No. 12-4659 (L)

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,

Appellee,

v.

AARON GRAHAM and ERIC JORDAN,

Appellants.

Appeal from the United States District Court for the
District of Maryland, Northern Division
Honorable Richard D. Bennett, District Judge

SUPPLEMENTAL BRIEF OF APPELLEE UNITED STATES OF AMERICA

Rod J. Rosenstein
United States Attorney

Sujit Raman
Chief of Appeals

Benjamin M. Block
Assistant United States Attorney

Nathan Judish
Attorney, Computer Crime & Intellectual Property Section
U.S. Department of Justice

36 South Charles Street
Baltimore, Maryland 21201
(410) 209-4800

August 1, 2014

Attorneys for the Appellee

TABLE OF AUTHORITIES

Cases

Statutes

RILEY v. CALIFORNIA IS OF NO HELP TO THE DEFENDANTS BECAUSE SPRINT'S RECORDS OF CELL TOWER USAGE ARE NOT CREATED BY THE USER OR STORED ON HIS CELL PHONE

In *Riley v. California*, 134 S. Ct. 2473, 2485 (2014), the Supreme Court held that information contained in a cell phone seized incident to an arrest is protected by the Fourth Amendment, just as the information would be if it were kept in the owner's home. But *Riley* leaves untouched the fundamental principle that there is no reasonable expectation of privacy in a third party's records. Such records, even if they reveal information about people, are not among "*their* persons, houses, papers and effects." U.S. Const. amend. IV (emphasis added). In this case, a cell-phone-service provider, in response to a court order, provided the government with records the provider kept of the cell towers that handled calls placed by cell phones used by the defendants. Obtaining such cell tower information is not a "search" of the defendants because they lack an expectation of privacy in business records created and stored by a third party business.

Even if the defendants had a privacy interest in Sprint's cell tower records, compulsory process of the form at issue here is subject only to a reasonableness standard. The analysis in *Riley* supports the principle that Fourth Amendment protection of information held by a third party depends on how the government obtained the information, not on the nature of the information itself.

A. *Riley* did not expand the scope of what constitutes a search under the Fourth Amendment. There, the parties agreed that the inspections of the phones

"involve[d] *searches* incident to arrest," and the Supreme Court explicitly declined to address "whether the collection or inspection of aggregated digital information amounts to a search under other circumstances." *Riley*, 134 S. Ct. at 2489 n.1. A customer continues to have no reasonable expectation of privacy in a business's records of its transactions with him. *See United States v. Miller*, 425 U.S. 435, 440 (1976) (customers have no privacy interest in bank records, which are "business records" over which customers "can assert neither ownership nor possession").

Riley's discussion of the pen register case, *Smith v. Maryland*, 442 U.S. 735 (1979), confirms that *Riley* did not expand the scope of what constitutes a Fourth Amendment search. The Supreme Court distinguished *Smith*, explaining that *Smith* "concluded that the use of a pen register was not a 'search' at all under the Fourth Amendment." *Riley*, 134 S. Ct. at 2492-93. There is no basis whatsoever for the defendants' claim that *Riley* "limited *Smith* to its facts." Defendants' Supplemental Brief ("Def.S.Br.") at 5. Instead, *Riley* distinguished inspecting an arrestee's cell phone, which is a search, from obtaining information from a third party phone company, which under *Smith* is not.

The defendants erroneously proclaim that the *Riley* Court "adopted the mosaic theory" and "recognized that aggregating data implicates a reasonable expectation of privacy." *Id.* at 3-4. They are wrong: the Court explicitly declined to reach or adopt the mosaic theory. *Riley*, 134 S. Ct. at 2489 n.1. *Riley* recognized that cell phones hold "many distinct types of information . . . that reveal

much more in combination than any isolated record," *id.* at 2489, but it did not hold that aggregating information constitutes a search or that a customer has a reasonable expectation of privacy in information created and maintained by a third party for its own purposes. Investigators routinely gather a variety of types of information that they aggregate to reveal evidence of criminal conduct, but search warrants normally are not required to obtain information from third parties.

It has always been the case that when a customer places or receives a phone call, the phone company needs to know where the phone is located. At the time of *Smith*, when phones were physically and permanently connected by copper wires, the company did not record where the phone was located each time a call was made *because the company always knew that fact.* Wireless technology frees the phone from a single physical location, but the phone company still has the same need to know the identity of the phone (including the phone number) and the location where the phone connects to the company's network (*i.e.*, the cell tower, as opposed to the phone jack). The phone company is thus the courier of the call (just as Federal Express is the courier of a package) and must know where to pick-up and deliver it. *Riley* is fully in harmony with the principle that the Fourth Amendment protects the *content* of a call conveyed through a cell tower, just as it would protect the contents of an envelope placed in a mailbox, but the tower location — the place where the phone meets the provider's network — is not information in which the customer has a privacy interest.

B. Although *Riley* does not control this case, it provides an instructive contrast between the legitimate governmental interests in a search incident to arrest, and in compulsory process such as 2703(d) orders. The search-incident-to-arrest exception serves two interests: protecting officer safety and preserving evidence. *See Riley*, 134 S. Ct. at 2485. The *Riley* Court found that these interests were at most minimally served by searching a cell phone incident to arrest. *See id.*

By contrast, the government's interest in compelling disclosure of non-privileged evidence is "both fundamental and comprehensive," as it is closely linked to the goals of the criminal justice system "that guilt shall not escape or innocence suffer." *United States v. Nixon*, 418 U.S. 683, 709 (1974); *see also In re Subpoena Duces Tecum*, 228 F.3d 341, 346 (4th Cir. 2000) (finding power to obtain testimony and physical evidence intrinsic to the government's investigative power). The ability to obtain relevant evidence from witnesses is critical to the truth-seeking function of the criminal justice process. Thus, "[t]o ensure that justice is done, it is imperative to the function of courts that compulsory process be available for the production of evidence." *Nixon*, 418 U.S. at 709.

The defendants' simplistic proclamation that the government should "[g]et a warrant," Def.S.Br. at 10, ignores the reality that, often, "the very purpose of requesting the information is to ascertain whether probable cause exists." *United States v. R. Enterprises*, 498 U.S. 292, 297 (1991). As a practical matter, investigators need the ability to obtain "building block" evidence that will be used

to establish probable cause for searches, like the search of a cell phone. To this end, investigators need to collect evidence from witnesses. There has never been a warrant requirement to obtain evidence from a witness, and the Supreme Court has long held that compulsory process is subject only to a reasonableness requirement. *See, e.g.*, *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186, 208 (1946).[1]

A phone company's records of the cell towers it uses to handle customer communications — records that are made and kept at the company's discretion, and are subject to its control, not its customers' — sometimes make the company a witness to criminal activity. Investigators frequently use 2703(d) orders at the early stages of important criminal investigations, when they lack probable cause to obtain a warrant. In such circumstances, cell tower records may deflect suspicion from the innocent, build probable cause against the guilty, and conserve scarce investigative resources. Imposing a warrant requirement on a provider's cell-site records would substantially hinder the government's ability to investigate and solve crimes. This Court should maintain the distinction between *Riley*, on the one hand, and *Smith* and *Miller*, on the other: while accessing data contained on a cell phone is a search, obtaining business records from a phone company is not.

C. This case is not about information maintained *on* a cell phone, and there is a quantitative and qualitative distinction between the privacy interest in

[1] The reasonableness standard was met here because a court found Sprint's records to be relevant and material to a criminal investigation. *See* JA 250-51, 259-60.

information stored on a cell phone and the cell tower information available via 2703(d) order. *Riley* noted the scope and breadth of the many functions served by cell phones, including as cameras, calendars, libraries, diaries, and repositories of web browsing and detailed location history. *Riley*, 134 S. Ct. at 2485, 2489.

The privacy interests in a phone company's business records obtained via 2703(d) order are minimal in comparison. These records include the time, date, phone numbers, and cell tower information associated with communications — data that is nothing like the comprehensive set of personal information found on a cell phone. Indeed, the defendants claim no privacy interest in any of this information other than the cell tower information; but that information merely placed their phones into a circle with a radius of at least two miles. JA 1966. Moreover, customers realize that they need to connect to a cell tower to place a call, but they often do not know the precise cell tower locations.

Contrary to the defendants' claim, *see* Def.S.Br. at 3, *Riley* said nothing about cell tower records. Cell tower locations are fixed and usually of no concern to the customer. *Riley* addressed location information only because many phones constantly compute their own precise latitude and longitude — data that often *is* valuable to the individual user. *Riley*, 134 S. Ct. at 2489 ("Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute…."). But smartphone location information generally remains *on the phone* unless the user chooses to share it with

a third party.[2] For a user to place or receive a call, by contrast, his phone must transmit information out to a tower, so the provider will know where to convey the contents of the call. The defendants err in conflating these very different types of location information.[3]

Unlike the broad range of information stored *on* a personal phone, cell tower records created and maintained by Sprint can be used only to determine the general area where the phone was located when it was in use. *See* JA 2668-3224. Furthermore, the Fourth Amendment does not limit the government's power to obtain business records of third parties that reveal sensitive information about customers. Financial records can disclose many sensitive aspects of a person's life,[4] but obtaining them from a third party is not a search under the Fourth Amendment. *United States v. Miller*, 425 U.S. 435 (1976).

Finally, although *Riley* stated that "[c]ell phone users often may not know whether particular information is stored on the device or in the cloud, and it

---

[2] For example, the iPhone "Frequent Locations" folder "will keep track of places you have recently been, as well as how often and when you visited them . . . . This data is kept solely on your device and won't be sent to Apple without your consent." *See* <support.apple.com/kb/HT5594> (last visited August 1, 2014).

[3] By analogy, a suspect may write an intimate confession in a private diary and tell similar information to a third party who creates a verbatim record. Although the recorded facts are substantially the same, differences in how and why the record was created and maintained are dispositive.

[4] Similarly, amazon.com likely knows more intimate details about many individuals' lives — what movies they watch, what books they read, what music they listen to, what gifts they send, and to whom — than their phone provider; but those details indisputably may be obtained with grand jury subpoenas.

generally makes little difference," *Riley*, 134 S. Ct. at 2491, the defendants err in asserting that this language implies that users have a privacy interest in cell tower records. Cell phone users have no control over the phone company's cell tower records. At most, *Riley* suggests that a user may have a privacy interest in his *own* information, such as the contents of his e-mail account, regardless of whether it is stored on his phone or in the cloud. *Riley* does not create a privacy interest in a *business's* records concerning its customers.

D. In a concurring opinion in *Riley*, Justice Alito emphasized the wisdom of allowing the legislative branch to balance privacy interests with the needs of law enforcement. *Riley*, 134 S. Ct. at 2497-98 (Alito, J., concurring). Similarly, in *United States v. Jones*, 132 S. Ct. 945 (2012), four Justices agreed that "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative…. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." *Id.* at 964 (Alito, J., concurring).

Congress *has* legislated for cell tower records, setting the "specific and articulable facts" standard of 18 U.S.C. § 2703(d). Moreover, Congress was specifically concerned with location information when it enacted the Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) ("CALEA"). CALEA enhanced privacy protections for location information. First, providers are limited from disclosing location information

"solely pursuant" to a pen/trap order. *See* CALEA § 103; 47 U.S.C. § 1002(a). Second, CALEA raised the standard for obtaining 2703(d) orders, like the ones in this case, from a "relevance" standard to the "specific and articulable facts" standard now in effect. *See* CALEA § 207; 18 U.S.C. § 2703(d). Especially in light of the "strong presumption of constitutionality" accorded to federal statutes challenged on Fourth Amendment grounds, *United States v. Watson*, 423 U.S. 411, 416 (1976), it is appropriate to respect the standard established by the Congress.

E. Disregarding this Court's direction to file supplemental briefs addressing *Riley*, the defendants devote much of their brief to other recent cases. If the Court seeks additional briefing about those cases, the government will gladly provide it. Otherwise, however, the government will not address those cases, except to make two brief points. First, *United States v. Davis*, __ F.3d __, 2014 WL 2599917 (11th Cir. 2014), *petition for rehrg. en banc filed* Aug. 1, 2014, is poorly reasoned in comparison with *In re Application*, 724 F.3d 600 (5th Cir. 2013). The Fifth Circuit included a careful analysis of the third party doctrine. *See id.* at 608-15. The *Davis* panel ignored that reasoning, *see Davis*, 2014 WL 2599917, at *4, and its dismissal of *Smith v. Maryland* is superficial, at best. *See id.* at *9.

Second, the defendants mistakenly cite two State cases that they claim hold that "warrantless searches of CSLI violate the Constitution." Def.S.Br. at 9. Both cases hold that a warrant is required to obtain cell-site records *solely under their*

respective State constitutions. *State v. Earls*, 214 N.J. 564, 589 (N.J. 2013); *Commonwealth v. Augustine*, 467 Mass. 230, 243-44 (Mass. 2014).

F. Finally, the defendants argue that *Riley* stands for the proposition that the Fourth Amendment prohibits the government from obtaining information that would either "cross the threshold of constitutionally protected space" or "recreate an intimate picture of an individual's life." Def.S.Br. 4. That amorphous rhetoric is not a viable legal standard. Just like one's relatives, friends, and enemies, businesses obtain information about people — often more sensitive than which cell tower is used to make a call — and may disclose it to criminal investigators. The Fourth Amendment does not protect facts qua facts. When information is kept in a place that the individual controls, it is protected even if it is a matter of purely public concern. But when information is created and maintained by a third party and kept in a place the customer does not control, it is not protected, irrespective of what sensitive facts it may reveal. The substance and sensitivity of information known by third parties is not the touchstone of Fourth Amendment protection.

In order to stay "on the right side of history,"[5] *id.* at 10, this Court should follow existing federal law and respect the long-established constitutional principle that there is no individual expectation of privacy in internal business records created and maintained by phone companies.

[5] The government's authority to compel disclosure of evidence has deep roots. This authority was accepted as early as 1562, and was an "indubitable certainty" by 1742. *Kastigar v. United States*, 406 U.S. 441, 443 (1972).

Respectfully submitted,

Rod J. Rosenstein
United States Attorney

By: /s/
Sujit Raman
Chief of Appeals

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on August 1, 2014, I electronically filed the foregoing with the Clerk of Court using the ECF System, which will send notice of such filing to the following registered ECF users:

Meghan S. Skelton, Esq.
Office of the Federal Public Defender
6411 Ivy Lane, Suite 710
Greenbelt, Maryland 20770
Counsel for Aaron Graham

Ruth J. Vernet, Esq.
31 Wood Lane
Rockville, Maryland 20850
Counsel for Eric Jordan

Nathan Freed Wessler, Esq.
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, New York 10004
Counsel for Amici Curiae

/s/
Sujit Raman
Chief of Appeals