IN THE SUPREME COURT OF MARYLAND

September Term, 2022

NO. 36

STATE OF MARYLAND,

Petitioner,

v.

DANIEL ASHLEY MCDONNELL,

Respondent.

ON WRIT OF CERTIORARI TO THE APPELLATE COURT OF MARYLAND

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION (ACLU) AND THE ACLU OF MARYLAND

IN SUPPORT OF RESPONDENT, BY WRITTEN CONSENT

Jennifer Stisa Granick
Of Counsel
American Civil Liberties Union Foundation
39 Drumm Street
San Francisco, CA 94111

David R. Rocah
(MD Bar ID 0312050001)
Counsel for Amici Curiae
ACLU of Maryland Foundation
3600 Clipper Mill Road, Suite 350
Baltimore, MD 21211
(410) 889-8555
rocah@aclu-md.org

(Additional of counsel listed on following page)

Brett Max Kaufman
Of Counsel
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

RULES & CONSTITUTIONAL PROVISIONS

OTHER AUTHORITIES

STATEMENT OF INTEREST

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to defending the principles embodied in the Federal Constitution and our nation's civil rights laws. The ACLU of Maryland is the local affiliate of the ACLU. The ACLU and the ACLU of Maryland have frequently appeared before courts—including this one—in Fourth Amendment cases, including in cases involving searches of electronic information based on consent, both as direct counsel—s*ee, e.g.*, *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021) (en banc)—and as *amici curiae*, *see, e.g.*, *People v. Hughes*, 958 N.W.2d 98 (Mich. 2020); *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021); *State v. Burch*, 961 N.W.2d 314 (Wisc. 2021); *State v. Mefford*, 517 P.3d 210 (Mont. 2022); *People v. McCavitt*, 185 N.E.3d 1192 (Ill. 2021); *State v. Andrews*, 227 Md. App. 350 (Md. Ct. Spec. App. 2016); *King v. State*, 425 Md. 550 (Md. Ct. Spec. App. 2012), *rev'd, Maryland v. King*, 569 U.S. 435 (2013).

INTRODUCTION

The U.S. Supreme Court has issued strong and clear admonitions that intimate, sensitive, and voluminous electronic data stored on personal devices and with communication service providers deserves *more* constitutional protection than physical papers and effects. *Riley v. California*, 573 U.S. 373, 403 (2014) (data

stored on cell phone); *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (mobile phone location data). And yet, in this case, the State urges this Court to create a special rule that would *diminish* Fourth Amendment protections for electronically stored information. This Court should refuse to do so.

Here, the State argues that when people agree to permit law enforcement to make a copy of their private data, the government may search that copy without limitation, regardless of the person's expectation of privacy in the original data or any limitations that were conditions of their consent. The Court of Appeals properly rejected that extreme argument.

Copying takes place in almost every forensic analysis of electronic data. Therefore, constitutional rules about ownership of and privacy expectations in copies are rules about constitutional protections for data generally. If law enforcement is constrained by the Fourth Amendment in how it may search computer data—and it is—it must also be constrained in how it searches copies of computer data. And if people are entitled to withdraw consent for electronic searches—and they are—they must also be entitled to withdraw consent for searches of copies of their data. Any other conclusion would deny individuals full protection of their right to be free from unjustified, plenary government searches of our most private and constitutionally protected conversations, papers, and effects.

This Court should not adopt the State's view, which radically and dangerously departs from longstanding Fourth Amendment precedent. The Court should instead affirm the Court of Appeals' decision.

ARGUMENT

I. SEARCHES OF DATA ON ELECTRONIC DEVICES, INCLUDING COPIES OF THAT DATA, CAN REVEAL EXTRAORDINARILY PRIVATE INFORMATION.

In *Riley v. California*, the U.S. Supreme Court affirmed that modern cell phones—and by extension other repositories of electronic data such as laptops and social media accounts—implicate privacy concerns far beyond those implicated by the search of physical items. 573 U.S. at 403. The Court observed that cell phones are uniquely private objects because they "collect[ ] in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record." *Id.* at 394. The same is true of today's laptops—which often contain complete backups of a user's cell phone.[1] Searches of computers will typically expose to the government far more than the most exhaustive search of a house: "A [digital device] not only contains in digital

[1] *See, e.g.*, Apple Inc., *Back Up Your iPhone, iPad, or iPod Touch in iTunes on PC*, https://support.apple.com/guide/itunes/back-up-your-iphone-ipad-or-ipod-touch-itns3280/windows.

form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form." *Id.* at 396–97.

These insights are even truer today than they were in 2014. When the Supreme Court decided *Riley*, the top-selling cell phone could store between sixteen to sixty-four gigabytes of data. *Id*. at 394. Today, new phones can hold as much as a terabyte of data,[2] while laptops ship with at least thirty-two gigabytes and as much as eight terabytes (8,000 gigabytes) of hard drive storage capacity.[3] One terabyte is the equivalent of more than 83.3 million pages of text.[4] Storage capacities continue to increase every year, as does the sheer volume of personal data stored on—and accessible from—laptop computers and cell phones.

Moreover, today's forensic tools enable law enforcement to glean insights about a device owner's "privacies of life" far beyond those available through a

---

[2] *See, e.g.*, Apple Inc., *iPhone 14 Pro*, https://www.apple.com/iphone-14-pro/specs.

[3] *See, e.g.*, Dell Techs., *Laptop Computers & 2-in-1 PCs*, https://www.dell.com/en-us/shop/dell-laptops/sr/laptops/windows-10-pro-with-windows-11-pro-license; Lenovo, *Find the Laptop to Fit Your Lifestyle*, https://www.lenovo.com/us/en/laptops/results; Apple Inc., *Which Mac Is Right for You?*, https://www.apple.com/mac. *See also* Scott Gilbertson, *How to Choose the Right Laptop: A Step-by-Step Guide*, Wired (Jan. 21, 2023), https://www.wired.com/story/how-to-buy-the-right-laptop-for-you/#storage (recommending a "minimum amount of [storage] space" of 256 gigabytes).

[4] *How Many Files Can I Store?*, Univ. of Alaska Anchorage (July 13, 2022), https://service.alaska.edu/TDClient/36/Portal/KB/ArticleDet?ID=95#:~:text=A%20Terabyte%20(TB)%20is%20equal,83.3%20million%20pages%20of%20text.

manual review. *Riley*, 573 U.S. at 403. Forensic tools extract data such as the owner's contacts, call logs, text conversations, photos, videos, saved passwords, GPS location records, usage records, online account information, deleted material, and app data.[5] While the Upturn report is specifically about cell phones, its insights are generally true about searches of laptops as well.

Data analysis tools can aggregate data from different applications and sort it by file type, or the time and date of creation, enabling police to view the data in ways the device user cannot, and to gain insights that would be impossible to gather through a manual review. Upturn Report at 12, 15. Police can use forensic tools' data-sorting capability to make sense of reams of data and tell a particular story about a person. People who give police permission to look at their electronic devices would be astounded by what the officers can learn about them from the data stored there.

In an investigation involving digital data, law enforcement starts by making a copy of a device's contents. A forensic examiner needs to be able to examine the data without modifying the original, as the State may need to prove that its investigative techniques did not damage, destroy, or contaminate evidence. Working

[5] Upturn, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 10, 16 (Oct. 2020), https://perma.cc/7DCK-PGMQ (hereinafter "Upturn Report"). Upturn is a 501(c)(3) organization that works in partnership with many of the nation's leading civil rights and public interest organizations to promote equity and justice in the design, governance, and use of digital technology.

from a copy helps to ensure that examined media will not be altered and that a forensic examiner will be able to authenticate any evidence.[6]

When law enforcement makes a bit-for-bit copy, the data must be restructured into files for investigators to make sense of it. Upturn Report at 15. Then, investigators extract, organize, search for, and review data contained in that copy. A forensic examiner searches the data, using both keywords and more advanced techniques such as face recognition, data visualization, and a technique known as "fuzzy matching," where the forensic analysis software makes predictions about what data is responsive to the search queries. *Id*. at 24. In sum, government searches that start with bit-for-bit copies do not reveal the contents of a device to law enforcement personnel absent further steps such as restructuring, extracting, and querying.

II. CONSENT-BASED SEARCHES, ESPECIALLY OF ELECTRONIC DATA, MAY EXTEND NO FURTHER THAN THE OWNER'S EXPLICIT PERMISSION—AND ONCE CONSENT IS WITHDRAWN, ALL SEARCHES PREMISED ON THAT CONSENT MUST STOP.

It is well-established that consent-based searches can only go as far as the

[6] U.S. Dep't of Just., Nat'l Insts. of Just., *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* 1 (Apr. 2004), https://www.ojp.gov/pdffiles1/nij/199408.pdf ("Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination. Examination is best conducted on a *copy* of the *original evidence*.").

scope of consent given. That is because the only source of authority to search a private space through consent is the terms of the consent itself. It follows that when the owner withdraws consent, any future searches and seizures need a new legal basis, and therefore require a warrant or some other justification compatible with the Fourth Amendment. When the defendant in this case revoked his permission to search his laptop, these officers' legal basis for examining his data ceased, and there were no other grounds for searching his data. At that point, law enforcement should have halted the search process immediately.

Warrantless searches are "per se unreasonable under the Fourth Amendment" unless they fall within one of the "few specifically established and well-delineated exceptions" to the warrant requirement. *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)); *see also Pacheco v. State*, 465 Md. 311, 321 (2019). Once the government invokes an exception to the warrant requirement, courts must ensure that its application is "limited in scope to that which is justified by the particular purposes served by the exception." *Florida v. Royer*, 460 U.S. 491, 500 (1983); *accord Collins v. Virginia*, 138 S. Ct. 1663, 1671–72 (2018) (a warrantless search must not be "untether[ed] . . . from the justifications underlying it" (cleaned up)).

Consent is one such exception to the warrant requirement. *Schneckloth v. Bustamonte*, 412 U.S. 218, 222 (1973). Consent must be freely and voluntarily given

for the search to be lawful. *Id.* And consent searches must be limited by the scope of the permission granted. *Florida v. Jimeno*, 500 U.S. 248, 252 (1991); *Walter v. United States*, 447 U.S. 649, 656 (1980) (consent searches are "limited by the terms of [their] authorization."). If police act outside the scope of consent, full Fourth Amendment protections apply to that conduct. *United States v. McFarley*, 991 F.2d 1188, 1191 (4th Cir. 1993); *State v. Green*, 375 Md. 595, 624 (2003) (approving search because "consent was not revoked nor did it expire").

If a person withdraws consent, the search must stop. *United States v. Lattimore*, 87 F.3d 647, 651 (4th Cir. 1996) (*en banc*) ("A consent to search is not irrevocable, and thus if a person effectively revokes . . . consent prior to the time the search is completed, then the police may not thereafter search in reliance upon the earlier consent." (citing 3 Wayne R. LaFave, *Search and Seizure* § 8.2(f), at 674 (3d ed. 1996) (alteration in original)). To search beyond the bounds of consent, an officer needs to ask for additional consent, get a warrant, or properly rely on another exception to the warrant requirement. *See McFarley*, 991 F.2d at 1191 ("[O]nce consent is withdrawn or its limits exceeded, the conduct of the officials must be measured against the Fourth Amendment principles."); *United States v. Assante*, 979 F. Supp. 2d 756, 762 (W.D. Ky. 2013) ("[U]pon revocation [of consent to a warrantless search], a previously valid consensual search should be terminated instantly and the officers should promptly depart the premises assuming they possess

no independent legal authority to remain." (cleaned up)). This requirement helps avoid the indiscriminate searches and seizures that were the "immediate evils," *Payton v. New York*, 445 U.S. 573, 583 (1980), motivating adoption of the Fourth Amendment. *Assante*, 979 F. Supp. 2d at 762.

Importantly, a person can withdraw consent to search at any time. *United States v. McWeeney*, 454 F.3d 1030, 1035 (9th Cir. 2006) (describing ability to withdraw consent as a "constitutional right"); *Jones v. State*, 343 Md. 448, 465 (1996) (search in progress of defendant's pockets should have stopped when he withdrew consent). There is no such thing as an irrevocable consent that permits government searches of private data in perpetuity. *Mason v. Pulliam*, 557 F.2d 426, 429 (5th Cir. 1977) (consent-based search was "implicitly limited by [the defendant's] right to withdraw his consent and reinvoke his Fourth Amendment rights").

Careful judicial enforcement of the limits of consent searches is critical because such searches present heightened risk of abuse as compared to searches conducted with a warrant—particularly in the digital context. They often are conducted without probable cause or even a lesser level of suspicion, based only on a person's decision to comply with a police investigation. There is no warrant or other written guidance about how officers should conduct the search in accordance with the scope of consent—no judge is involved at the time of execution. Unlike

warrants, there is no point at which officers must report back to a judicial officer of the scope of their (authorized) invasion into individual privacy or property rights. Md. Rule 4-601(f) ("[a]n officer who executes a search warrant shall prepare a detailed search warrant return"). Therefore, often, the officers' description of the purported agreement defining the scope of consent is the only limitation on the searches and seizures courts allow law enforcement officials to do.[7]

III. SEARCHING A COPY OF A PERSON'S DATA INVADES THEIR EXPECTATION OF PRIVACY IN THE SAME WAY THAT SEARCHING THE ORIGINAL DATA DOES.

If one loses a reasonable expectation of privacy in their data merely because it is a copy, then it is not clear that the Constitution would ever protect this information from arbitrary and limitless government searches. Instead, even when

[7] Scholars and practitioners have long criticized the consent exception to the Fourth Amendment's warrant requirement on policy grounds, often referencing the inherently coercive nature of law enforcement "requests." *See, e.g.*, Marcy Strauss, *Reconstructing Consent*, 92 J. Crim. L. & Criminology 211, 236 (2002) ("most people would not feel free to deny a request by a police officer"); Janice Nadler, *No Need to Shout: Bus Sweeps and the Psychology of Coercion*, 2002 Sup. Ct. Rev. 153, 156 (2002) ("the fiction of consent in Fourth Amendment jurisprudence has led to suspicionless searches of many thousands of innocent citizens who 'consent' to searches under coercive circumstances"). Many have also observed that coercion is particularly present for people of color, and especially Black Americans, who may fear physical harm if they decline a request from a law enforcement officer. *See, e.g.*, Devon W. Carbado, *(E)Racing the Fourth Amendment*, 100 Mich. L. Rev. 946, 971, 972 & n.121, 973 (2002); *United States v. Washington*, 490 F.3d 765, 773–74 (9th Cir. 2007) (finding lack of consent after two incidents where white police officers shot African-Americans during traffic stops).

people lose control over their property, they do not lose their reasonable expectation of privacy in the contents of that property. *See Warden v. Hayden*, 387 U.S. 294, 304 (1967) (searches may violate the Fourth Amendment even if the Government has a superior property interest because the principal object of the Fourth Amendment is protection of privacy). Searches and seizures are different beasts. *See Horton v. California*, 496 U.S. 128, 133 (1990) ("The right to security in person and property protected by the Fourth Amendment may be invaded in quite different ways by searches and seizures."). "Even when government agents may lawfully seize [ ] a package to prevent loss or destruction of suspected contraband, the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package." *United States v. Jacobsen*, 466 U.S. 109, 114 (1984) (footnote omitted). So too, when police lawfully possess someone's laptop or cell phone, they do not necessarily have lawful access to the data stored there. In *Riley*, the Supreme Court made clear that police can be barred from searching information contained in a cell phone even when they have the legal authority to possess the device. 573 U.S. at 403. In so holding, the Court recognized that the defendant's privacy and possessory interests in the data stored in a phone were separate from—and more extensive than—his interests in the physical phone itself. *Id.* at 393. Moreover, the fact that the police had physical possession of the phone did not diminish the defendant's expectation of privacy in the information stored on the device. *See, e.g.*,

Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 703 (2010) (explaining that an individual's "possessory interest extends to both the original and any copies made from it" and that the owner's possessory interest is in "the data").

Courts recognize an ongoing expectation of privacy in lawfully obtained copies of data by routinely holding that searches of such data that fall outside the scope of legal permission are unconstitutional. For example, in *People v. Hughes*, the Michigan Supreme Court held that police could not search a copy of the defendant's cell phone data for evidence of a second crime not identified in the warrant. That is because the seizure and search of cell-phone data does not extinguish the otherwise reasonable expectation of privacy in the entirety of the seized data. 958 N.W.2d 98, 111 (Mich. 2020); *see also United States v. Nasher-Alneam*, 399 F. Supp. 3d 579, 593 (S.D. W.Va. 2019) (rejecting government assertion that when electronic records are lawfully seized and imaged "there's no problem and no limitation to go back and look at them later"); *United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. 1999) (search of a copy of defendant's data outside the scope of the warrant was an "unconstitutional general search" which violated the suspect's expectation of privacy).

IV. IN THIS CASE, ONCE THE DEFENDANT WITHDREW HIS CONSENT, THE STATE COULD NO LONGER SEARCH HIS DATA OR A COPY OF HIS DATA ON THE BASIS OF THAT WITHDRAWN CONSENT.

Searches conducted pursuant to consent must stop when that consent is withdrawn, even if those searches are taking place—as they almost always will be—on copies of data. Otherwise, the State can readily evade longstanding constitutional limitations on government authority to search private conversations, papers, and effects by promptly making copies of electronic data.

The thrust of the State's argument is that once the defendant consented to the search of his laptop, the copied data became "government property." State Br. 59. But when the government invades a person's expectation of privacy by that person's consent, its authority to search is limited by the scope of that consent. And government searches of copies of a person's data implicate the same expectation of privacy as searches of original data. Accordingly, if the defendant could have withdrawn his consent to search the *original* data—and he could—he could also withdraw his consent to search the *copied* data—which he did. The State's novel assertion that making a copy frees it from complying with the Fourth Amendment is unprincipled.

When the defendant in this case revoked his consent to search, the search process should have stopped. Since the government had not yet queried or seen his laptop data, it could no longer rely on his withdrawn consent to do so. The defendant

did not *need* to explicitly reserve his right to withdraw his consent for that withdrawal to be effective. *Illinois v. Rodriguez*, 497 U.S. 177, 183–89 (1990) (explaining that scope of consent is a "reasonableness"-based inquiry). But, it's worth noting, he actually *did*. As the form he signed stated: "I understand that I may withdraw my consent at any time." State App. 003.

To support its position, the State relies on three cases from the 1970s that generally say that the government can keep photocopies of business records that were disclosed to the Internal Revenue Service as part of tax investigations, so long as the copies were made before the document owner withdrew consent. The State argues that this means people lose their privacy interest in copies of their personal hard drives that were made before they withdraw consent. But the State's cases are outdated, and the State's argument fails to grapple with the fact that the privacy interests in a few boxes of tax-related business documents pale in comparison to the gigabytes of personal emails, address books, text conversations, photos, videos, location data, and more that are stored on hard drives. *See supra* Section I.

In one of the State's cases, *United States v. Ponder*, 444 F.2d 816 (5th Cir. 1971), a taxpayer responded to a civil audit by the Internal Revenue Service by sending business and financial records to the agency. *Id.* at 818. The taxpayer then requested the return of those records. *Id.* Rather than premising his reversal of consent on his Fourth Amendment rights and his reasonable expectation of privacy

in the records, the taxpayer indicated that he "needed the records for business reasons" and "placed no restriction on the use of the records by the government" at all. 444 F.2d at 820. The agency either continued to copy the records, or sent previously photocopied records, to its criminal division, which began an investigation into the taxpayer's filing of false tax returns. *Id.* at 818, n.4. The taxpayer argued that retaining a photocopy of his documents after he asked for them back was an illegal search and seizure under the Fourth Amendment, but the court rejected the argument. *Id.* at 820.

Ponder is likely no longer good law, if it ever was. *Ponder* rests on two cases, *McGarry v. Riley*, 363 F.2d 421 (1st Cir. 1966) and *Boren v. Tucker*, 239 F.2d 767 (9th Cir. 1956). *Ponder*, 444 F.2d at 818–19. Those cases were decided before *Katz*, 389 U.S. 347, which undermined their holdings, and thus also *Ponder*, by establishing the "reasonable expectation of privacy" test for Fourth Amendment rights. It is that constitutional standard, and not the law in 1956 or 1966, that applies to government searches of data copies today. It is telling that the State must reach back to authorities decided before *Katz*—the foundation of the Fourth Amendment law of searches for over 50 years—for support for its outlandish position.

Just a few years after it decided *Ponder*, the Fifth Circuit implicitly limited it in *Mason*, 557 F.2d 426. There, without a connection to a subpoena, a taxpayer gave consent to an IRS agent to examine personal records, and withdrew that consent a

week later through his attorney. *Id.* at 429. The Fifth Circuit held that the revocation of consent was binding on the IRS, and affirmed the district court's order to return the records and any copies—though it did permit the IRS to retain the copies the agency had made prior to the withdrawal of consent. *Id.* Notably, the IRS made an argument strikingly similar to the State's in this case: "that when [the taxpayer] voluntarily permitted [an IRS agent] to take possession of his papers for the purpose of examining and copying, he forever waived his Fourth Amendment rights and any underlying reasonable expectations of privacy." *Id.* at 428. But the court rejected this broad proposition. *Id.*[8]

The third case the State relies on is *United States v. Ward*, 576 F.2d 243 (9th Cir. 1978). *Ward* explicitly questions whether *Ponder* is still good law in light of the *Mason* decision. *Id.* at 244. *Ward* also limited *Ponder* to its facts, noting that the records taken in *Ponder* were produced pursuant to an administrative summons, whereas this was not the case in *Mason* (or here), and that the *Ponder* court limited its holding to a situation where the demand for return of the records was not grounded in a claim for protection of constitutional rights (unlike here). *Id.*; *see Linn v. Chivatero*, 714 F.2d 1278, 1288–89 (5th Cir. 1983) (Clark, C.J., concurring)

[8] As the Ninth Circuit has observed, "the *Mason* decision casts considerable doubt on continued reliance on *Ponder*." *United States v. Ward*, 576 F.2d 243, 244 (9th Cir. 1978); *see Vaughn v. Baldwin*, 950 F.2d 331, 333 (6th Cir. 1991) (similar).

(explaining that in *Ponder* the court "expressly refused to consider what that taxpayer's position would have been had he demanded the return of his records for the declared purpose of protecting his constitutional rights"). Like *Mason*, *Ward* allowed the IRS to use any evidence gathered or copies made before the taxpayer withdrew his consent. *Id.* at 244–45.

So, the State cites no good caselaw in which the government was allowed to commence review of any kind of copies after consent to search an original was withdrawn. The State implies that the IRS had not yet reviewed the contents of the taxpayers' documents and *Ponder*, *Mason*, and *Ward* allowed the agency to start to do so after the taxpayers withdrew their consent. This assumption is unsupported. Whether or not the government had reviewed the documents was not raised in any of the three opinions. The courts may have assumed that making paper copies of a taxpayer's business records is closely connected to seeing the contents of those documents. In contrast, understanding the contents of a copy of a hard drive requires restructuring, extracting, querying, and reviewing the results. The State claims that making photocopies does not necessarily reveal the content of those documents, because "an investigating officer can load paper into a document feeder without reviewing the contents of individual documents". State Br. 28. This is much like "saying a ride on horseback is materially indistinguishable from a flight to the moon.

Both are ways of getting from point A to point B, but little else justifies lumping them together." *Riley*, 573 U.S. at 393.

The State also relies on *Varriale v. State* for the proposition that a failure to expressly limit a search at the time consent is provided constitutes a waiver of any future privacy interest. State Br. 42–43, 57 (citing *Varriale*, 444 Md. 400, 419 (2015)). But *Varriale* is inapposite. First, the defendant there did not withdraw his consent prior to the State's testing his DNA. 444 Md. at 413–14. Second, while the Court did hold there was no expectation of privacy implicated by the government's use of the DNA, it did not do so based on the law of consent. Rather, it based its holding on the U.S. Supreme Court's contemporaneously-recent decision in *Maryland v. King*, which held there was no expectation of privacy in use of limited DNA testing post-arrest, to serve the government's heightened interest in conducting searches designed to identify and process arrestees. *King*, 569 U.S. 435, 449 (2013); *Varriale*, 444 Md. at 442 (Harrell, J. dissenting) (citing *King*, 569 U.S. 435). That situation is quite distinct from the government conduct at issue here. *Varriale* has nothing to say about post-withdrawal government investigations that normally *do* constitute searches.

V. PERNICIOUS CONSEQUENCES FLOW FROM THE STATE'S PROPOSED RULE.

The State's rule would give the government powers far beyond those the drafters of the Fourth Amendment intended. The State could obtain consent under

essentially false pretenses, telling device owners that they have the right to withdraw their consent at any time, quickly copy those devices in the squad car, and then conduct plenary and exploratory reviews of private data even after consent was withdrawn. Law enforcement could then rely on revoked consent to engage in hunch-based searches without limit. It arguably could conduct rummaging and overbroad searches even based on particularized warrants that appropriately limit searches of original data—because the State's position is that once it copies data, that copy becomes "government property" in which an individual has no expectation of privacy at all.

Importantly, accused defendants are not the only people who would be implicated by the State's rule. Witnesses, victims, and individuals cleared of suspicion—indeed, anyone who consented to a search of their digital device in the context of one investigation—could not prevent law enforcement from storing a copy of all their information in a database and "min[ing] [it] for information years into the future." *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). The rule would disincentivize cooperation with law enforcement. There are many who may want to share relevant evidence with law enforcement without losing control over *all* of their private information. Crime victims, for example, may consent to a limited search of their electronic devices for a specific purpose but wish to retain control over their data, because they do not want to share all their personal

information with the police, or to risk that it may fall into the hands of their assailant through discovery.

People should not lose their privacy rights in all their data as a price of assisting in the prosecution of crimes witnessed by or perpetrated against them. A strong expectation of privacy follows this data exactly *because* it was shared with trusted law enforcement officers in connection with an investigation of a criminal offense—and *not* "abandoned" or made publicly available. State Br. 41, 54, 60. The State's contention that "[n]o reasonable person would let the government search their digital information, then expect to retain a privacy interest in copies that the government made with their consent," State Br. 38, is hard to square with the valid and understandable privacy concerns that suspects, witnesses, victims, and other members of the public have when cooperating with police.

CONCLUSION

For the foregoing reasons, *amici curiae* respectfully urge this Court to affirm the decision of the Appellate Court.

Respectfully submitted,

David R. Rocah (MD Bar ID 0312050001)
ACLU of Maryland Foundation
3600 Clipper Mill Road,
Suite 350
Baltimore, MD 21211

Counsel for Amici Curiae

CERTIFICATE OF WORD COUNT AND COMPLIANCE WITH RULE 8-112

1. This brief contains 4,905 words, excluding the parts of the brief exempted from the word count by Rule 8-503.

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

/s/ David R. Rocah
David R. Rocah

CERTIFICATE OF SERVICE

I hereby certify that, pursuant to Rule 20-201(g), on May 5, 2023, the foregoing Brief of *Amici Curiae* in Support of Respondent was served via the MDEC File and Serve Module, and that, pursuant to Rule 8-502(c), two copies of each were mailed, postage prepaid, first-class, to:

ANDREW H. COSTINETT
Counsel of Record
Assistant Attorney General Attorney
ANTHONY G. BROWN
Attorney General of Maryland
Office of the Attorney General
Criminal Appeals Division
200 Saint Paul Place
Baltimore, Maryland 21202
(410) 576-6422
acostinett@oag.state.md.us

ZACHARY D. TRIPP, *pro hac vice*
JOSHUA M. WESNESKI, *pro hac vice*
Counsel of Record
WEIL, GOTSHAL & MANGES LLP
2001 M Street NW, Suite 600
Washington, DC 20036
(202) 682-7248
Joshua.Wesneski@weil.com

DANIEL M. LIFTON, *pro hac vice*
WEIL, GOTSHAL & MANGES LLP
767 Fifth Avenue
New York, NY 10153

J. DENNIS MURPHY, JR.
MURPHY & PRICE, LLP
5700 Coastal Highway
Suite 305
Ocean City, MD 21842

/s/ David R. Rocah
David R. Rocah