Public Interest Law Reporter

Volume 23 | Issue 1 Article 4

2017

Smartphones, Fingerprints, and Search Warrants

Fabiola De Armas

Follow this and additional works at: https://lawecommons.luc.edu/pilr

 Part of the Civil Rights and Discrimination Commons, Criminal Procedure Commons, Environmental Law Commons, and the Human Rights Law Commons

Recommended Citation
Fabiola De Armas, *Smartphones, Fingerprints, and Search Warrants*, 23 Pub. Interest L. Rptr. 14 (2017).
Available at: https://lawecommons.luc.edu/pilr/vol23/iss1/4

This Article is brought to you for free and open access by LAW eCommons. It has been accepted for inclusion in Public Interest Law Reporter by an authorized editor of LAW eCommons. For more information, please contact law-library@luc.edu.

Loyola Public Interest Law Reporter

Smartphones, Fingerprints, and Search Warrants

Fabiola De Armas

This past decade alone, the smartphone evolved from a device solely used to make phone calls to a device that stores all aspects of life in addition to making phone calls. With advanced smart phones, individuals can store sensitive material, pictures, and personal information. Currently, in the criminal system, smartphones pose two fundamental issues: (1) whether smartphones can be seized during a search with a valid warrant; and (2) whether individuals can be compelled to provide their fingerprints to unlock their smartphones during a valid search without violating Fourth and Fifth Amendment rights to be free from unreasonable searches and seizures and self-incrimination.[1]

Courts have held that constitutional protections extend to smartphones, and violations of those protections can affect anyone who owns one.[2] In September 2017, the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation filed a suit in Boston's federal court on behalf of eleven travelers whose electronic devices were searched without a warrant.[3] The plaintiffs argued that searching personal electronic devices without a warrant based on probable cause violated "the constitutional rights of individuals to keep the private and expressive details of their lives free from unwarranted government scrutiny."[4]

Without a bright-line rule from the U.S. Supreme Court, federal courts face difficulties ruling on these issues. To address these two issues, federal courts must determine whether probable cause exists, whether fingerprints can be used to unlock coded cellphones, and whether a search has exceeded the scope of the warrant.[5]

---

1 U.S. CONST. amend. IV-V.

2 *Riley v. California*, 134 U.S. 2473, 2489 (2014) (finding cellphones store data subject to privacy protections).

3 Debra Cassens Weiss, *ACLU suit challenges warrantless searches of electronic devices at border*, ABA JOURNAL (Sept. 13, 2017), http://www.abajournal.com/news/article/aclu_suit_challenges_warrantless_searches_of_electronic_devices_at_border.

4 *Id.*

5 *See People v. McCarty*, 223 Ill. 2d 109, 149 (2006); *In re Application for a Search Warrant*, 236 F. Supp. 3d 1066, 1069 (N.D. Ill. 2017); *United States v. Winn*, 79 F. Supp. 3d 904, 914 (2015).

Published by LAW eCommons, 2017

PROBABLE CAUSE

A valid search warrant requires probable cause— "facts and circumstances known to the arresting officer at the time of the arrest would lead a reasonable person to believe that a crime had occurred and the suspect had committed it."[6] A valid search warrant must provide specific details of the location, identification, and nature the evidence expected to be recovered.[7] Generally, "a search warrant's description is sufficient if it enables the officer executing the warrant, with reasonable effort, to identify the place to be searched."[8] Valid warrants for electronic devices demand "specific facts as to who is involved in the criminal conduct linked to the subject premises, or specific facts as to what particular Apple-branded encrypted device is being employed (if any)" and specific details stating "what will be found at the subject premises and what the government expects to find at subject premises."[9]

FORCED FINGERPRINTING

Uncertainty exists with forced fingerprinting because unlocking a smartphone can constitute testimonial evidence.[10] Generally, the Constitution protects oral testimonial evidence but not fingerprints.[11] No rule addresses "forced fingerprinting" of individuals present during the search, including residents or visitors.[12] According to Magistrate Judge Mary M. Rowland of the US District Court for the Northern District of Illinois, the current rule states: if during a search, the smartphone's ownership is known, then the forced fingerprint to unlock the cellphone does not constitute testimonial.[13] However, if the smartphone's owner is not known, then the opposite results.[14]

For example, in *Application for a Search Warrant*, the warrant authorized the search and seizure and used specific language: "various items presumed to be located at a particularly identified location" and "various items including

---

6 *People v. McCarty*, *supra* note 6; *People v. Edgar*, 2014 IL App (1st) 141703, ¶ 110.

7 *People v. McCarty*, *supra* note 6.

8 *Id.*

9 *In re Application for a Search Warrant*, *supra* note 6.

10 *Hiibel v. Sixth Judicial Dist. Court*, 542 U.S. 177, 188 (2004) (fingerprinting can establish a suspect's connection with the crime).

11 *In re Application for a Search Warrant*, *supra* note 6.

12 *In re Application for a Search Warrant*, *supra* note 6; Phone Interview with Mary Rowland, Magistrate Judge, U.S. District Court for the Northern District of Illinois, in Chicago, IL (Nov. 2, 2017).

13 Interview with Mary Rowland, *supra* note 13.

14 *Id.*

various forms of electronic storage media and computer equipment."[15] The government sought the authority to "compel any individual who is present at the subject premises at the time of the search to provide his fingerprints and/or thumbprints 'onto the Touch ID sensor of any Apple iPhone, iPad, or other Apple brand device in order to gain access to the contents of any such device.'"[16] However, the Court found, the language of the latter part of the warrant was too broad and over-inclusive because it intended to authorize the search and seizure of any "persons at the Subject Premises" to apply their fingerprints to any Apple electronic device recovered at the premises.[17] In this case, forced fingerprinting violated Fourth and Fifth Amendment rights.[18] The smartphone's owner was not known, and compelling the individuals present during the search to "apply their fingerprints to any Apple electronic device recovered at the premises" constituted testimonial evidence and violated constitutional protections.[19]

WHETHER THE SEARCH EXCEEDED THE SCOPE OF THE WARRANT

The language of the warrant establishes the scope of the allowable search.[20] However, searching the contents of a smartphone generally requires an additional search warrant.[21] When information is uncovered on smartphones in the absence of additional search warrants, courts uphold individuals' constitutional rights against potentially incriminating information.[22] The additional search warrant remedies this issue by requiring police officers to specify details of the smartphone's content, and the information they intend to recover.[23]

The U.S. Supreme Court recognizes that cellphones have a "particularly powerful possessory interest" and an additional search warrant addresses these privacy issues.[24] For example, in *Riley v. California*, the Court found that "a cell phone is not immune from a search but that a warrant is generally required

15 *In re Application for a Search Warrant*, *supra* note 6 at 1066.

16 Id. at 1067.

17 Id. at 1068; Interview with Mary Rowland, *supra* note 13.

18 *In re Application for a Search Warrant*, *supra* note 6 at 1068.

19 *Id.*

20 *McCarty*, 223 Ill. 2d.

21 Interview with Mary Rowland, *supra* note 13.

22 *In re Application for a Search Warrant*, *supra* note 6 at 1074.

23 *Id.*

24 *United States v. Winn*, supra note 6.

before such a search, even when a cell phone is seized incident to arrest."[25] The state court litigation follows this ruling. In *People v. Davis*, the Illinois Appellate Court declined to extend "the search-incident-to arrest exception" to include searches of the data on a cellphone and held that "a warrant is generally required before such a search, even when a cell phone is seized incident to arrest."[26] The following year, in *People v. Butler*, the Illinois Appellate Court acknowledged "a search of a cellphone contains an immense amount of digital information pertaining to a person's 'privacies of life' and that as a result, cell phones implicate privacy concerns far beyond those implicated in searches of objects such as purses or wallets."[27]

The additional search warrant requirement for smartphones ensures that individuals are afforded a supplemental layer of protection by mandating that the language of the warrant address specific details of the location, identification, and nature of the information expected to be recovered.[28] In *United States v. Winn*, the Defendant was charged a misdemeanor of public indecency because he allegedly took inappropriate pictures of young children at the public pool and was fondling over his swimsuit.[29] The warrant authorized the officer to search "any or all files contained on said cellphone" which included photos, messages, and deleted items.[30] The warrant provided sufficient details specifying the scope of the search—the location and nature of the information the officer expected to be recovered.[31] While the Court found that the officer had probable cause to seize the Defendant's cellphone, the officer abused his discretion by exceeding the scope of the search, and the evidence was suppressed.[32] The Court reasoned that the officer did not have probable cause to "rummage through every conceivable bit of data, regardless of whether it bore any relevance to the criminal activity."[33] Thus, the Court found that the officer acted in good faith in applying for the search, but overstepped the scope of the

---

25 *Riley v. California*, supra note 2 at 2493.

26 *People v. Davis*, 2014 IL App (4th) 121040, ¶ 23.

27 *People v. Butler*, 2015 IL App (1st) 131870, ¶ 39.

28 Interview with Mary Rowland, *supra* note 13.

29 *United States v. Winn*, *supra* note 6 at 909, 911-12.

30 *Id.* at 911 (searching phone's "SIM Card or SD Card to include but not limited to the calendar, phonebook, contacts, SMS messages, MMS messages, emails, pictures, videos, images, ringtones, audio files, all call logs, installed application data, GPS information, WIFI information, internet history and usage, any system files on phone, SIM Card, or SD Card, or any data contained in the cellphone, SIM Card or SD Card to include deleted space").

31 *Id.*

32 *Id.* at 927.

33 *Id.* at 922.

search, and the evidence recovered violated the Defendant's Fourth Amendment rights.[34]

CONCLUSION

Smartphones, in addition to making phone calls, act as mini-computers and can store personal and sensitive information. In the wake of emerging technologies and fingerprint recognition features to unlock smartphones, two main questions arise regarding constitutional protections and search warrants: (1) whether smartphones can be seized during a search with a valid warrant; and (2) whether individuals can be compelled to provide their fingerprint to unlock their smartphone during a valid search without violating Fourth and Fifth Amendment rights to be free from unreasonable searches and seizures and self-incrimination.[35] Since a bright-line rule does not exist, answering these questions requires an analysis of whether probable cause exists, whether fingerprints can be used to unlock coded cellphones, and whether a search has exceeded the scope of the warrant.[36]

Smartphones can be seized during a search pursuant to a search warrant if probable cause exists and the seizure falls within the scope of the search warrant.[37] Additionally, individuals can be compelled to provide their fingerprints to unlock their smartphones during a valid search without violating constitutional rights.[38] However, the person conducting the search must have an additional search warrant detailing the specific content of the phone and the information expected to be recovered.[39] Then, the person conducting the search must determine whether the forced fingerprint constitutes testimonial evidence.[40] If the smartphone's owner is known, then the forced fingerprint does not constitute testimonial evidence.[41] However, if the smartphone's owner is not known, and the forced fingerprint is used to identify the owner, then the forced fingerprint constitutes testimonial evidence and violates constitutional rights.[42]

---

34 *Id.* at 926-27.

35 U.S. CONST. amend. IV-V.

36 *See People v. McCarty*, *supra* note 6; *In re Application for a Search Warrant*, *supra* note 6; *United States v. Winn*, *supra* note 6.

37 *People v. McCarty*, *supra* note 6.

38 Interview with Mary Rowland, *supra* note 13.

39 *In re Application for a Search Warrant*, *supra* note 6 at 1074.

40 *Id.*

41 *Id.*

42 *Id.*

The answers to these questions are highly fact and circumstance-specific. As smartphone technology continues to evolve to include features such as face and voice recognition, it is likely that courts will be faced with even more questions concerning constitutional rights and search warrants.[43] Because no bright-line rules exist for these rapidly evolving technologies, courts must continue to adapt and expand on these concepts that shape the nature of Fourth and Fifth Amendment rights and search warrants.

[43] *Id.*