United States v. Graham

US Federal Appeals Court for the 4th Circuit, No. 12-4659, 31 May 2016

The Court's ruling is the latest in a line of appeals decisions to confirm that the US Government can obtain cell-site location data as long as a court order is issued pursuant to the US Stored Communications Act.

A 31 May 2016 US federal appeals court decision holding that the police did not need to obtain a warrant to receive cell-site location data for two bank robbery suspects[1] generated many privacy-related headlines. Looking behind those headlines, however, demonstrates that the Court simply followed other federal appeals court rulings in their interpretation of US law. All of these appeals courts ruled that the US Government can obtain cell-site location data as long as a court order is issued pursuant to the federal law known as the Stored Communications Act.

The facts

This case began in early 2011, with a series of six armed robberies of businesses located in and around Baltimore, Maryland. The jury found that each of the robberies involved Aaron Graham acting alone or in concert with others. The robberies began on 17 January 2011 and ended with the fifth and sixth robberies on 5 February 2011.

The fifth and sixth robberies occurred on 5 February, when Mr Graham, wearing the same jacket worn during the January robberies, entered a fast-food restaurant, and used a gun to threaten the restaurant manager into opening several cash registers, which Mr Graham robbed. The manager saw Mr Graham enter a dark Ford F-150 truck. Approximately 45 minutes later, Mr Graham entered a different fast-food restaurant, brandished the gun and demanded the restaurant manager open several cash registers, which Mr Graham robbed. The manager saw Mr Graham enter a dark F-150 truck.

A Baltimore police officer was investigating the first fast-food restaurant robbery when he heard a radio call about the second fast-food restaurant robbery, and that the F-150 was possibly heading his way. The officer saw the truck and a passenger wearing a jacket matching the description given by the restaurant manager. The officer pursued the truck, and the chase ended in an almost Hollywood-like fashion: the truck became trapped between heavy traffic, a construction barrier, and a moving train. The police officer and his partner arrested Mr Graham and the truck driver, locating a gun from under the passenger seat of the truck and $1,100 in cash.

Subsequent police investigation

A Baltimore detective recognised the similarities between the fast-food robberies and some of the January robberies. He sought and obtained from a judge a search warrant for Mr Graham's residence, for the truck driver's residence, and for the truck. The search of the pickup truck resulted in the discovery of two cell phones. The detective sought and obtained from a judge a search warrant for each of the phones.

The US Government then sought and obtained a court order for the cell-site location information from Sprint/Nextel for the two cell phones. The timeframe sought and that the court granted was 1 July 2010 through 6 February 2011 - a total of 221 days, and 29,659 location data points for defendant Graham (and 28,410 location data points for the truck driver). Note that the court order pertained only to the location data, and did not include any content of any calls or text messages.

The US Government sought that court order pursuant to a federal law known as the Stored Communications Act, which permits the Government to obtain records from third party service providers (like Sprint/Nextel) upon a showing of 'specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought [...] are relevant and material to an ongoing criminal investigation[2].' A federal appeals Court characterised this standard as "essentially a reasonable suspicion standard[3]." In contrast, the standard to obtain a warrant under the Fourth Amendment to the US Constitution is probable cause - a substantially higher standard[4].

Trial

The defendants made a pre-trial motion to exclude the cell-site location information, on the grounds that the information was obtained in violation of the Fourth Amendment. (In other words, the defendants argued that the Stored Communications Act standard violated the Fourth Amendment.) The Court denied the motion. At trial, the Government introduced the cell-site location information only to establish the two defendants' locations at various times before and after most of the robberies. The jury convicted both defendants on all counts.

The defendants appealed.

2015 Appellate Court ruling

A three-judge panel of the Fourth Circuit Court of Appeals heard the appeal and, on 5 August 2015, issued a split opinion. In its 2-1 ruling, the Court held that the Government's procurement of the cell-site data location information was an unreasonable search in violation of the Fourth Amendment. Nevertheless, the Court ruled that the data did not need to be suppressed because the Government had acted in good-faith reliance on the Stored Communications Act and the court orders issued pursuant to that federal law.

The majority held that the

Government "conducts a search under the Fourth Amendment when it obtains and inspects a cell phone user's historical CSLI [cell-site location information] for an extended period of time." That information can be used to "discover the private activities and personal habits of the user. Cell phone users have an objectively reasonable expectation of privacy in this information." Therefore, the majority reasoned, a search warrant would be required unless an exception applied.

The Government argued - and the dissenting judge agreed - that the 'third party doctrine' exception applied: "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," as the US Supreme Court stated in 1979[5]. That 1979 case involved a 'pen register' that a telephone company installed upon the request of the police to record the telephone numbers dialled from the home phone of a robbery suspect. The Supreme Court held that the defendant voluntarily conveyed those phone numbers to the phone company and had no legitimate expectation of privacy (a) in the dialled phone numbers or (b) that the phone company would not convey that information to a third party. Note that the defendant did not have ownership of those records: the telephone company did.

In the 2015 opinion, the appellate court majority held that this exception did not apply: "We cannot accept the proposition that cell phone users volunteer to convey their location information simply by choosing to activate and use their cell phones and to carry the devices on their person."

The dissent found that, like two other federal appeals courts that had examined the issue, "individuals do not have a reasonable expectation of privacy in historical CSLI records that the government obtains from cell phone service providers through a § 2703(d) order[6]."

The US Government appealed to the full Fourth Circuit (15 judges).

2016 *en banc* Appeals Court opinion

By a 12-3 vote, the full ('*en banc*') Fourth Circuit reversed the 2015 opinion, holding that "the Government's acquisition of historical CSLI from Defendants' cell phone provider did not violate the Fourth Amendment." Citing the US Supreme Court's 1979 opinion described above, the Court held that "Defendants did not have a reasonable expectation of privacy in the historical CSLI" because they "unquestionably 'exposed' the information at issue to the phone company's 'equipment in the ordinary course of business.'" The majority also pointed out that this ruling agreed with the three other federal appeals courts that had reached the issue, and that "the vast majority of federal district court judges have reached the same conclusion."

The majority specifically found that users voluntarily conveyed location information to the service provider in order for cell services to work: "Anyone who has stepped outside to 'get a signal' or has warned a caller of a potential loss of service before entering an elevator, understands, on some level, that location matters." The majority also dismissed the dissent's point that the third party doctrine required specific knowledge on the part of the user in what information was being conveyed. The majority found that specific knowledge is not required, but even if it were "we fail to see how a phone user could have a reasonable expectation of privacy in something he does not know."

Impact

Because all four federal appeals courts that have reviewed the issue agree that the US Government can obtain cell-site location data as long as a court order is issued pursuant to the Stored Communications Act, it seems unlikely that the US Supreme Court would accept an appeal on this issue.

Sue Ross Senior Counsel
Norton Rose Fulbright US LLP, New York
susan.ross@nortonrosefulbright.com

1. United States v. Graham, No. 12-4659 (4th Cir. 31 May 2016) (en banc).
2. 18 U.S.C. § 2703(d).
3. In *re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 708 F.3d 283, 287 (4th Cir. 2013).
4. *United States v. Graham*, Nos. 12-4659, 12-4825 (4th Cir. 2015). The Fourth Amendment to the US Constitution reads in full: 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.'
5. *Smith v. Maryland*, 442 U.S. 735 743-44 (1979).
6. The dissent cited *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (*en banc*) and In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013). The dissent also cited a third federal appeals court opinion, which found that users did not 'voluntarily' share location information with a cell provider, but the government can legally obtain the location information pursuant to a § 2703(d) order. In *re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010).