly.

IV. The majority departs from precedent outlining limited exceptions to the warrant requirement.

Without finding that AIR's searches are specifically exempted from the warrant requirement, the majority cannot properly proceed to its balancing test.

In the case at hand, only the catch-all special needs doctrine should even be considered for a possible exception to the warrant requirement for AIR, because other warrant exceptions require special circumstances not present here. Only certain specific situations necessitate warrantless suspicionless searches. *Katz v. United States*, 389 U.S. 347, 357 (1967). The majority relates AIR to other programmatic searches, but each of the cited programs concerns a special circumstance. *Leaders* at 9-10. This is not a border search nor a search of incarcerated people, but a search of everyone visibly outdoors in Baltimore.

However, the majority does not even appear to analyze whether the program fulfills any special need, but instead proceeds straight to a test balancing "the burden on constitutional rights against other law enforcement and public safety needs." *Leaders* at 15-16. The majority opinion never explicitly mentions the special needs doctrine, instead

presenting the program as variously meeting a “serious law enforcement need” or “addressing imperatives of public safety.” *Id.*

AIR does not actually fulfill any special need of law enforcement, so it cannot meet the doctrine’s requirements. In limited “special needs” circumstances, suspicionless searches may be reasonable if those special needs are balanced against privacy and other interests. Importantly, this exception applies only to programs “divorced from the State’s general law enforcement interest,” *Ferguson v. City of Charleston*, 532 U.S. 67, 68 (2001), such as preventing car crashes caused by intoxicated driving. *Michigan Dept. of State Police v. Sitz*, 496 U.S. 444, 451 (1990). The Supreme Court has held that the Fourth Amendment’s warrant requirement is necessary to restrict officer discretion and has struck down programs that fail to restrict it. *Delaware v. Prouse*, 440 U.S. 648, 649 (1979).

In fact, the majority recognizes that the purpose of the AIR program is standard crime control. The majority notes that the program “serves critical governmental purposes” by responding to a city “plagued by violent crime” and addressing holes in existing surveillance networks. *Leaders* at 18. A police department implementing a program to address

violent crime is quintessential crime control – entirely a “general law enforcement interest.” *Ferguson*, 532 U.S. at 68.

The majority cites *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989), for the standard, but the facts in *Von Raab*, unlike the case at hand, offer a clear example of a program instituted to fulfill a special need. In *Von Raab*, the Supreme Court held that an employee drug testing program was reasonable precisely because it was outside of ordinary law enforcement needs:

The purposes of the program are to deter drug use among those eligible for promotion to sensitive positions within the Service and to prevent the promotion of drug users to those positions. These substantial interests . . . present a special need that may justify departure from the ordinary warrant and probable-cause requirements.

Id. at 666.

The special needs doctrine exists to allow for drug test programs to ensure sobriety or prevent intoxicated driving, not aerial surveillance programs to prevent and respond to crimes.

CONCLUSION

The Center on Privacy & Technology at Georgetown Law urges the Court to grant Appellants' Motion for Rehearing en banc so that the Court can address the significant harms that this holding could inflict on low-income communities of color, accurately assess the factual intrusiveness of this surveillance, and fully apply *Carpenter's* analysis to the AIR program.

Dated: November 27, 2020

Respectfully Submitted,

/s/ Laura M. Moy

Laura M. Moy

Counsel of Record

Michael Rosenbloom

Communications & Technology

Law Clinic, Georgetown Law

600 New Jersey Avenue, NW

Washington, DC 20001

(202) 662-9547

CERTIFICATE OF COMPLIANCE

Under the Federal Rules of Appellate Procedure 29(a)(4)(G), I hereby certify the following:

This brief complies with the word limit of Rule 29(a)(5) as it is 2594 words long, which is within the limit of 2600 words, excluding those parts of the brief that are exempted under Rule 32(f).

This brief complies with the typeface requirements of Rule 32(a)(5) and 32(a)(6), as this brief's text was prepared in a proportionally spaced Roman typeface, 14-point Book Antiqua, in Microsoft Word.

Dated: November 27, 2020

/s/ Laura M. Moy

Laura M. Moy

Michael Rosenbloom

CERTIFICATE OF SERVICE

I certify that I electronically filed this document with the Clerk of the Court using the appellate CM/ECF system on November 27, 2020. All participants in the case are registered CM/ECF users and service will be accomplished by the appellate CM/ECF system.

/s/ Laura M. Moy

Laura M. Moy

Michael Rosenbloom

No. 20-1495

**UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT**

LEADERS OF A BEAUTIFUL STRUGGLE; ERRICKA BRIDGEFORD;
KEVIN JAMES,

Plaintiffs-Appellants,

v.

BALTIMORE POLICE DEPARTMENT; MICHAEL S. HARRISON, in his
official capacity as Baltimore Police Commissioner,

Defendants-Appellees.

On Appeal from the United States District Court for the District of Maryland, at
Baltimore. Richard D. Bennett, District Judge. (1:20-cv-00929-RDB)

**MOTION FOR LEAVE TO FILE BRIEF OF CENTER ON PRIVACY AND
TECHNOLOGY AT GEORGETOWN LAW AS *AMICUS CURIAE* IN
SUPPORT OF APPELLANTS' PETITION FOR REHEARING EN BANC**

Laura Moy
Counsel of Record
Michael Rosenbloom
Communications & Technology Law
Clinic, Georgetown Law
600 New Jersey Avenue NW
Washington, DC 20001
(202) 662-9547

MOTION FOR LEAVE TO FILE BRIEF OF THE CENTER ON PRIVACY & TECHNOLOGY AT GEORGETOWN LAW AS *AMICUS CURIAE* IN SUPPORT OF APPELLANTS' PETITION FOR REHEARING EN BANC

The Center on Privacy and Technology at Georgetown Law, by and through undersigned counsel, respectfully moves for leave to file a 2594 word amicus curiae brief pursuant to Rule 29 of the Federal Rules of Appellate Procedure, in support of Appellants' Petition for rehearing en banc. Amicus states the following:

1. The Center on Privacy & Technology at Georgetown Law is a think tank focused on privacy and surveillance law and policy.

2. The Center has an interest in safeguarding the privacy rights of everyday people from illegal government and corporate surveillance. The Center especially focuses on protecting the privacy of historically marginalized communities, who are neglected in discussions about surveillance programs yet often disparately impacted by them. The Center advocates for careful consideration of race, class, and power in privacy policy.

3. The proposed amicus brief is helpful to the Court. It shows how the panel majority's holding will lead to harm to low-income communities of color from disproportionate surveillance, and how the majority's

holding conflicts with Supreme Court precedent in *Carpenter v. U.S.*, 138 S. Ct. 2206 (2018).

4. All parties have consented to this filing.

For the foregoing reasons, amicus respectfully requests the Court grant this motion for leave to file the accompanying amicus curiae brief.

Respectfully Submitted,

/s/ Laura M. Moy

Laura M. Moy

Counsel of Record

Michael Rosenbloom

Communications & Technology

Law Clinic, Georgetown Law

600 New Jersey Avenue NW

Washington, DC 20001

(202) 662-9547

CERTIFICATE OF SERVICE

I hereby certify that on November 27, 2020 I electronically filed the foregoing motion and attached amicus curiae brief using the CM/ECF system. Counsel for all parties are registered CM/ECF users and will be served through CM/ECF.

Respectfully Submitted,

/s/ Laura M. Moy

Laura M. Moy

Counsel of Record

Michael Rosenbloom

Communications & Technology

Law Clinic, Georgetown Law

600 New Jersey Avenue NW

Washington, DC 20001

(202) 662-9547

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
APPEARANCE OF COUNSEL FORM

BAR ADMISSION & ECF REGISTRATION: If you have not been admitted to practice before the Fourth Circuit, you must complete and return an [Application for Admission](#) before filing this form. If you were admitted to practice under a different name than you are now using, you must include your former name when completing this form so that we can locate you on the attorney roll. Electronic filing by counsel is required in all Fourth Circuit cases. If you have not registered as a Fourth Circuit ECF Filer, please complete the required steps at [Register for eFiling](#).

THE CLERK WILL ENTER MY APPEARANCE IN APPEAL NO. 20-1495 as

Retained Court-appointed(CJA) CJA associate Court-assigned(non-CJA) Federal Defender

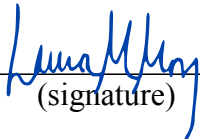
Pro Bono Government

COUNSEL FOR: Center on Privacy & Technology at Georgetown Law

as the

(party name)

appellant(s) appellee(s) petitioner(s) respondent(s) amicus curiae intervenor(s) movant(s)


 (signature)

Please compare your information below with your information on PACER. Any updates or changes must be made through PACER's [Manage My Account](#).

Laura M. Moy
 Name (printed or typed)

202-662-9547
 Voice Phone

Georgetown University
 Firm Name (if applicable)

 Fax Number

600 New Jersey Ave NW

Washington, DC 20001
 Address

laura.moy@georgetown.edu
 E-mail address (print or type)

CERTIFICATE OF SERVICE (required for parties served outside CM/ECF): I certify that this document was served on _____ by personal delivery; mail; third-party commercial carrier; or email (with written consent) on the following persons at the addresses or email addresses shown:

 Signature

 Date