United States Court of Appeals,
Fifth Circuit.
In re Application of the UNITED STATES of America FOR HISTORICAL CELL SITE DATA.
United States of America, Appellant.

724 F.3d 600
July 30, 2013.

Before REAVLEY, DENNIS, and CLEMENT, Circuit Judges.

EDITH BROWN CLEMENT, Circuit Judge:

We are called on to decide whether court orders authorized by the Stored Communications Act to compel cell phone service providers to produce the historical cell site information of their subscribers are per se unconstitutional. We hold that they are not.

I. FACTUAL AND PROCEDURAL BACKGROUND

In early October 2010, the United States filed three applications under § 2703(d) of the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701–2712, seeking evidence relevant to three separate criminal investigations. Each application requested a court order to compel the cell phone service provider for a particular cell phone to produce sixty days of historical cell site data and other subscriber information for that phone. The Government requested the same cell site data in each application: "the antenna tower and sector to which the cell phone sends its signal." It requested this information for both the times when the phone sent a signal to a tower to obtain service for a call and the period when the phone was in an idle state.

For each application, the magistrate judge granted the request for subscriber information but denied the request for the historical cell site data, despite finding that the Government's showing met the "specific and articulable facts" standard set by the SCA for granting an order to compel the cell site data. Shortly thereafter, the magistrate judge invited the Government to submit a brief justifying the cell site data applications. Four days after the Government submitted its brief, the magistrate judge issued a written opinion taking judicial notice of a host of facts about cell phone technology, primarily derived from the testimony of a computer science professor at a congressional hearing, but also including information from published studies and reports and service provider privacy policies. He concluded his opinion by declaring that, based on these facts viewed in light of Supreme Court precedent, "[c]ompelled warrantless disclosure of cell site data violates the

Fourth Amendment." *Id.* at 846.

The Government filed objections with the district court to the magistrate judge's ruling on the constitutionality of the SCA and his judicial notice of facts. Although there was no party adverse to the Government's ex parte application, the ACLU and Electronic Frontier Foundation ("EFF"), among others, participated as amici curiae. As part of its submissions, the Government provided the court with additional evidence in the form of an affidavit from one of the service providers detailing its cell site records. After the parties submitted their briefs, the district judge issued a single-page order. He concluded:

> When the government requests records from cellular services, data disclosing the location of the telephone at the time ***603** of particular calls may be acquired only by a warrant issued on probable cause. The records would show the date, time called, number, and location of the telephone when the call was made. These data are constitutionally protected from this intrusion. The standard under the Stored Communications Act is below that required by the Constitution.

III. DISCUSSION

B. Fourth Amendment challenge

The district court held that the SCA violates the Fourth Amendment because the Act allows the United States to obtain a court order compelling a cell phone company to disclose historical cell site records ***606** merely based on a showing of "specific and articulable facts," rather than probable cause. We review this ruling, applying *Katz v. United States* and its progeny to determine whether the Government's acquisition of these electronic records constitutes a search or a seizure subject to the Fourth Amendment's probable cause. 389 U.S. 347, 353, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967).

The Government recognizes that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz*, 389 U.S. at 351, 88 S.Ct. 507; *see also id.* at 350–51, 88 S.Ct. 507 ("[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.' That Amendment protects individual privacy against certain kinds of *governmental intrusion*.... But the protection of a person's general right to privacy—his right to be let alone by *other people*—is, like the protection of his property and of his very life, left largely to the law of the individual States." (emphasis added)).

***610** Therefore, the Government, when determining whether an intrusion constitutes a search or seizure, draws a line based on whether it is the Government collecting the information or requiring a third party to collect and store it, or whether it is a third party, of its own accord and for its own purposes, recording the information. Where a third party collects information in the first instance for its own purposes, the Government claims that it can obtain this information later with a § 2703(d) order, just as it can subpoena other records of a private entity. *Compare Smith*, 442

U.S. at 743, 99 S.Ct. 2577 (finding significant that "the phone company does in fact record this information *for a variety of legitimate business purposes* " (emphasis added)), *with* *Jones*, 132 S.Ct. at 964 (Alito, J., concurring in the judgment) (expressing concern over the application of existing Fourth Amendment doctrine to "the use of GPS tracking technology *for law enforcement purposes* " (emphasis added)). We agree.

[11] This question of *who* is recording an individual's information initially is key because:

> [T]he individual must occasionally transact business with other people. When he does so, he leaves behind, as evidence of his activity, the records and recollections of others. He cannot expect that these activities are his private affair. To the extent an individual knowingly exposes his activities to third parties, he surrenders Fourth Amendment protections, and, if the Government is subsequently called upon to investigate his activities for possible violations of the law, it is free to seek out these third parties, to inspect their records, and to probe their recollections for evidence.

Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1043 (D.C.Cir.1978). Moreover, "[t]he fortuity of whether or not the [third party] in fact elects to make a quasi-permanent record" of information conveyed to it "does not ... make any constitutional difference." *Smith*, 442 U.S. at 745, 99 S.Ct. 2577. The third party can store data disclosed to it at its discretion. And once an individual exposes his information to a third party, it can be used for any purpose, as "[i]t is established that, when a person communicates information to a third party *even on the understanding that the communication is confidential*, he cannot object if the third party conveys that information or records thereof to law enforcement authorities." *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743, 104 S.Ct. 2720, 81 L.Ed.2d 615 (1984) (emphasis added).[FN11]

> FN11. Although the ACLU contends that this sort of compulsory process requires notice and an opportunity to litigate the order's validity before it is executed, the Government notes that it is the party who owns the records, not the party whose information is recorded, that has this right to challenge the order. *See* *Jerry T. O'Brien*, 467 U.S. at 743, 104 S.Ct. 2720 (concluding that Supreme Court precedents "disable respondents from arguing that notice of subpoenas issued to third parties is necessary to allow a target to prevent an unconstitutional search or seizure of his papers"). The SCA provides that "[a] governmental entity receiving records or information [of non-content data] is not required to provide notice to a subscriber or customer" before or after government officials obtain this infor-

mation. § 2703(c)(3). Insofar as the ACLU believes that the SCA is constitutionally problematic because it does not require these officials to ever disclose to the subscriber that they sought and obtained his non-content records—whether or not information gleaned from the records led to a criminal prosecution, *cf. Jones*, 132 S.Ct. at 964 (showing special concern for situations where government officials "*secretly* monitor" individuals (emphasis added))—we note that nothing in the non-content records provisions of the SCA prevents cell service providers from informing their subscribers of such government requests.

***611** The Government does concede that the subpoenaed third party must have possession of—the right to control—the records before officials can require it to turn them over. The Government, therefore, distinguishes cases where a landlord or hotel manager merely has the right to enter the apartment or room of another. The Government acknowledges that "the government may not subpoena the landlord to produce the tenant's personal papers from her apartment." However, it contrasts these situations from the one presented in *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). In *Miller*, the Court rejected a bank depositor's Fourth Amendment challenge to a subpoena of bank records because, as the bank was a party to the transactions, the records belonged to the bank. *Id.* at 440–41, 96 S.Ct. 1619 ("[T]he documents subpoenaed here are not respondent's private papers.... [R]espondent can assert neither ownership nor possession. Instead, these are the business records of the bank[ ].... [They] pertain to transactions to which the bank was itself a party." (citation and internal quotation marks omitted)).

This qualification that the right to possession hinges on whether the third party created the record to memorialize its business transaction with the target, rather than simply recording its observation of a transaction between two independent parties, recently gained context and support from a case decided by the Sixth Circuit. In that case, *United States v. Warshak*, the court of appeals held that the "government may not compel a commercial [internet service provider] to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause." 631 F.3d 266, 288 (6th Cir.2010). The court reasoned that the emails were communications between two subscribers, not communications between the service provider and a subscriber that would qualify as business records. The provider was merely the "intermediary." *Id.* at 286.

Defining business records as records of transactions to which the record-keeper is a party also fits well with the historical and statutory distinction between communications content and addressing information. *See United States v. Forrester*, 512 F.3d 500, 511 (9th Cir.2008) ("In a line of cases dating back to the nineteenth century, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties.") (collecting cases); *see, e.g.*, 18 U.S.C. § 2703(b)-(c). Communications content, such

as the contents of letters, phone calls, and emails, which are not directed to a business, but simply sent via that business, are generally protected. However, addressing information, which the business needs to route those communications appropriately and efficiently are not. *See* *Smith*, 442 U.S. at 741, 99 S.Ct. 2577 (finding significant that pen registers, unlike the listening device employed in *Katz*, "do not acquire the *contents* of communications" and do not require a warrant); *Forrester*, 512 F.3d at 511 ("The government's surveillance of e-mail addresses also may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail.... E-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient.").

Under this framework, cell site information is clearly a business record. The cell service provider collects and stores historical cell site data for its own business purposes, perhaps to monitor or optimize service***612** on its network or to accurately bill its customers for the segments of its network that they use. The Government does not require service providers to record this information or store it. The providers control what they record and how long these records are retained. The Government has neither "required [n]or persuaded" providers to keep historical cell site records. *Jones*, 132 S.Ct. at 961 (Alito, J., concurring in the judgment). In the case of such historical cell site information, the Government merely comes in after the fact and asks a provider to turn over records the provider has already created.

Moreover, these are the providers' own records of transactions to which it is a party. The caller is not conveying location information to anyone other than his service provider. He is sending information so that the provider can perform the service for which he pays it: to connect his call. And the historical cell site information reveals his location information for addressing purposes, not the contents of his calls.[FN12] The provider uses this data to properly route his call, while the person he is calling does not receive this information.

> FN12. The Ninth Circuit has similarly concluded that "e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers." *Forrester*, 512 F.3d at 510. It noted that:
>
> > Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a pre-recorded information or subject-specific line, such as sports scores, lottery results or phone sex

> lines, the phone number may even show that the caller had access to specific content information. Nonetheless, the Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here.

Id. These observations are equally applicable to historical cell site data.

The ACLU points out that this conveyance of location information to the service provider nevertheless must be voluntary in order for the cell phone owner to relinquish his privacy interest in the data. The ACLU asserts that here it is not. According to the ACLU, "[w]hen a cell phone user makes or receives a call, there is no indication to the user that making or receiving that call will ... locate the caller." A user cannot voluntarily convey something which he does not know he has.

The Government disputes the assertion that cell phone users do not voluntarily convey location information. It contends that the users know that they convey information about their location to their service providers when they make a call and that they voluntarily continue to make such calls. We agree.

In *Smith,* the Supreme Court recognized that:

> All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.

442 U.S. at 742, 99 S.Ct. 2577. Furthermore, it observed that "[m]ost phone books tell subscribers, on a page entitled 'Consumer Information,' that the company 'can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls.' " *Id.* at 742–43, 99 S.Ct. 2577.

***613** A cell service subscriber, like a telephone user, understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call. *See United States v. Madison,* No. 11–60285–CR, 2012 WL 3095357, at *8 (S.D.Fla. July 30, 2012) (unpublished) ("[C]ell-phone users have knowledge that when they place or receive calls, they, through their cell phones, are transmitting signals to the nearest cell tower, and, thus, to their communications service providers."). Cell phone users recognize that, if their phone cannot pick up a signal (or "has no bars"), they are out of the range of their service provider's network of towers. And they realize that, if

many customers in an area attempt to make calls at the same time, they may overload the network's local towers, and the calls may not go through. Even if this cell phone-to-tower signal transmission was not "common knowledge," *California v. Greenwood*, 486 U.S. 35, 40, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988), the Government also has presented evidence that cell service providers' and subscribers' contractual terms of service and providers' privacy policies expressly state that a provider uses a subscriber's location information to route his cell phone calls. In addition, these documents inform subscribers that the providers not only use the information, but collect it. *See also Madison*, 2012 WL 3095357, at *8 ("Moreover, the cell-phone-using public knows that communications companies make and maintain permanent records regarding cell-phone usage, as many different types of billing plans are available.... Some plans also impose additional charges when a cell phone is used outside its 'home area' (known commonly as 'roaming' charges). In order to bill in these different ways, communications companies must maintain the requisite data, including cell-tower information."). Finally, they make clear that providers will turn over these records to government officials if served with a court order. Cell phone users, therefore, understand that their service providers record their location information when they use their phones at least to the same extent that the landline users in *Smith* understood that the phone company recorded the numbers they dialed.

Their use of their phones, moreover, is entirely voluntary. *See United States v. Skinner*, 690 F.3d 772, 777 (6th Cir.2012) ("There is no Fourth Amendment violation because Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone."). The Government does not require a member of the public to own or carry a phone. As the days of monopoly phone companies are past, the Government does not require him to obtain his cell phone service from a particular service provider that keeps historical cell site records for its subscribers, either. And it does not require him to make a call, let alone to make a call at a specific location.

Nevertheless, the ACLU argues that, while an individual's use of his phone may be voluntary, he does not voluntarily convey his cell site information because he does not *directly* convey it to his service provider. The only information he directly conveys is the number he dials. *See In re Application of the United States*, 620 F.3d at 317 ("[W]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed."). This crabbed understanding of voluntary conveyance would lead to absurd results. For example, if a user programmed a contact's telephone number into his phone's speed dial memory, he would only need to dial the speed dial reference number to make the call. Would that mean that the Government would be unable to obtain the contact's actual telephone number from his service provider? Clearly not. The contact's***614** telephone number is necessary for the service provider to connect the call; the user is aware of this fact; therefore, he is aware that he is conveying that

information to the service provider and voluntarily does so when he makes the call. A similar analysis for cell site information leads to the conclusion that a user voluntarily conveys such information when he places a call, even though he does not directly inform his service provider of the location of the nearest cell phone tower. Because a cell phone user makes a choice to get a phone, to select a particular service provider, and to make a call, and because he knows that the call conveys cell site information, the provider retains this information, and the provider will turn it over to the police if they have a court order, he voluntarily conveys his cell site data each time he makes a call.

Finally, the ACLU argues that advances in technology have changed society's reasonable expectations of privacy in information exposed to third parties. *See Jones*, 132 S.Ct. at 963–64 (Alito, J., concurring in the judgment) ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical.... Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap."); *see also id.* at 957 (Sotomayor, J., concurring). We agree that technological changes can alter societal expectations of privacy. *See id.* at 962 (Alito, J., concurring) ("Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."). At the same time, "[l]aw enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system." *Skinner*, 690 F.3d at 778 (citing *United States v. Knotts*, 460 U.S. 276, 284, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983)). Therefore, "[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." *Jones*, 132 S.Ct. at 964 (Alito, J., concurring in the judgment).

Congress has crafted such a legislative solution in the SCA. The statute conforms to existing Supreme Court Fourth Amendment precedent. This precedent, as it now ***615** stands, does not recognize a situation where a conventional order for a third party's voluntarily created business records transforms into a Fourth Amendment search or seizure when the records cover more than some specified time period or shed light on a target's activities in an area traditionally protected from governmental intrusion. We decline to create a new rule to hold that Congress's balancing of privacy and safety is unconstitutional.

[12] We understand that cell phone users may reasonably want their location information to remain private, just as they may want their trash, placed curbside in opaque bags, *Greenwood*, 486 U.S. at 40–41, 108 S.Ct. 1625, or the view of their property from 400 feet above the ground,

Florida v. Riley, 488 U.S. 445, 451, 109 S.Ct. 693, 102 L.Ed.2d 835 (1989), to remain so. But the recourse for these desires is in the market or the political process: in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections. The Fourth Amendment, safeguarded by the courts, protects only reasonable *expectations* of privacy.

Recognizing that technology is changing rapidly, we decide only the narrow issue before us. Section 2703(d) orders to obtain *historical* cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional. We do not address orders requesting data from all phones that use a tower during a particular interval, orders requesting cell site information for the recipient of a call from the cell phone specified in the order, or orders requesting location information for the duration of the calls or when the phone is idle (assuming the data are available for these periods). Nor do we address situations where the Government surreptitiously installs spyware on a target's phone or otherwise hijacks the phone's GPS, with or without the service provider's help.