SMU | Dedman School of Law

SMU Law Review

Volume 71 | Issue 2 Article 6

January 2018

"You're Not Gonna Reach My Telephone"— The Resurgence of the Fourth Amendment's Particularity Requirement

Tammie Beassie Banko
Southern Methodist University

"You're Not Gonna Reach My Telephone"—The Resurgence of the Fourth Amendment's Particularity Requirement

*Tammie Beassie Banko**

TO determine whether a state action violates the Fourth Amendment, the Supreme Court employs a balancing test, weighing on the one hand "the degree to which [the action] intrudes upon an individual's privacy and . . . the degree to which it is needed for the promotion of legitimate governmental interests" on the other hand.[1] However, in an era in which a catalogue of a person's GPS locations, text messages, emails, Google searches, banking information, personal notes, and grocery lists—potentially anything police would need to corroborate a crime—can be seized in one small cellular device, the scales seem to instantly dive, not merely tip, in favor of governmental interests. This is, in part, because officers seeking a warrant to search for and seize cellphones have had an easy case to make before a magistrate: (1) I have probable cause to believe X committed a crime; (2) almost every person owns a cellphone; (3) most criminals use cellphones to communicate and conspire; (4) X is a person and therefore probably owns a cellphone; and (5) evidence of his involvement in this alleged crime is likely within his phone inside his home. On this seemingly logical basis, a "valid" warrant to seize *any* cellphone would issue for *any* person suspected of committing *any* crime—a notion that the Fourth Amendment should not tolerate. The D.C. Circuit agrees.

In *United States v. Griffith*, the D.C. Circuit rightly held that the mere ubiquity of cellphones, coupled with officers' subjective knowledge of their potential use in criminal transactions, is insufficiently particular under the Fourth Amendment for a warrant to issue.[2] Further, the court's

* J.D. Candidate, SMU Dedman School of Law, May 2019; B.A. University of Texas, May 2011. Thank you to my husband and thought-partner, Ryan Banko, for his comments and support, and to my mother and father, Rhonda and Les Beassie, for teaching me to love the law.

1. Riley v. California, 134 S. Ct. 2473, 2484 (2014) ("[W]e generally determine whether to exempt a given type of search from the warrant requirement 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'").

2. United States v. Griffith, 867 F.3d 1265, 1270–71 (D.C. Cir. 2017).

break with other circuits and academics' recommendations in decidedly invalidating overseizure of electronic devices represents a strong victory for personal privacy and restores force to the particularity requirement in the digital age. Finally, the court's refusal to apply the good-faith exception to the exclusionary rule to save a facially deficient warrant adds teeth to its ruling, reminding officers that failure to meet the particularity requirement may not cure the invalid warrant or save the fruits of the search.

In January 2013, police were investigating a gang-related homicide.[3] Video footage displayed the getaway car circling the crime scene.[4] Officers suspected Ezra Griffith, a known gang member, to be the driver.[5] More than a year after the murder, officers sought a warrant to search the apartment Griffith shared with his girlfriend in hopes of obtaining a cell phone that would connect him to the murder.[6] The application requested authority to seize "all electronic devices to include, but not limited to cellular telephone(s), computer(s), electronic tablet(s), devices capable of storing digital images (to include, but not limited to, PDAs, CDs, DVD's [and] jump/zip drives)" as well as "evidence of ownership of such devices."[7]

The portion of the affidavit supporting search and seizure of a cell phone was solely supported by the officer's personal experience and conjecture. The officer asserted that "gang/crew members involved in criminal activity maintain regular contact with each other, even when they are arrested or incarcerated, and that they often stay advised and share intelligence about their activities through cell phones and other electronic communication devices and the Internet to include Facebook, Twitter and E-mail accounts."[8] The affidavit concluded that "aforementioned facts and circumstances," coupled with the officer's "experience and training," were sufficient to establish "probable cause to believe that secreted inside of [the apartment] is evidence relating to the homicide discussed above."[9] The magistrate agreed.[10]

On January 7, 2013, the officers executed the warrant.[11] Officers observed a gun flying out of the window near where Griffith was standing.[12] They seized the gun, entered the apartment, and seized "a number of cell phones."[13] Griffith was charged with possession of a firearm by a convicted felon.[14] He moved to suppress all evidence and challenged the war-

3. *Id.* at 1268.
4. *Id.*
5. *Id.* at 1269.
6. *Id.*
7. *Id.*
8. *Id.*
9. *Id.*
10. *Id.*
11. *Id.* at 1270.
12. *Id.*
13. *Id.*
14. *Id.*

rant as facially invalid because there was no evidence that he owned a cell phone or that any of the items would be within the apartment prior to executing the warrant.[15] Countering these arguments, the government argued that the ubiquity of cell phones was sufficient to establish probable cause that Griffith owned a cell phone, that the cell phone would contain evidence, and that the device would be within the home.[16] The government alternatively requested the application of the good-faith exception.[17] The trial court denied the motion to suppress, applied the good-faith exception, and failed to decide whether the warrant was facially invalid.[18] Griffith was convicted of felonious possession of a firearm.[19]

On appeal, the D.C. Circuit reversed the denial of Griffith's motion to suppress and vacated his conviction.[20] Challenging other circuit rulings and many courts' interpretations of *Riley v. California*,[21] the D.C. Circuit held that "the general pervasiveness of cell phones affords an inadequate basis" for establishing probable cause to search a home and seize electronics within unless there is evidence given to believe the specific person in question (1) owns a phone and (2) has the phone within the home to be searched in compliance with the Fourth Amendment's particularity requirement.[22] Finding otherwise would "verge on authorizing a search of a person's home almost anytime there is probable cause to suspect her of a crime."[23] Further, the court chastised the overbreadth of the warrant because it allowed officers to seize *all* electronic devices, which are "otherwise lawful objects," even if they affirmatively knew that the devices belonged to Griffith's girlfriend or the child within, both of whom were of no legal interest to the government.[24] The court refused to apply the good-faith exception as a result.[25]

The court's ruling was a surprising and warranted blow to many courts' erroneous tendency to allow officers' subjective knowledge and experience to substitute for the Fourth Amendment's particularity requirement when issuing warrants. Many lower courts across circuits uphold warrants to seize cell phones based solely on officer "knowledge and experience" that the alleged crimes under investigation involved digital communications without any specific knowledge that the particular suspect had a cell phone. For example, in *United States v. Reed*, the court upheld a seizure of a cell phone pursuant to a search warrant based solely on the "general knowledge [the officer] has acquired about controlled substance traffick-

15. *Id.*
16. *See id.* at 1272.
17. *Id.* at 1270.
18. *Id.*
19. *Id.*
20. *Id.* at 1281.
21. Riley v. California, 134 S. Ct. 2473, 2484–85 (2014) (holding that cell phones maintain such a heightened expectation of privacy that officers must obtain an additional warrant to search the contents of a phone after seizure).
22. *Griffith*, 867 F.3d at 1275–76.
23. *Id.* at 1275.
24. *Id.*
25. *Id.* at 1279.

ers through his training, experience, and participation in investigations."[26] Because traffickers "commonly maintain addresses or telephone numbers related to their activities in 'electronic/digital devices/media,'" the court held that there was probable cause to support the warrant.[27]

This is not an isolated incident; rather, this is common practice. The district court (affirmed by the Fourth Circuit) in *United States v. Harris* upheld a warrant on bare assumptions, citing several instances upon which courts in a variety of circuits have upheld warrants solely based on officers' general knowledge of how criminals operate with digital communications without any *particular* factual reason for believing the alleged criminal himself had a cell phone and without any description of the devices sought to be seized.[28] It appears that courts, desiring the potential wealth of evidence stored in a cellphone, turn a blind eye to the particularity requirement when reviewing warrants for electronic devices.

Courts have gone further, finding that "cell phones are such common and integral tools of the criminal trade that their incriminating nature is immediately apparent and therefore their seizure falls within the plain view exception to the warrant requirement."[29] Thus, regardless of whether an officer has done any level of due diligence in determining whether the suspect even owns a phone, the ubiquity of cell phones plus officers' general knowledge appears to have been sufficient for courts to uphold warrants that clearly fail the particularity requirement. Under this rationale, should officers fail to include these electronic devices within the warrant application, it appears that they could enter a home pursuant to an otherwise valid warrant and grab a cell phone charging on the kitchen counter. After all, the criminal nature of a cellphone is "immediately apparent."

Despite courts' selective blindness in issuing and upholding warrants, Fourth Amendment jurisprudence is clear: particularity is not an optional suggestion but an explicit requirement stated within the text of the amendment itself that is supported by years of Supreme Court decisions. The Constitution requires that "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."[30] The text of the amendment appears to be conjunctive, including a *dual* requirement: (1) probable cause, that is, "fair probability"[31] to believe that

26. United States v. Reed, No. 2:13-CR-29-1, 2013 WL 5503691, at *3 (D. Vt. Oct. 2, 2013).

27. *Id.*

28. United States v. Harris, No. 3:15CR170, 2016 WL 1441382, at *11–12 (E.D. Va. Apr. 11, 2016), *aff'd*, 688 F. App'x 223 (4th Cir. 2017), *cert. denied*, 138 S. Ct. 436 (2017).

29. *Id.* at *12.

30. U.S. CONST. amend. IV.

31. Illinois v. Gates, 462 U.S. 213, 214 (1983) ("The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, there is a fair probability that contraband or evidence of a crime will be found in a particular place. And the duty of a reviewing court is simply to

evidence will be found, and (2) particularity.[32] The "fair probability" based on the ubiquity of cellphones only partially satisfies the requirements for a valid warrant. The second requirement, particularity, demands a bit more than common knowledge that people own cell phones and that cell phones contain valuable information. Particularity demands a description of the "things to be seized."[33]

As the D.C. Circuit held in *Griffith*, "the requirement of particularity is closely tied to the requirement of probable cause."[34] In this way, the failure of particularity tarnishes instances where there may very well be a "fair probability" that evidence will be found, as is the case with ubiquitous items like cell phones. Therefore, the court correctly rejected the government's proposition that because nearly everyone now carries a cell phone, and because a phone frequently contains all sorts of information about the owner's daily activities, a person's suspected involvement in a crime ordinarily justifies searching her home for any cell phones, regardless of whether there is any indication that she in fact owns one.[35]

Further, the court's analysis challenges decisions that have leaned so heavily toward government interest and police expediency that they view electronic devices as almost *per se* criminal tools. The court correctly notes that the devices sought were "otherwise lawful objects," not "contraband items like 'weapons [or] narcotics.'"[36] The court explicitly deems cell phones as "innocuous" items that require care to ensure that the search is "conducted in a manner that minimizes unwarranted intrusions upon privacy."[37] Because the home is the "first among equals," "[t]he general pervasiveness of cell phones affords an inadequate basis for eroding that core protection."[38] Consequently, an officer must state with *particularity* his reason to believe that (1) the suspect owns a cell phone, (2) the phone contains incriminating information, and (3) the phone will be found within the home. Any less may satisfy the first requirement of "fair probability" but will (at least in the D.C. Circuit) fail the second requirement of particularity.

The D.C. Circuit's opinion also cuts against other circuits' propensity to uphold, if not encourage, warrants that allow overseizure in the digital device realm. As noted by Professor Adam M. Gershowitz, "particularity challenges are often made in computer search warrant cases," but "they

---

ensure that the magistrate had a substantial basis for concluding that probable cause existed.").

32. Groh v. Ramirez, 540 U.S. 551, 557 (2004) ("The fact that the *application* adequately described the 'things to be seized' does not save the warrant from its facial invalidity. The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents.") (emphasis in original).

33. *Id.*

34. United States v. Griffith, 867 F.3d 1265, 1275 (D.C. Cir. 2017).

35. *Id.* at 1274.

36. *Id.* at 1276.

37. *Id.*

38. *Id.* at 1275.

are rarely successful."[39] As shown in these cases, "the particularity guarantee has provided little protection to defendants in the digital context."[40] The two rare instances in which a court may invalidate warrants in the face of a particularity challenge are the following: (1) where the warrant fails to state the crime or fails to state a sufficient nexus between the alleged crime and the evidence sought, and (2) where a warrant uses overbroad language.[41] However, despite the few decisions that sustain these Fourth Amendment challenges to problematic warrants, many "search warrants authorize extremely broad searches that resemble general warrants," a few are invalidated, and many are saved by the good-faith exception.[42]

Some scholars agree with courts upholding overbroad warrants, arguing that overbroad search warrants are a necessary evil in the digital age. Professor Orin Kerr has explicitly stated that "courts should not impose limits at the physical search stage."[43] Admitting that "allowing a full seizure [of electronics] at the physical search stage technically permits an overseizure," Kerr argues that there is "no reasonable alternative given the time-consuming nature of electronic searches."[44] He likens a digital search to foraging through a haystack in search of a needle.[45] So, rather than have officers take "weeks or longer" on site to determine whether the device in question even belongs to the suspect, the government is justified in seizing the whole haystack.[46] It seems to be the only option when an agent might find "a dozen computers, five backup hard drives, ten flash drives, and 100 CD-ROMs."[47] It would be impractical for officers to linger in a citizen's home determining which devices fall within the scope of the search and which do not.[48] Instead, seize the day—and all the devices!

While the D.C. Circuit acknowledged that there may be circumstances in which a brief overseizure may be necessary to determine the device's relevance to the investigation, such as in cases where officers learn of a suspect's phone usage without direct description of the cell phone model,[49] the court refused to accept a warrant's facial overbreadth where there was no attempt to restrict the search. The court chastised the war-

39. Adam M. Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 VAND. L. REV. 585, 600 (2016). Note that this article is largely about warrants to search the contents of cell phones rather than physical overseizure of devices. However, Gershowitz's analysis also applies to courts' approach to overbroad search warrants.

40. *Id.* at 599.

41. *Id.*

42. *Id.* at 600.

43. Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1, 11 (2015).

44. *Id.*

45. *See id.*

46. *Id.*

47. *Id.* at 12.

48. *See id.*

49. United States v. Griffith, 867 F.3d 1265, 1276 (D.C. Cir. 2017).

rant in this case as failing to "establish probable cause to suspect that any cell phones or other electronic devices belonging to Griffith and containing incriminating information would be found in the apartment," yet turning around and authorizing "seizure of *all* cell phones and electronic devices, without regard to ownership."[50] The court could not tolerate the notion that the warrant as stated allowed officers to seize *all* cell phones even if officers had every reason to know that any given phone, in fact, did not belong to Griffith. Instead, the "warrant must be tailored to the justifications for entering the home," thereby demonstrating some attempt to limit "the scope of permissible seizure to devices owned by Griffith, or linked to the shooting."[51] While other courts have implied a limitation where an overbroad warrant fails to do so, such as reading the warrant in light of the crime alleged, the D.C. Circuit held that the lack of limitation on the face of the warrant rendered it impermissibly overbroad.

The court appears to give primacy where the Fourth Amendment does—to privacy rather than expediency. Despite Professor Kerr's assessment that the court got it wrong because "overseizure is necessary" and because "courts should allow it because you never know where the electronic evidence might be,"[52] the D.C. Circuit did not quite place a ban on overseizure where necessary. Instead, the court placed a prohibition on general warrants that refuse even a paltry attempt at limiting the scope of a predictably overbroad search. The D.C. Circuit merely required compliance with the Fourth Amendment: a particular basis for knowledge that the alleged criminal has a cell phone, a description of it, and reason to know that the cell phone will be within the home.[53] In the alternative, if ideal particularity (such as a description of the specific devices) cannot be achieved, officers must include some form of limitation within the warrant to keep from obtaining free-rein authority to seize even things that obviously do not involve the person or the crime in question.[54] In this regard, the ruling balances, rather than tips, the scale by allowing officers to overseize electronics where necessary so long as there is a limitation to protect individual privacy. This seems to harmonize with the purposes of the Fourth Amendment rather than allow blanket overseizure without so much as an attempt to circumscribe its intrusion on others within the home.

The D.C. Circuit's ruling in *Griffith* is undoubtedly controversial but not because it is legally erroneous. Quite the opposite, the ruling restores balance to warrant practices that have gone far afield from the Fourth

50. *Id.*
51. *Id.*
52. Orin S. Kerr, *D.C. Circuit Forbids Seizing All Electronic Storage Devices in Computer Warrant Cases*, WASH. POST (August 22, 2018), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/08/22/d-c-circuit-forbids-seizing-all-electronic-storage-devices-in-computer-warrant-cases/?utm_term=.19e948943a0c [https://perma.cc/FD4P-H6GV].
53. *See Griffith*, 867 F.3d at 1277.
54. *See id.*

Amendment's requirements and protections for individual privacy. In an era of digital pervasiveness, the *Griffith* court reminds law enforcement that there are constitutional limits to the searches they request. This may require officers to do more reconnaissance on the front-end: observe the suspect, ensure a factual basis for the searches to be executed, limit the scope, and demonstrate deference for the privacy interests inevitably invaded. The court makes it very clear that the preference for practicality over privacy has come to a screeching halt. Particularity is a constitutional requirement, and where officers or magistrates ignore this reality, not even the broadly applied good-faith exception will cure the deficiency.