wiley

NEWSLETTER

Maryland Court of Appeals Updates the 'Particularity' Standard for Cell Phone Searches as U.S. Courts Develop New Doctrines for Electronic Evidence

September 2022

Privacy In Focus®

On August 29, 2022, the Maryland Court of Appeals issued its opinion in *Richardson v. Maryland*, expanding the protection of the Fourth Amendment for subjects of criminal investigations whose cell phones are subject to a warrant search.[1] In doing so, Maryland joins a small but growing number of states and federal district courts that have developed special rules for cell phone search warrants. And in dicta, Judge Jonathan Biran endorsed the use of "search protocols" in warrant applications for cell phones.[2] The *Richardson* decision is part of a growing trend in digital evidence warrants toward more narrowly tailored searches, specific search protocols, or device segmentation. Such a trend could trigger significant changes to law enforcement practices and the obligations of telecommunications and online services companies.

The Court of Appeals Found the Warrant to Search Richardson's Cell Phone Overly Broad

The Fourth Amendment requires that a search warrant must be based on probable cause, supported by oath or affirmation, and describe with particularity "the place to be searched, and the persons or things to be seized."[3] Petitioner Richardson was involved in a fight at a high school in Prince George's County, MD. When Richardson ran from the scene, the responding school resource officer found three smartphones and a handgun in the backpack Richardson left

Authors

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
jfbrown@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Privacy, Cyber & Data Governance

behind. Police linked one of the phones to a recent armed robbery that the perpetrators had arranged using an online marketplace app. Detectives then sought and obtained a warrant to search that phone. The warrant's broad language permitted officers to seize "[a]ll information, text messages, emails, phone calls (incoming and outgoing), pictures, videos, cellular site locations for phone calls, data and/or applications, geo-tagging metadata, contacts, emails, voicemails, oral and/or written communication and any other data stored or maintained inside of" the phone.[4]

In a suppression hearing, Richardson argued that allowing the police to search and seize "any and all information" and "any and all data" in the phone violated the particularity requirement of the Fourth Amendment.[5] The trial court denied the motion to suppress. On appeal, the Maryland Court of Special Appeals upheld the warrant on the grounds that the "detailed, particularized facts provided in the application and affidavit were incorporated into the search warrant."[6]

Maryland's highest court, the Court of Appeals, however, disagreed and held that the warrant to search Richardson's cell phone failed the particularity requirement. Citing the U.S. Supreme Court's 2011 decision in *Riley v. California*,[7] the Court of Appeals noted that "the particularity requirement is of even greater importance in the context of computers and smartphones than it is in the physical world," because they contain a detailed record of nearly all aspects of a user's life.[8]

The Maryland Court of Appeals ultimately upheld the State's use of the evidence derived from the cell phone because the police provided detailed information about the specific crime under investigation in the affidavit submitted as part of the application for the search warrant. The officers had reasonably relied on the warrant in executing the search of the cell phone and, as in most cases involving the outer boundaries of the Fourth Amendment, the good faith exception to the exclusionary rule applied to the fruits of the cell phone search.[9] However, the Court's finding the cell phone warrant invalid, and its discussion of balancing privacy concerns with law enforcement needs, are notable.

Courts Around the U.S. Are Developing New Doctrines for Electronic Evidence

Law enforcement officers face challenges in identifying all the possible places evidence might be found on a smartphone or computer. Electronic devices can hold vast quantities of documents across multiple data storage formats. Law enforcement may not know in advance where relevant electronic evidence will be located, and investigators are often challenged to review and exploit electronic evidence in a timely manner. The Maryland Court of Appeals identified three recent approaches to restricting electronic device searches in order to maintain Fourth Amendment protections:

- *First*, search protocols that outline for the court the technical means by which the government will decide what parts of the device to search and separate out what data on the device is subject to seizure and what is not.[10] One federal magistrate asked for a "sophisticated technical explanation" so that the Court could determine whether the government was making a genuine effort to limit itself to a particularized search.[11]

- *Second,* limits on the areas of the device, types of content, or time frame of the content to be searched, depending on the particulars of the warrant applications. The Massachusetts Supreme Judicial Court endorsed a time-limited approach in a 2021 case involving a cell phone.[12]
- *Third*, the Maryland Court of Appeals identified a developing body of decisions striking down warrants that use "catchall" terms such as "any and all information."[13] Reinforcing the factually-intensive nature of these inquiries, the Court allowed that broader "catchall" search terms may be permissible as rare exceptions when there is probable cause to believe a narrower search would miss hidden or mislabeled evidence, citing experience from financial fraud or child exploitation cases in which suspects intentionally concealed digital evidence on their devices.[14]

In analyzing the *Richardson* cell phone warrant, the Court of Appeals held that the language permitting search of "all information" and "any other data stored or maintained inside of" the phone was overly broad.[15] While recognizing that "[t]here is no "one size fits all" solution for ensuring particularity in cell phone search warrants,"[16] Judge Biran suggested that both temporal limits and limiting the search to the online marketplace app, "as well as texting and other communication applications, call logs, and navigation/location data for evidence relating to the crime of robbery" would have been appropriate in this case.[17]

The Court of Appeals also encouraged Maryland judges to consider including search protocols "in cell phone search warrants in appropriate cases."[18] Though dicta, this encouragement is an important development and could lead to the first widespread imposition of a search protocol requirement for cell phone searches. The validity and desirability of requiring search protocols before issuing a warrant to search electronic evidence is the subject of academic debate, with some commentators and magistrate judges arguing that *ex ante* search protocols are essential to fulfilling the particularity requirements. Others suggest that *ex ante* limits lack a constitutional basis and can never ultimately be more protective than a post-search review of the search's reasonableness. The *Richardson* decision makes it significantly more likely that Maryland will become the test ground for working through these issues.

Expectations for More Narrowly Tailored Search Protocols for Electronic Devices Are Likely to Increase

Looking forward, as judges begin to require the inclusion of search protocols in warrant applications for cell phones, law enforcement agencies throughout the U.S. will need to craft warrant applications that are more narrowly tailored to the specific device and information targeted. We anticipate that courts could also look to apply these protections to warrants for information stored online. As a result, challenges and claims stemming from alleged overbreadth or alleged lack of particularity are expected to increase in frequency as criminal defendants seek to suppress search warrant results. Wireless providers and companies that provide apps for cell phones, as well as online storage and services, should be aware of these potential changes and consider how to prepare to incorporate them into their legal and compliance operations.

[1] *Richardson v. Maryland*, slip op No. 46, September 2021 term, Maryland Court of Appeals https://www.courts.state.md.us/data/opinions/coa/2022/46a21.pdf

[2] *Id.* at 26-27.

[3] U.S. Const. amend IV.

[4] *Richardson v. Maryland* at 6-7.

[5] *Id.* at 9-10.

[6] *Richardson v. State*, 252 Md. App. 363, 390 (2021).

[7] *Riley v. California*, 573 U.S. 373, 393 (2014).

[8] *Richardson v. Maryland* at 22.

[9] *Richardson v. Maryland* at 42-43.

[10] *In re Cellular Telephones*, No. 14-MJ-8017-DJW, 2014 WL 7793690 at *8 (D. Kan. Dec. 30, 2014) (footnotes and citations omitted).

[11] *In the Matter of the Search of Apple iPhone IMEI 01388803738427*, 31 F. Supp. 3d 159, 169 (D.D.C. 2014)

[12] *Commonwealth v. Snow*, 160 N.E. 3d 277, 288 (Mass. 2021).

[13] *Richardson v. Maryland* at 30 (citing State v. Henderson, 854 N.W.2d, 616, 625, 633 (Neb. 2014)).

[14] *Id.* at 31.

[15] *Id.* at 33.

[16] *Id.* at 32.

[17] *Id.* at 36-37.

[18] *Id.* at 24.