THE FOURTH AMENDMENT IN THE TWENTY FIRST CENTURY: SMARTPHONES

Devika Singh*

In *Commonwealth v. Doleras*, the Supreme Judicial Court of Massachusetts upheld a warranted search of a defendant's iPhone photo library and found that the warrant affidavit showed probable cause to justify searching the entire phone.[1] The court, in validating the search warrant, set a narrow scope for Massachusetts' Fourth Amendment protections against unreasonable searches of smartphones. The court's decision also highlights the challenge U.S. courts face in defining the bounds of the Fourth Amendment right against unreasonable search and seizure as applied to increasingly sophisticated technology.[2]

In July 2011, after receiving reports of a shooting in Boston's Hyde Park, police discovered Michael Lerouge with gunshot wounds in his back.[3] Defendant Bricknell Doleras was near the scene of the crime, with gunshot wounds in his leg, and he was wearing a green jacket similar to the one described by witnesses to the shooting. A witness also testified that Doleras had been receiving threatening phone calls and text messages from Lerouge.[4] Chicago police eventually discovered a gun and iPhone in Doleras's apartment.[5] Based on the information above, the police believed that the iPhone contained evidence linking Doleras to Lerouge.[6] They obtained a warrant for the phone and found pictures of Doleras wearing a green jacket while holding a gun in the phone's photo library.[7]

Doleras filed a motion to suppress the photographs by arguing that the warrant affidavit contained probable cause to search text messages and images attached to text messages but not the phone's separate repository of pictures.[8] The trial court denied the motion and in January 2016, the Supreme Judicial Court of Massachusetts affirmed.[9] Judge Cordy, writing for the majority, held that the warrant, which permitted a

---

* Georgetown University Law Center, J.D. expected 2018. Ms. Singh is a Featured Online Contributor for the *American Criminal Law Review*.

[1] *See* Commonwealth v. Dorelas, 43 N.E.3d 306, 314 (Mass. 2016) (affirming denial of defendant's motion to suppress evidence obtained from iPhone's photo repository pursuant to a warrant).

[2] U.S. CONST. amend. IV, cl. 1.

[3] *Dorelas*, 43 N.E. 3d at 308.

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.* at 310.

[8] *Id.*

[9] *Id.* at 310, 314.

search of the entire cellphone, was supported by probable cause—based on witness testimony, the phone contained information linking Doleras to Lerouge.[10]

As dissenting Judge Lenk pointed out, however, Judge Cordy glossed over the fact that based on the information that police had at the time—that someone was threatening Dorelas over the phone—the police really only had probable cause to believe that Dorelas's *communications* might link him to Lerouge.[11] The police had justification under the Fourth Amendment to pull Dorelas's text messages, images attached to those text messages, and his phone records, but no additional facts to warrant searching any of the other stored information on his phone.[12] Judge Cordy countered by asserting that communications can come in many forms, including photographs.[13] He ignored the fact that the photo repository on a smartphone is similar to a computer hard drive; the photos are not communications unless sent to someone through text messages.

Why should the court have made a distinction? Some historical context is helpful. States ratified the Fourth Amendment in the eighteenth century, when an unreasonable search and seizure would most likely occur when law enforcement officers trespassed onto one's physical property.[14] Under Anglo-Saxon law, a man's home was considered his castle. When debating and writing the Fourth Amendment, the Founders wished to ensure that the sovereign state could not enter one's home arbitrarily.[15] Since then, Fourth Amendment law has evolved to focus on violations of one's privacy rather than trespass, but even today, the home receives the highest level of protection from unreasonable entry.[16] In today's world, however, a law enforcement official might discover more about a person retrieving data from his smartphone than rummaging through his house. Smartphones essentially function as a mini-computer, storing not only massive quantities of information, but also sensitive information, such as bank information and private photographs. The search of a smartphone could be a greater intrusion of one's privacy than the search of a home.

---

[10] *Id.* at 314.
[11] *Id.* at 316 (Lenk, J., dissenting).
[12] *Id.*
[13] *Id.* at 313.
[14] David Behm, *The Resurrection of the "Trespass" Element of Fourth Amendment Law*, MARQ. UNIV. L. SCH.: FAC. BLOG (Feb. 23, 2012), http://law.marquette.edu/facultyblog/2012/02/28/the-resurrection-of-the-trespass-element-of-fourth-amendment-law/.
[15] Joan Rapczynski, *Search and Seizure,* YALE-NEW HAVEN TCHR. INST. (2000), http://www.yale.edu/ynhti/curriculum/units/2000/2/00.02.04.x.html.
[16] *See* Katz v. United States, 389 U.S. 347, 349 (1967) (holding that federal agents using a listening device to overhear an individual's conversation inside a phone booth violated the Fourth Amendment right to privacy).

The founders also meant the Fourth Amendment to prevent courts from issuing general search warrants, or orders allowing law enforcement to conduct blanket searches of one's property.[17] In the revolutionary era, British officers used general search warrants to enforce tax collection—an officer could enter a colonist's home in the middle of the night at will and search everything.[18] In part to address this concern, the Fourth Amendment contains a "particularities" clause, requiring that a warrant specify the "place to be searched and the things to be seized."[19] The courts should rigorously apply the particularities requirement to searches of phones and computers. Americans' technological effects are treasure troves of information. A limitless search of a phone is similar to the general searches the Fourth Amendment was meant to guard against. Warrants should specify the different data repositories to be searched—for instance, communications—and provide probable cause for each.

Arguably, this standard could create arbitrary and cumbersome distinctions for law enforcement officials. Still, the courts must strike a balance between protecting the privacy of Americans and unreasonably burdening law enforcement. As Justice Sotomayor argued in *United States v. Jones*, a crucial check on law enforcement is the burden of limited resources.[20] As technology evolves, the burden grows lighter. Previously, law enforcement would have to spend days to learn information about a person now available on a single smartphone. Today, the police can extract that same information within minutes. Requiring specification of what parts of a phone are to be searched re-equalizes the balance between privacy and law enforcement interests.

Public policy also justifies specific search warrants for smartphones—a vast majority of Americans use them. According to a study conducted by the Pew Research Center, nearly two-thirds of Americans owned a smartphone in 2015.[21] This number had nearly doubled within a span of only four years—up from thirty-five percent in 2011.[22] Nineteen percent of Americans rely on smartphones to access the internet, either because they lack broadband at home or because they have few other options for online access.[23] Sixty-two percent of smartphone owners used their phone to look up information about a

---

[17] Rapczynski, *supra* note 15.
[18] *Id.*
[19] U.S. CONST. amend. IV, cl. 2.
[20] *See* United States. v. Jones, 132 S. Ct. 945, 956 (stating that GPS monitoring makes available large amounts of information at little cost to the government) (Sotomayor, J., concurring).
[21] Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RES. CTR. (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.
[22] *Id.*
[23] *Id.*

health condition.[24] Fifty-seven percent used their phone to conduct online banking.[25] Eighteen percent used it to submit a job application.[26] Without search warrants describing particularities, police can extract this information in an instant—even if there is no probable cause tying the information to a crime. With the potential privacy consequences for so many Americans, courts need to closely examine Fourth Amendment jurisprudence in the context of technology, and draw clear standards for the probable cause showing necessary to search data rich items such as smartphones.

[24] *Id.*
[25] *Id.*
[26] *Id.*