IN THE SUPREME COURT OF MARYLAND

No. 36
September Term, 2022

STATE OF MARYLAND, *Petitioner*,

v.

DANIEL ASHLEY MCDONNELL, *Respondent*.

On Writ of Certiorari to the Appellate Court of Maryland

BRIEF OF *AMICI CURIAE* THE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS AND THE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF RESPONDENT

Brandon L. Boxler*
KLEIN THOMAS LEE & FRESARD
919 E. Main St., Suite 1000
Richmond, VA 23231
Tel.: (703) 621-2109
brandon.boxler@kleinthomaslaw.com

Ian K. Edwards*
KLEIN THOMAS LEE & FRESARD
101 W. Big Beaver Rd., Suite 1400
Troy, MI 48084
Tel: (248) 509-9272
ian.edwards@kleinthomaslaw.com

Terri S. Reiskin (AIS No. 9507130008)
NELSON MULLINS RILEY & SCARBOROUGH LLP
101 Constitution Ave. NW, Suite 900
Washington, DC 20001
Tel.: (202) 689-2814
terri.reiskin@nelsonmullins.com

Counsel for Amici Curiae. Additional counsel listed on inside cover.
**Motion for special admission pending.*

Elizabeth A. Franklin-Best
ELIZABETH FRANKLIN-BEST, P.C.
3710 Landmark Drive, Suite 113
Columbia, SC 29204
Tel.: (803) 445-1333
elizabeth@franklinbestlaw.com

David B. Smith
DAVID B. SMITH, PLLC
108 North Alfred Street, 1st Fl.
Alexandria, VA 22314
Tel.: (703) 548-8911
dbs@davidbsmithpllc.com

Counsel for Amicus Curiae
National Association of Criminal
Defense Lawyers

Jennifer Lynch
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: (415) 435-9333
jlynch@eff.org
andrew@eff.org

Counsel for Amicus Curiae
Electronic Frontier Foundation

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

INTEREST OF *AMICI CURIAE*

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. Founded in 1958, NACDL has a nationwide membership of approximately 10,000 lawyers, including private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges.

NACDL is dedicated to advancing the proper, efficient, and fair administration of justice. It files many *amicus* briefs each year in the U.S. Supreme Court and other federal and state courts, seeking to provide assistance in cases raising issues important to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole. NACDL has a particular interest in this appeal because it involves the Fourth Amendment, individual liberty, and privacy rights.

The Electronic Frontier Foundation ("EFF") is a member-supported, nonprofit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for more than 30 years. With roughly 35,000 active donors across the

country, including in Maryland, EFF represents technology users' interests in court cases and broader policy debates. EFF regularly participates both as direct counsel and as *amicus curiae* in the U.S. Supreme Court, the U.S. Court of Appeals for the Fourth Circuit, and other state and federal courts in cases addressing the Fourth Amendment and its application to new technologies.

Because this case asks the Court to apply the Fourth Amendment's consent exception to modern-day technologies, EFF believes it has a unique perspective to share that would benefit the Court's consideration of the question presented.[1]

INTRODUCTION

The State wrongly treats digital data like an ordinary physical object. Citing cases from the 1970s, the State argues that copying a piece of paper "provides a useful analogy" when considering whether McDonnell had a "reasonable privacy interest" in the data copied from his computer. Petitioner Br. 28. In the State's view, "copies of digital data" should be treated "no differently than photocopies of documents."

[1] No person other than *amici*, their members, or their counsel made any monetary or other contribution to the preparation or submission of this brief. Counsel for all parties to this appeal have consented to the filing of this brief.

Id. at 30. Suspects supposedly have no privacy interest in data copied from their computers during a period of consent because the data—and all personal information that can be gleaned from it—becomes "*the government's* property." *Id.* at 60 (emphasis in original). Police can keep, search, share, aggregate, and do whatever else they want with the copied data for any reason at any time, in perpetuity, without judicial oversight—and there is nothing the defendant can do about it.

The State's position ignores the "seismic shifts in digital technology" that have created "an entirely different species" of privacy interests that "do[ ] not fit neatly under existing precedents." *Carpenter v. United States*, -- U.S. --, 138 S. Ct. 2206, 2214-19 (2018). To compare photocopying a piece of paper to forensically copying a computer hard drive "is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Riley v. California*, 573 U.S. 373, 393 (2014). True, both involve "copies." But the similarities end there. The information that can be obtained from computer data, "as a category, implicate privacy concerns far beyond those implicated by the" information that can be obtained from a piece of paper. *Id.* at 393.

"It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001). Ignoring the heightened privacy interests that attach to digital data would impermissibly allow "technology to erode the privacy guaranteed by the Fourth Amendment." *Kyllo*, 533 U.S. at 34.

The constitutional analysis, then, must reflect—not ignore—the heightened privacy interests that attach to personal data stored on modern-day technologies. Those interests compel the conclusion that McDonnell retained a reasonable expectation of privacy in the data police copied from his computer. The Court should affirm the decision of the Appellate Court of Maryland.

ARGUMENT

The "central concern underlying the Fourth Amendment" is to avoid "giving police officers unbridled discretion to rummage at will among a person's private effects." *Arizona v. Gant*, 556 U.S. 332, 345 (2009). Yet that is precisely what would happen under the State's proposed rule: police would *own* a person's digital data after copying it "during the period of consent," giving the government carte blanche authority to

rummage through the person's personal data anytime, anywhere—in perpetuity—*even if* the person later revokes consent. Petitioner Br. 8. Such "general, exploratory rummaging" by the government was "abhorred by the colonists" and was a key reason they enacted the Fourth Amendment. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

I. Computers And Other Technological Devices Store Huge Quantities Of Highly Sensitive Personal Information.

Computers, cell phones, and other technologies "implicate privacy concerns far beyond those implicated by the search of" ordinary "physical items." *Riley*, 573 U.S. at 393. Digital devices have immense storage capacity and can hold a "record of nearly every aspect of [our] lives, from the mundane to intimate." *Id.* at 395. For these reasons, the Supreme Court held in *Riley* that the "search incident to arrest" exception to the Fourth Amendment's warrant requirement *allows* warrantless searches of the "physical aspects" of a cell phone but *prohibits* warrantless searches of the phone's "[d]igital data." *Id.* at 387; *see also* Petitioner Br. 54 (conceding that "*Riley* recognized a privacy interest in the digital contents of a cell phone distinct from that in the physical aspects of the phone").

The privacy concerns that animated *Riley* nearly ten years ago are far more substantial today. When the Supreme Court decided *Riley* in 2014, the top-selling smartphone could store 16 gigabytes of data. *See Riley*, 573 U.S. at 394. The *minimum* storage available on Apple's current line of iPhones is now 128 gigabytes. *See* Apple, *BuyiPhone14*, https://tinyurl.com/52nubey5 (last visited Apr. 29, 2023). That's about 6,400,000 printed pages. *See* FindLaw, *eDiscovery Processing: Metrics*, https://tinyurl.com/weh9bhmk (last visited May 1, 2023).

The storage capacity of computers is far greater. A modern MacBook laptop comes with up to 2 *terabytes* of storage, which is equal to 2,000 megabytes or roughly 100,000,000 printed pages—about 40,000 boxes. *See* Apple, *MacBook Pro 13*, https://tinyurl.com/5ananwv9 (last visited Apr. 24, 2023); FindLaw, *eDiscovery Processing: Metrics*, https://tinyurl.com/weh9bhmk (last visited May 1, 2023).

The storage capacity of a modern-day computer "is akin to a virtual warehouse of private information." Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 551-52 (2005). Computers store so much data that police cannot possibly search all of it in a matter of minutes, hours, or even days—which is why police create a copy of the

data to search over time, as they did here. *See United States v. Hill*, 459 F.3d 966, 974-75 (9th Cir. 2006) ("[T]he officers would have to examine every one of what may be thousands of files on a disk—a process that could take many hours and perhaps days.").

What type of information is stored on computers is also constitutionally significant. "There is a world of difference between the limited types of personal information" that police could learn from searching an object in the pre-digital era and the "exhaustive chronicle" of information that police can learn from searching a digital device. *Carpenter*, 138 S. Ct. at 2219. In the past, the most invasive type of search would involve "ransacking [a suspect's] house for everything which may incriminate him." *United States v. Kirschenblatt*, 16 F.2d 202, 203 (2d Cir. 1926) (Hand, J.). Today, searching a cell phone, computer, or other technological device "would typically expose to the government far *more* than the most exhaustive search of a house." *Riley*, 573 U.S. at 396. That is because these devices contain "in digital form many sensitive records previously found in the home" *plus* "a broad array of private information never found in a home in any form." *Id.* at 396-97.

And it's not just documents. The potential types of data stored on computers include banking and financial records, medical records, photos, emails, internet search histories, calendar entries, videos, Facebook messages, Twitter posts, passwords, and more—all dating back years, or even decades. *See Smallwood v. State*, 113 So. 3d 724, 731-32 (Fla. 2013) (explaining that "[v]ast amounts of private, personal information can be stored and accessed in or through . . . small electronic devices"). "The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal [information] in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs." *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009); *see also United States v. Gourde*, 440 F.3d 1065, 1077 (9th Cir. 2006) (Kleinfeld, J., dissenting) (describing the "many secrets on people's computers, most legal, some embarrassing, and some potentially tragic in their implications").

Indeed, the data stored on computers is typically more sensitive and more extensive than the data stored on cell phones—the type of digital device at issue in *Riley*. An increasing number of people routinely backup

their phone data to their computers, meaning the data from the phone is often the *minimum* amount of personal data available on a computer. *See* Petroc Taylor, *Frequency of Data Backups Among Adult Computer Owners in the United States in 2008 and 2018*, Statista (May 23, 2022), https://tinyurl.com/2yz93tfe.

Further, because computers have larger storage capacities and can run more powerful software programs, people use computers for more time-intensive, complicated projects. *See* Computer Hope, *Computer vs. Smartphone* (Nov. 6, 2021), https://tinyurl.com/mvb6et3u. People also conduct more thorough web searches on their computers, leaving behind a more robust digital trail of information. *See* Margaret Tinger, *Mobile vs Desktop: 13 Essential User Behaviors*, Appticles (Mar. 5, 2016), https://tinyurl.com/3erfv7fd; *see also* Eric Enge, *Mobile v. Desktop Usage in 2020*, Perficient (Mar. 23, 2021), https://tinyurl.com/ybzw5at9 (reporting that U.S. consumers spend an average of 323 seconds per website with 3.68 page views on a computer, compared to 158 seconds per website with 2.54 page views on a cell phone).

Consider the incredibly detailed information that can be gleaned from just one type of data on a computer: internet search history.

Information about what a person searched—and when—can reveal social interests, sexual preferences, medical history, political beliefs, past whereabouts, and other personal information. Internet search history data can also include downloaded files, bookmarks, cookies,[2] metadata,[3] and other granular information that many people might not know exist but that reveal even *more* intimate details about someone's life. As a former official of the National Security Agency put it, "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content." David Cole, *We Kill People Based on Metadata*, N.Y. Review of Books (May 10, 2014, 10:12 AM), https://tinyurl.com/r7ex2654 (quoting former NSA General Counsel Stewart Baker); *see also Riley*, 573 U.S. at 394 ("The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions.").

---

[2] "Cookies are text files with small pieces of data—like a username and password—that are used to identify your computer as you use a computer network." Kaspersky, *What are Cookies?*, https://tinyurl.com/46ud5s8h (last visited Apr. 29, 2023). They let websites recognize users, personalize sessions, suggest items to purchase or keep in shopping carts, build targeted advertisements, and more. *See id.*

[3] Metadata is hidden reference data in essentially every computer file that helps to describe, sort, and identify digital information. *See* TechTarget Network, *Metadata*, https://tinyurl.com/589ryh6z (last visited Apr. 29, 2023). For simple documents, metadata includes information such as how and when the file was created, who created it, the location of creation, and more. *See id.*

Forensic searches of digital data also "frequently involve searching personal information relating to the subject of the search *as well as third parties*." *In re Cunnius*, 770 F. Supp. 2d 1138, 1144 (W.D. Wash. 2011) (emphasis added). That is because emails, social media messages, photographs, videos, and other data (and metadata) on a computer can reveal information about friends, colleagues, and strangers. Many computers are also shared with family members or other people, which increases the number of third parties whose personal information might be collected and revealed in a forensic search of computer data. *See id.*

There is simply no physical analogue to digital data. Given the immense amount of personal information stored on computers and other digital devices, a search of a computer "implicate[s] privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Riley*, 573 U.S. at 393. Copying and searching data on a computer is nothing like copying and searching a piece of paper—or even a bulging file cabinet of hard copy documents. And as technology continues to evolve, the amount of information created and stored on digital devices will only increase. So too will the privacy expectations that attach to that information.

II. Police Are Increasingly Collecting And Searching Digital Data Without Judicial Oversight.

The digital era has led to the creation of "an entirely different species" of easily searchable information and a dramatic increase in police power to invade privacy rights. *Carpenter*, 138 S. Ct. at 2222. With a few clicks, police can access an incredible amount of personal information that was unimaginable just a few decades ago.

Police are using this newfound power—a lot. "Computer forensic examination is now a common tool in all types of criminal investigations." Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 Berkeley J. Crim. L. 112, 112 (2011). This is due, in part, to how easy it is to use computers "to communicate to cohorts, ensnare victims, and generally to prepare and orchestrate criminal conduct." *United States v. Vilar*, 2007 U.S. Dist. LEXIS 26993, at *115 (S.D.N.Y. Apr. 4, 2007). But it is also due to the ease with which police can copy a treasure trove of information from a digital device and then perform multiple searches on the information at a later date. *See* Darren R. Hayes, A Practical Guide to Computer Forensics Investigations, at 86 (2014) (noting that police can "clone" a hard drive—*i.e.*, transfer a "bit-for-bit copy"—in "less than an hour").

Police usually search a digital device after making a copy or "image" that replicates all of the data on the original. Kerr, *supra*, 119 Harv. L. Rev. at 540-41. Imaging software is even "capable of retrieving files that have been deleted, increasing the amount of digital information available to the government during the search." Sean O'Grady, Note, *All Watched Over by Machines of Loving Grace: Border Searches of Electronic Devices in the Digital Age*, 87 Fordham L. Rev. 2255, 2270 (2019). Imaging duplicates "the entire target drive, . . . including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original." Petitioner Br. 20-21 (quotation marks omitted).

Police even have tools to copy digital data "in the field" without a warrant as soon as someone gives consent. For example, "mobile device forensic tools" or "MDFTs" allow police to extract "the maximum amount of information possible" from a cell phone, including a user's contacts, call logs, text conversations, photos, videos, saved passwords, GPS location records, phone usage records, online account information, app data, and more. Logan Koepke et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*, Upturn.org (Oct. 2020), at 10, 16 https://tinyurl.com/jz95phv9. MDFTs can also access data

stored remotely in the cloud and collect data the user previously deleted. *Id.* at 16-17, 21-23. These tools even use login credentials stored on the phone to extract data from apps, websites, and services that are otherwise password-protected. *Id.* at 17-20.

The data police collect from a digital device can be organized, sorted, and searched to identify connections in the extracted data. *See* Koepke, *supra*, at 7, 13. Using a range of software tools, police can aggregate data from different locations on the device and sort it by location, file type, or the time and date of creation. *See id.* They also can combine the data with information from other sources—*e.g.*, police surveillance databases or gang databases—to create even more powerful searches. *See id.* at 53-54. These techniques empower police to view the data in ways a phone user cannot, gaining insights that would be impossible if the data remained siloed on the device itself.

The advent of cloud computing has further increased the amount of data police can obtain from a digital device. Cloud computing allows an internet-connected device to "display data stored on remote servers rather than on the device." *Riley*, 573 U.S. at 397. By copying account credentials stored on a computer, police can access from the computer

"any cloud data that the user has access to," including social media data, historical email data, or "backups of photos or other data." Koepke, *supra* at 17. Police could, for instance, "siphon and collect all data from an iCloud account, or all emails from a Gmail account," even if that information—which could be years or decades old—is stored in the cloud instead of on the computer's hard drive. *Id.* at 54.

In the State's view, if police copy a computer's data with consent, they could collect all of this personal information, store it indefinitely, combine it with other data, and run any searches on it at will without limitation, without a warrant, and without judicial oversight. And the owner of the computer can do nothing to stop them. Because the copied data supposedly becomes "*the government's property*," anything goes. Petitioner Br. 60 (emphasis in original).

III. The Consent Exception Should Reflect The Heightened Privacy Expectations That Attach To Digital Data.

The State's Fourth Amendment analysis (i) flouts the heightened privacy interests that attach to digital data and (ii) relies on an artificial distinction between searching data on a computer and searching a copy of the same data.

A. People Have Heightened Privacy Interests In Their Digital Data Regardless Of Where The Data Is Stored.

Searches of digital data "differ in both a quantitative and a qualitative sense" from ordinary physical objects. *Riley*, 573 U.S. at 393. Those differences are not just constitutionally *significant*; they can be constitutionally *dispositive*, as in *Riley*. "[T]he uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property." *United States v. Cotterman*, 709 F.3d 952, 966 (9th Cir. 2013); *see also State v. Wilson*, 315 Ga. 613, 622 (2023) (Pinson, J., concurring) (explaining that "it is pretty hard to read all of the reasons *Riley* gave for [its] holding and come away thinking that the rest of the Fourth Amendment is business as usual" when it comes to digital devices).

The U.S. Supreme Court first recognized the possibility of a consent exception to the Fourth Amendment's warrant requirement in 1921. *See Amos v. United States*, 255 U.S. 313, 314 (1921). It took another 25 years for the Court to revisit the exception. *Zap v. United States*, 328 U.S. 624 (1946). And about 25 years later, the Court held that "consent" alone is

a legal basis for a search, even if the person who consented was not aware of the right to refuse. *Schneckloth v. Bustamonte*, 412 U.S. 219 (1973).

A lot has changed since *Amos*, *Zap*, and *Schneckloth*. Failing to recognize these differences upsets legitimate expectations of privacy in data harvested from technologies that were "nearly inconceivable" when the consent doctrine was first developed. *Riley*, 573 U.S. at 385.

Analyzing the constitutionality of a consent-based warrantless search is not as simple as mechanistically applying consent cases involving traditional physical objects (*i.e.*, those that can be photocopied). "When confronting new concerns wrought by digital technology," courts must be "careful not to uncritically extend existing precedents." *Carpenter*, 138 S. Ct. at 2222. The Court "should not mechanically apply the rule used in the predigital era to the search" of modern-day digital devices. *Riley*, 573 U.S. at 406-07 (Alito, J., concurring); *see also United States v. Miller*, 425 U.S. 435, 451-52 (1976) (Brennan, J., dissenting) ("Development of . . . electronic computers and other sophisticated instruments have accelerated the ability of the government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently judicial interpretations of the reach

of the constitutional protection of individual privacy must keep pace with the perils created by these new devices.").

Rather than "tread carefully" given the unique aspects of digital technologies, *Carpenter*, 138 S. Ct. at 2220, the State makes mechanical arguments built on precedents involving "photocopies of documents," Petitioner Br. 28. It argues that "copies of digital data" are "no different[ ] than photocopies of documents," *id.* at 20, urging this Court to "hold that an individual has no reasonable expectation of privacy in a copy of digital data created within the scope of their consent," *id.* at 44.

A copy of a piece of paper is nothing like a copy of computer data. A piece of paper can reveal a discrete amount of information; a computer's hard drive can reveal intimate details about every aspect of someone's life. The nature of the privacy invasion from searching digital data "bears little resemblance to the type of . . . physical search[es]" of paper—or even reams of paper—that courts have considered in past consent cases. *Riley*, 573 U.S. at 386. The Fourth Amendment analysis should be viewed "through the same lens *Riley* did—that is, one that accounts for the uniquely expansive and complex nature of [digital] data." *Wilson*, 315 Ga. at 625 (Pinson, J., concurring); *see also State v. Smith*, 124 Ohio 3d

163, 169 (2009) (recognizing that computers "are entitled to a higher expectation of privacy").

The State's position—that people have no privacy interest *in their own personal information* revealed in data copied from a digital device—would invite misuse and abuse, defying "the Fourth Amendment's goal to curb arbitrary exercises of police power." *United States v. Jones*, 565 U.S. 400, 416-17 (2012) (Sotomayor, J., concurring). It would mean that a suspect *forever* lacks the ability to stop law enforcement from storing and searching the copied data and "min[ing] [it] for information years into the future." *Id.* at 415. Police could search it when they want, how they want, for whatever reason they want—even if the purpose of the search had nothing to do with the reason police obtained consent in the first place. Such indiscriminate searches were the very "evils that motivated the framing and adoption of the Fourth Amendment." *Payton v. New York*, 445 U.S. 573, 583 (1980).

B. The State's Effort To Distinguish Between Computer Data And Copies Of Computer Data Makes No Sense And Defies Reasonable Expectations Of Privacy.

The State's position puts unbearable weight on a purported distinction between the data stored on a computer and a copy of that data

stored elsewhere. It argues that "McDonnell always retained a property interest in his laptop hard drive and could therefore expect to reassert a privacy interest" in the data on the computer itself, Petitioner Br. 60, but he "lacked any reasonable expectation of privacy in the image copy created with his consent," *id.* at 13. In the State's view, "McDonnell had different privacy interests in his laptop hard drive and the image copy." *Id.* at 52; *see also id.* at 45 (arguing that "distinct copies of data can merit different Fourth Amendment treatment).

As the State concedes, however, a forensic copy of digital data contains the *exact same* information as the data on the computer itself. *See* Petitioner Br. 20-21. So it makes no sense to say that a person who revokes consent has a reasonable expectation of privacy in the information as it is stored on the computer but lacks a reasonable expectation of privacy in the *same information* as it is stored on the copy. The information is identical. Thus, "identical privacy concerns" apply regardless of where the information is stored. *United States v. Metter*, 860 F. Supp. 2d 205, 212 (E.D.N.Y. 2012).

The State's "hairsplitting argumentation has no place in an inquiry addressed to the issue of reasonableness." *New Jersey v. T. L. O.*, 469

U.S. 325, 346 n.12 (1985). It is "troublesome and artificial to treat copies as different from originals." Kerr, *supra*, 119 Harv. L. Rev. at 564.

If a person has a reasonable expectation of privacy in their emails, bank records, or other digital data, they have a reasonable expectation of privacy in their emails, bank records, or other digital data. Period. *Where* that information exists does not change the privacy expectation, which attaches to the information regardless of where the information is stored. It therefore does "not matter if data is copied, transferred, or otherwise manipulated." Kerr, *supra*, 119 Harv. L. Rev. at 564.

In short, a person's expectation of privacy in their data does not change if the data is stored on the computer's hard drive, in the cloud, on a remote server, on a police thumb drive, or somewhere else. "The Fourth Amendment protects *information* in which one has a reasonable expectation of privacy." *United States v. Jarmon*, 14 F.4th 268, 272 (3d Cir. 2021) (emphasis added), *cert. denied*, 142 S. Ct. 930 (2022). The expectation of privacy "resides in the data itself, not in the medium on which it is stored." *People v. McCavitt*, 2021 IL 125550, ¶ 68 (2021).

IV. McDonnell Retained A Reasonable Expectation Of Privacy In His Personal Data.

The "touchstone" of the constitutionality of any warrantless search is "reasonableness." *Samson v. California*, 547 U.S. 843, 855 n.4 (2006); *see also Florida v. Jimeno*, 500 U.S. 248, 250 (1991) (same). "[T]he reasonableness of a search is determined '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 government interests.'" *United States v. Knights*, 534 U.S. 112, 118-19 (2001) (citation omitted). Without analyzing the discrete privacy interests associated with the location of a search, a court cannot determine whether the search violated a reasonable expectation of privacy.

Applying that Fourth Amendment framework here compels the conclusion that McDonnell had a reasonable expectation of privacy in the copy of his digital data after he revoked his consent. Given the amount of personal information revealed in data contained on digital devices, society would and should recognize that people do not forever forfeit their right to privacy in their data just because they consented to a search long enough for police to make a copy.

This conclusion is further supported by the nature of consent searches, which are inherently coercive and are by far the most common type of warrantless searches today. *See, e.g.*, Ric Simmons, *Not "Voluntary" But Still Unreasonable: A New Paradigm for Understanding the Consent Searches Doctrine*, 80 Ind. L.J. 773, 773 (2005) (reporting that more than 90 percent of warrantless searches are accomplished through the use of consent); Rebecca Strauss, Note, *We Can Do This the Easy Way or the Hard Way: The Use of Deceit to Induce Consent Searches*, 100 Mich. L. Rev. 868, 871 (2002) (similar). "[M]ost people would not feel free to deny a request by a police officer." Marcy Strauss, *Reconstructing Consent*, 92 J. Crim. L. & Criminology 211, 236 (2002). "This may be especially true for racial minorities, who are disproportionately stopped and asked to submit to consent searches." Roseanna Sommers & Vanessa K. Bohns, *The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance*, 128 Yale L.J. 1962, 1968-69 (2019).

Suspects, victims, witnesses, and other people understandably feel pressure to "consent" when police ask for permission to perform a search. *See* Janice Nadler, *No Need to Shout: Bus Sweeps and the Psych of*

Coercion, 2002 Sup. Ct. Rev. 153, 156 (2002). "Implicit in the introduction of the officer and the initial questioning is a show of authority to which the average person encountered will feel obliged to stop and respond. Few will feel that they can walk away or refuse to answer." *Lawrence v. United States*, 566 A.2d 57, 61 (D.C. 1989). "All the police must do is conduct what will inevitably be a charade of asking for consent. If they display any firmness at all, a verbal expression of assent will undoubtedly be forthcoming." *Schneckloth*, 412 U.S. at 284 (Marshall, J., dissenting).

Under the State's view, people who "consent" to a search of their digital device to end a traffic stop or even to help police find a suspect could wind up losing *all* privacy interests in *all* data police can copy before consent is revoked. As technology is making it easier for police to quickly image the contents of a digital device, a "consent" period of only a few minutes or a few seconds could be long enough for police to copy enough data to obtain information about "nearly every aspect" of someone's life, "from the mundane to the intimate." *Riley*, 573 U.S. at 395. A split-second decision—by a suspect, witness, or victim—to grant

consent could mean losing a right to privacy in *decades* of highly personal information, even if consent is revoked moments later.

That result is unreasonable. A lay person would not understand the drastic implications of consenting to a search under the State's proposed rule—*i.e.*, irretrievably giving the State *ownership* of decades' worth of personal data. Even a person with some knowledge about the breadth of digital data and the invasiveness of forensic search tools might not fully appreciate just how revealing such searches could be given the "virtually unlimited" personal details stored on computers and other digital devices. *Riley*, 573 U.S. at 399. The "power and information asymmetries . . . are egregious." Koepke, *supra*, at 59.

The State provides a useful analogy to see why. It argues that what police did here is "no different than if one makes a file publicly available and the State downloads a copy: the owner cannot reasonably claim to retain a privacy interest in the downloaded copy just because he could shut off access to the original in the future." Petitioner Br. 38. But no reasonable person would voluntarily make public *all* of their bank records, emails, search history, medical records, and other private information; people closely guard such digital data with passwords,

multifactor authentications, and other security tools. And if *some* of that information gets publicly exposed, people panic, rush to change passwords, hire experts to prevent identify theft, and do whatever else they can to restore the privacy of their personal information.

It strains credulity, then, to argue that a person effectively agrees to make their personal information "publicly available" when consenting to police copying a digital device. A reasonable person in that situation would not believe that consenting would let the government use powerful tools to transform *the person's* private data into "*the government's* property," and then authorizing the government to do whatever they want with the data in perpetuity. Petitioner Br. 60 (emphasis in original). The person would believe—rightly so—that consenting would *not* mean that they have lost all expectation of privacy in their personal information, especially if they later revoke their consent. Consenting to a search when confronted by a police officer is nothing like sharing with the public every intimate detail of information stored on a digital device.

Indeed, research has confirmed that police often obtain consent from people who do not fully understand their rights and the nature of the searches police will perform. *See* Koepke, *supra*, at 60 & n.195. The

form McDonnell signed, for example, did not specify how police would search his data, what tools they would use to search it, how long they would keep his data, the scope of the search(es), whether they would combine the data with other databases to perform searches, and so on. "[A] consent form may do relatively little to improve a suspect's understanding of her rights, particularly when the suspect is poorly educated, frightened, or otherwise unable to understand the form." Nancy Leong & Kira Suyeishi, *Consent Forms and Consent Formalism*, 2013 Wis. L. Rev. 751, 753 (2013).

No reasonable person in McDonnell's position would think he or she was consenting to the government forever taking ownership of all data stored on the device. Nor would the average person know that police have powerful forensic tools to extract and search the data, including data the person had deleted in an effort to keep the information private.

* * *

"With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities." *Arizona v. Evans*, 514 U.S. 1, 17-18 (1995) (O'Connor, J., concurring). "New technologies bring with them not only new opportunities for law

enforcement to catch criminals but also new risks for abuse and new ways to invade constitutional rights." *United States v. Denson*, 775 F.3d 1214, 1218 (10th Cir. 2014). The State gives short shrift to these heightened constitutional responsibilities, glossing over the substantial privacy interests that McDonnel had—and has—in his digital data. Those interests exist regardless of where the data is stored.

CONCLUSION

The rule this Court adopts should account for the heightened privacy interests that attach to the huge amounts of highly personal data stored on computers, cell phones, and other digital devices. The rule also "must take account of more sophisticated systems" of searching data "that are already in use or in development." *Kyllo*, 533 U.S. at 36. Those considerations compel the conclusion that McDonnell retained a reasonable expectation of privacy in the data police copied from his computer. The Court should affirm the decision of the Appellate Court of Maryland.

Dated: May 5, 2023

Respectfully submitted,

/s/ Brandon L. Boxler*
KLEIN THOMAS LEE & FRESARD
919 E. Main St., Suite 1000
Richmond, VA 23231
Tel.: (703) 621-2109
brandon.boxler@kleinthomaslaw.com

Ian K. Edwards*
KLEIN THOMAS LEE & FRESARD
101 W. Big Beaver Rd., Suite 1400
Troy, MI 48084
Tel: (248) 509-9272
ian.edwards@kleinthomaslaw.com

Terri S. Reiskin (AIS No. 9507130008)
NELSON MULLINS RILEY &
SCARBOROUGH LLP
101 Constitution Ave. NW, Suite 900
Washington, DC 20001
Tel.: (202) 689-2814
terri.reiskin@nelsonmullins.com

*Counsel for Amici Curiae. *Motion for special admission pending.*

Elizabeth A. Franklin-Best
ELIZABETH FRANKLIN-BEST, P.C.
3710 Landmark Drive, Suite 113
Columbia, SC 29204
Tel.: (803) 445-1333
elizabeth@franklinbestlaw.com

David B. Smith
DAVID B. SMITH, PLLC
108 North Alfred Street, 1st Fl.
Alexandria, VA 22314
Tel.: (703) 548-8911
dbs@davidbsmithpllc.com

Counsel for Amicus Curiae
National Association of Criminal
Defense Lawyers

Jennifer Lynch
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: (415) 435-9333
jlynch@eff.org
andrew@eff.org

Counsel for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF WORD COUNT AND COMPLIANCE WITH RULE 8-112

1. This brief contains 5,675 words, excluding the parts of the brief exempted from the word count by Rule 8-503.2

2. This brief complies with the font, spacing, and type-size requirements stated in Rule 8-112.

/s/ *Terri S. Reiskin*
Terri S. Reiskin
Counsel for *Amici Curiae*

CERTIFICATE OF SERVICE

Pursuant to Rule 20-201(g), I certify that on May 5, 2023, the foregoing brief was served via the MDEC File and Serve Module and that, pursuant to Rule 8-502(c), two copies each were mailed, postage prepaid, first-class to:

Anthony G. Brown
Andrew H. Costinett
Office of the Attorney General
Criminal Appeals Division
200 Saint Paul Place
Baltimore, MD 21202

Counsel for Petitioner

/s/ Terri S. Reiskin
Terri S. Reiskin
Counsel for *Amici Curiae*