

No. 12-4659

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

UNITED STATES OF AMERICA,
Plaintiff/Appellee,

v.

AARON GRAHAM and ERIC JORDAN,
Defendants/Appellants.

**On Appeal from the United States District Court
for the District of Maryland, Northern Division
(The Honorable Richard D. Bennett)**

SUPPLEMENTAL REPLY BRIEF OF APPELLANTS

JAMES WYDA
Federal Public Defender
MEGHAN S. SKELTON
Appellate Attorney
6411 Ivy Lane, Suite 710
Greenbelt, Maryland 20770
(301) 344-0600

Counsel for Aaron Graham

RUTH VERNET
Ruth J. Vernet Esq., LLC

31 Wood Lane
Rockville, MD 20850
(301) 251-9500

Counsel for Eric Jordan

ARGUMENT

The government finds no support in *Riley*. In the face of overwhelming authority to the contrary, and its own line prosecutors' arguments to juries, the government doggedly clings to its claim that CSLI just approximates location. (Gov. Supp. Br. 6.) The Supreme Court, on the other hand, concludes the opposite.¹ *Riley v. California*, 134 S. Ct. 2473, 2490 (2014) (noting that historic CSLI can trace an individual inside a building). *See also* JA 2056-60, 2446, 2663-66; *In re Application*, 724 F.3d 600, 609 (5th Cir. 2013).

The government is quite candid in its brief that it wishes to use cell phone location data to conduct dragnet surveillance without any individualized suspicion, or even a belief that a crime has occurred. It claims that CSLI is a simple building block at the beginning of an investigation that is the equivalent of chatting with bystanders.² *Riley* refused to countenance this warrantless practice when it explained

¹ Even if the illusory limit on the intrusion into an individual's reasonable expectation of privacy that the government describes were true several years ago, it no longer is. And the degree of privacy intrusion will only increase as the number and density of cell towers multiplies. The Supreme Court already rejected a similar government argument that, because a "relatively crude" technology resulted in a limited privacy intrusion, no Fourth Amendment violation occurred. The Court decided that faith in the government's assurances would "leave the homeowner at the mercy of advancing technology," recognizing that "the rule we adopt must take account of more sophisticated systems that are already in use or in development." *United States v. Kyllo*, 533 U.S. 27, 35-36 (2001).

² Here, this argument is demonstrably false. Appellants had already been arrested and indicted—and multiple search warrants had already been issued—before

that location data qualifies as one of the “privacies of life” that the Fourth Amendment protects. 134 S. Ct. at 2490, 2495. The Court has never approved this type of warrantless surveillance of location information. *See United States v. Jones*, 132 S. Ct. 945, 952 n.6 (2012) (contrasting other location tracking from the “dragnet-type law enforcement practices” that GPS tracking makes possible).

The government complains that the warrant requirement imposes too heavy a burden on law enforcement, which is yet another argument that *Riley* already considered and rejected. (Gov. Supp. Br. 5.) “We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime.” 134 S. Ct. at 2493. “Police efficiency,” the Court explained, does not trump the Fourth Amendment, particularly where (like here) law enforcement seeks to rummage through private data, unrestrained, with “revised general warrants” like those that inspired the Fourth Amendment in the first place. *See id.* at 2493-94.

In the same vein, the government tries to deflect attention away from the reasonable expectation of privacy that *Riley* recognized by insisting that it enjoys fundamental and comprehensive subpoena power. It of course also has the power to obtain search warrants. The ability to issue subpoenas says nothing about complying with the warrant requirement when the Fourth Amendment so directs. *Riley*, in step with the parade of recent CSLI decisions and statutes, indicates that, if it wants to use

the government first sought the 18 U.S.C. § 2703(d) orders. (JA 154, 174, 183, 191, 199, 209.) In fact, some of the warrants were to search the *cell phones*.

CSLI in an investigation, the government needs to get a warrant, not a subpoena.

Also steadfast in the face of *Riley's* contrary conclusion, the government adheres to the notion that the service provider's nominal, limited possession of the data removes it from an individual's private sphere.³ *Riley*, however, drew no meaningful distinction between locally stored data and cloud-based data. *Id.* at 2491, 2388. Cell service providers, like other cloud-based technologies, incidentally accumulate massive quantities of information about users that, when aggregated, implicate significant privacy rights. *Riley* recognized a reasonable expectation of privacy in this data, even if the government refuses to do so. *See id.* at 2489-90.

The government might think that a single federal statute defines reasonableness under the Fourth Amendment, but this Court should consider the growing chorus of voices from the broader community and look to the list of jurisdictions that requires warrants before the government may track a person's private movements using historic CSLI. Section 2703(d) violates the Fourth Amendment.

³ Contrary to the government's assertion, nobody at Sprint witnessed Appellants' movements, let alone any criminal activity. The government required Sprint to *record* his movements, using Sprint as the custodian. The technology itself needs only ephemeral and anonymous detection of location. Using this artefact of the technology as a retrospective homing beacon does not transform Sprint into a witness. Without the government's action, no person would have ever known or seen the Appellants' every move over the course of seven months.

JAMES WYDA
Federal Public Defender
District of Maryland

/s/

MEGHAN S. SKELTON
Appellate Attorney
6411 Ivy Lane, Suite 710
Greenbelt, Maryland 20770
Telephone: (301) 344-0600
Counsel for Appellant

CERTIFICATE OF SERVICE

This is to certify that on this 8th day of August, 2014, a copy of the foregoing Supplemental Reply Brief of Appellant was filed electronically through CM/ECF, which automatically sends notice of such filing to the following registered CM/ECF users:

Sujit Raman
Benjamin Block, Esq.
Assistant U.S. Attorneys
Office of the U.S. Attorney
36 South Charles St., 4th Floor
Baltimore, Maryland 21201

/s/

Meghan S. Skelton
Appellate Attorney