State of Maryland v. Daniel Ashley McDonnell, No. 36, September Term, 2022

CONSTITUTIONAL LAW – FOURTH AMENDMENT – SEARCHES AND SEIZURES – REASONABLE EXPECTATION OF PRIVACY – CONSENT – FORENSIC COPY OF DIGITAL DATA – Supreme Court of Maryland held that defendant had reasonable expectation of privacy in data stored on his laptop's hard drive, whether data was electronically stored on his hard drive or government's copy of hard drive made with defendant's consent. Defendant's reasonable expectation of privacy was not eliminated by government's copying of hard drive because no data was exposed prior to his withdrawal of consent. Supreme Court held that, under circumstances of defendant's consent, reasonable person would not think that government could examine data on copy after withdrawal of consent when no examination occurred prior to withdrawal. Government's examination of data after defendant withdrew consent was search, which was unreasonable because government lacked any authority to conduct search, by warrant or exception to warrant requirement.

Circuit Court for Anne Arundel County
Case No. C-02-CR-21-000487

Argued: June 2, 2023

IN THE SUPREME COURT

OF MARYLAND*

No. 36

September Term, 2022

STATE OF MARYLAND

v.

DANIEL ASHLEY MCDONNELL

Fader, C.J.
Watts
Hotten
Booth
Biran
Gould
Eaves,

JJ.

Opinion by Watts, J.

Filed: July 7, 2023

*At the November 8, 2022 general election, the voters of Maryland ratified a constitutional amendment changing the name of the Court of Appeals of Maryland to the Supreme Court of Maryland. The name change took effect on December 14, 2022.

In this case, we must determine what protection, if any, the Fourth Amendment provides to a person who voluntarily consents to the government seizing his laptop computer, creating an exact copy of its hard drive, and searching the data on it, but who, after the copy is made but before the government has examined the data, withdraws the consent. We must decide whether, for Fourth Amendment purposes, the consensual creation of a copy of the hard drive permanently eliminates the laptop owner's privacy interest in the data on the hard drive, *i.e.*, what impact the owner's withdrawal of consent has on the government's right to examine the data on the copy.

In this case, we conclude that Daniel Ashley McDonnell, Respondent, had a reasonable expectation of privacy in the data contained on his hard drive, whether the data was electronically stored on his laptop's hard drive or the government's computer via a copy of the hard drive. We hold that, because the government did not examine the data before he withdrew his consent, Mr. McDonnell did not lose his reasonable expectation of privacy in the data, and the examination of the data was a search. As such, we conclude that the government conducted an unreasonable search by examining the data without any authority to do so, by a warrant or an exception to the warrant requirement. We, therefore, affirm the judgment of the Appellate Court of Maryland[1] reversing the Circuit Court for Anne Arundel County's decision that examination of the data was not a search in violation of the Fourth Amendment.

[1]At the November 8, 2022 general election, the voters of Maryland ratified a constitutional amendment changing the name of the Court of Special Appeals of Maryland to the Appellate Court of Maryland. The name change took effect on December 14, 2022.

BACKGROUND

On June 1, 2019, agents of the United States Army Criminal Investigation Command ("USACIDC")[2] visited Mr. McDonnell's home for a "knock-and-talk" with him. Lacking a warrant, the agents asked for Mr. McDonnell's consent to search his home, phone, and computers as part of an investigation into his possession and distribution of child pornography. Mr. McDonnell declined. On July 12, 2019, however, Mr. McDonnell met with the agents and signed a written consent form, permitting the agents to search his home and seize electronic devices. With his signature on the consent form and initials next to each paragraph of the document, Mr. McDonnell indicated his understanding of and consent to the search of his home and the seizure and search of his electronic devices and media as follows:

> I have been informed of my right to refuse to consent to such a search. I hereby authorize the undersigned Special Agent, another Special Agent or other person designated by USACIDC, to conduct at any time a complete search of: . . . all digital media including cell[ ]phones, thum[b]drive[s], hard disk drives, laptops & any other media relevant to this investigation.
>
> * * *
>
> I understand that any contraband or evidence found on these devices may be used against me in a court of law.
>
> I relinquish any constitutional right to privacy in these electronic devices and any information stored on them. I authorize USACIDC to make and keep a copy of any information stored on these devices. I understand that any copy made by USACIDC will become the property of USACIDC and that I will

[2]In 2021, USACIDC was renamed the United States Army Criminal Investigation Division, or "CID." See U.S. Dep't of the Army Crim. Investigation Div., Our History, https://www.cid.army.mil/The-Agency/Our-Mission/ [https://perma.cc/7TGL-EWX4]. Because the events at issue occurred before the name change, we will refer to the agency as "USACIDC," as the parties do.

have no privacy or possessory interest in the copy.

> I give this written permission voluntarily. I have not been threatened, placed under duress, or promised anything in exchange for my consent. I have read this form or it has been read to me and I understand it. . . .
>
> I understand that I may withdraw my consent at any time.

(Some capitalization omitted).

After Mr. McDonnell signed the consent form, the agents entered his home and seized a number of electronics, including a Dell laptop computer. Shortly thereafter, at their offices, the agents imaged,[3] *i.e.*, copied, the laptop's hard drives,[4] between July 12 and July 16, 2019. On July 19, 2019, counsel for Mr. McDonnell sent an email to USACIDC withdrawing "any purported consent to the seizure of [Mr. McDonnell's]

[3]Imaging a computer's hard drive is the first of a two-step process in most forensic computer examinations: acquiring the data and analyzing it. See Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 547 (2005). Imaging a hard drive "duplicates every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original." Id. at 541 (footnote omitted). This creates a replica of the computer's data at the time of imaging that cannot be edited, but can be searched and analyzed. See id. at 540. The identical nature of this mirror-image (also called a bitstream) copy and the original drive is verified by a mathematical function called hashing. See id. at 541. Imaging is necessary because of the length of time that a forensic analysis requires, and the ease with which data on a computer can be inadvertently changed or lost. See id. at 540-41; Stephen Moccia, Bits, Bytes, and Constitutional Rights: Navigating Digital Data and the Fourth Amendment, 46 Fordham Urb. L.J. 162, 184-85 (2019).

[4]According to the Agent's Investigation Report dated July 16, 2019, two hard drives from the Dell laptop were "imaged." The agent who authored the report stated for each hard drive that "[t]he image was verified to be an exact, bit-for-bit-copy of the hard drive through a comparison of hash values with no errors." The image copies of Mr. McDonnell's hard drives were put onto a new hard drive and the new hard drive containing the copy of Mr. McDonnell's hard drives was submitted to the agency's evidence repository. In this opinion, we will refer to the hard drives imaged from Mr. McDonnell's laptop as the "laptop's hard drive" and the imaged copies as the "copy of the hard drive" or the "copy."

laptop, or examination of its contents" and requesting the laptop's return. On September 3, 2019, a Special Agent of the USACIDC's Digital Forensics and Research Branch authored a report concerning the results of a forensic examination of the data on the copy of Mr. McDonnell's hard drive, which the agent had conducted between August 5 and 20, 2019. The report noted that the evidence examined was a hard disk drive containing the forensic images of the Dell laptop's operating system hard disk drive and storage hard disk drive. The report stated that "no evidence of child pornography" was found but explained that "[a]n examination of the media revealed evidence of child pornography search terms in the internet browser history[.]"

Proceedings in the Circuit Court

On March 26, 2021, Mr. McDonnell was indicted in the circuit court on charges of possessing, promoting, and distributing child pornography. Thereafter, Mr. McDonnell filed an omnibus motion that included a request to suppress illegally seized evidence, and later filed a memorandum in which he asked the circuit court to suppress the evidence from the forensic examination of the copy of his laptop's hard drive.

On August 16, 2021, the circuit court held a hearing on Mr. McDonnell's motion to suppress. The relevant facts relating to the motion were not disputed. The State argued that "a valid consent to search carries with it the right to examine and photocopy" and that downloading and creating the "mirror image copy" of the hard drive of Mr. McDonnell's laptop was "essentially photocopying digitally." Continuing with that analogy, the State asserted that federal case law instructs that, once the originals of documents are returned, the government can lawfully retain photocopies and then examine them. Relying on our

holding in Varriale v. State, 444 Md. 400, 119 A.3d 824 (2015), the State argued that, in circumstances involving DNA, blood samples, or firearms, the government can analyze samples even after consent has been withdrawn. The State contended that "once something was outside of the possession of the defendant, [] there was no more reasonable expectation" of privacy in the item.

Mr. McDonnell's counsel asserted that the laptop was akin to the cell phone in Riley v. California, 573 U.S. 373 (2014), and, therefore, the agents needed authority both to seize it and then to examine its contents. Mr. McDonnell's counsel contended that the language of the consent form purported to waive his Fourth Amendment rights and permit copying of the laptop, but did not permit the examination of the data on the copy. Mr. McDonnell's counsel argued that applying this Court's holding in Varriale concerning the ability to test DNA samples in a case that did not involve the withdrawal of consent would be contrary to the holding of the Supreme Court of the United States in Riley. At the conclusion of the hearing, the circuit court indicated that within one week's time either party could submit research on whether defense counsel is authorized to withdraw consent. On August 30, 2021, the circuit court issued a one-page order denying Mr. McDonnell's motion to suppress.

On September 24, 2021, the circuit court conducted a plea proceeding at which Mr. McDonnell entered a plea of not guilty with an agreed statement of facts, reserving the

right to appeal the circuit court's denial of the motion to suppress.[5] The prosecutor advised the circuit court of agreed-upon facts, which we summarize as follows. Special Agents of USACIDC had identified an IP address[6] connected to a network that was sharing files depicting child pornography. The agents contacted Comcast to determine the IP address. The result of a subpoena revealed that the IP address that was associated with the uploaded pornography came back as Comcast subscriber Daniel McDonnell at an address in Severn, Maryland. Thereafter, on June 1, 2019, the agents conducted a knock-and-talk with Mr. McDonnell and subsequently on July 12, 2019, Mr. McDonnell met with the agents and signed the written consent form. The laptop computer was copied between July 12 and 16, 2019. On July 19, 2019, Mr. McDonnell's counsel sent an email withdrawing consent to search the laptop. Between August 5 and 20, 2019, the copy of Mr. McDonnell's hard drive was forensically analyzed. The forensic examination did not reveal images of child pornography; however, it did reveal that Mr. McDonnell had run "digital forensic deleting software" on June 7, 2019, a few days after the knock-and-talk. The examination also

[5]In Maryland, a defendant can plead not guilty, forgo a full trial, and proceed "on an agreed statement of facts or stipulated evidence to preserve appeal on a suppression issue." Bishop v. State, 417 Md. 1, 16, 7 A.3d 1074, 1083 (2010). "Under an agreed statement of facts[,] both the State and the defense agree as to the ultimate facts" and "the facts are not in dispute[.]" Taylor v. State, 388 Md. 385, 396, 879 A.2d 1074, 1081 (2005) (cleaned up). "The trier of fact is not called upon to determine the facts as the agreement is to the truth of the ultimate facts themselves. . . . To render judgment, the court simply applies the law to the facts agreed upon." Id. at 396-97, 879 A.2d at 1081 (cleaned up).

[6]"The term 'IP address' is derived from the phrase 'Internet protocol[,]' and means 'the numeric address of a computer on the Internet[.]'" State v. Sample, 468 Md. 560, 572 n.6, 228 A.3d 171, 179 n.6 (2020) (citing *IP Address*, Merriam-Webster, https://www.merriam-webster.com/dictionary/IP%20address [https://perma.cc/2C7G-TX4Q]) (alterations in original).

revealed that Mr. McDonnell had made recent searches with terms consistent with the search for child pornography. The State introduced into evidence Exhibits 1 through 6, which, among other things, included images that the parties agreed would in fact have constituted child pornography, and were related to Counts I, II, and III of the indictment.

The circuit court found Mr. McDonnell guilty of three counts of distribution of child pornography and sentenced him to ten years' incarceration on each of the three counts, consecutively, for a total of thirty years' incarceration, all suspended, and five years of supervised probation with the conditions that Mr. McDonnell register as a Tier II sex offender, have no unsupervised contact with minors, and allow authorities to monitor his computer and phone. Mr. McDonnell timely appealed.

Opinion of the Appellate Court of Maryland

On December 1, 2022, the Appellate Court of Maryland reversed the circuit court's judgment. See McDonnell v. State, 256 Md. App. 284, 297, 286 A.3d 113, 120 (2022). Relying on Riley, 573 U.S. 373, the Appellate Court concluded that, "because individuals have a legitimate expectation of privacy in the digital data within their computer," Mr. McDonnell's "revocation of his consent to examine data from his laptop computer precluded a forensic examination of the mirror-image copy of its hard drive without a warrant." McDonnell, 256 Md. App. at 296, 286 A.3d at 120. The Appellate Court did not accept the State's argument that Mr. McDonnell had no privacy interest in the copy of the hard drive. See id. at 295-96, 286 A.3d at 119-20.

The Appellate Court distinguished Varriale, 444 Md. 400, 119 A.3d 824, and Wallace v. State, 373 Md. 69, 816 A.2d 883 (2003), because, unlike the defendants in those

cases, Mr. McDonnell unequivocally revoked his consent, which "expressly limited or eliminated the examination of the data" and "reclaimed [his] reasonable expectation of privacy in the data." McDonnell, 256 Md. App. at 296, 286 A.3d at 120. The Appellate Court held that, because Mr. McDonnell revoked his consent before the data on the copy was examined, the government's examination of the data was precluded without a warrant. See id. at 296, 286 A.3d at 120. The Appellate Court relied on this Court's discussion in Richardson v. State, 481 Md. 423, 282 A.3d 98 (2022), regarding the "importance and sensitivity of digital information" and the need for courts to be vigilant in enforcing the requirements of the Fourth Amendment in the digital age, as support for its conclusion. McDonnell, 256 Md. App. at 296, 286 A.3d at 120. The Appellate Court emphasized the obligation of courts to not allow "subtler and more far-reaching means of invading privacy [that] have become available to the Government . . . [to] erode Fourth Amendment protections." McDonnell, 256 Md. App. at 296, 286 A.3d at 120 (quoting Carpenter v. United States, ___ U.S. ___, 138 S. Ct. 2206, 2223 (2018)) (internal quotation marks omitted).

Petition for a Writ of *Certiorari*

On January 19, 2023, the State petitioned for a writ of *certiorari*, raising the following two issues:

> 1. Did McDonnell lack any legitimate expectation of privacy in a mirror-image copy of his laptop hard drive that the government created with his consent, and as to which he expressly disclaimed any possessory or privacy interest before the copy was created?
>
> 2. Did the Appellate Court of Maryland err in holding that McDonnell's revocation of consent to examine the contents of his laptop

barred investigators from examining the mirror-image copy of his hard drive, when the post-withdrawal examination of the copy was not a search?

On March 2, 2023, we granted the petition. See State v. McDonnell, 483 Md. 263, 291 A.3d 776 (2023).

DISCUSSION[7]

A. The Parties' Contentions

The State contends that USACIDC's examination of the copy of the hard drive was not a search because Mr. McDonnell had consented to his laptop's seizure, search, and copying. According to the State, by consenting to the copying of his laptop's hard drive, Mr. McDonnell "retain[ed] no reasonable expectation of privacy in any copies the government create[d] within that consent." The State asserts that the lack of case law addressing "whether a defendant retains any reasonable expectation of privacy in copies of digital data created within the scope of consent" merits reliance on case law regarding photocopies of paper evidence for guidance. (Citation omitted). The State brings to our attention opinions from federal appellate courts, such as United States v. Ponder, 444 F.2d 816, 820 (5th Cir. 1971), and United States v. Ward, 576 F.2d 243, 244-45 (9th Cir. 1978), holding that a defendant's consent to search also signifies consent to copy and that the government can retain and examine copies of papers made before consent is withdrawn.

The State argues that courts in other jurisdictions have applied this approach and determined that a defendant has no reasonable expectation of privacy in a copy of digital

[7]We address the two questions raised in the petition for *certiorari* together because of the interrelation of the issues.

data made while consent was in effect. The State cites unreported decisions of federal District Courts that treated imaged copies of hard drives as photocopies of papers and determined that copying prior to revocation of consent allowed the ongoing use of the copies.[8] The State argues that, in two cases, United States v. Lutcza, 76 M.J. 698, 703 (A.F. Ct. Crim. App. 2017), and United States v. Campbell, 76 M.J. 644, 658 (A.F. Ct. Crim. App. 2017), the United States Air Force Court of Criminal Appeals has reached the conclusion that a defendant consenting to the initial copying allows examination of the copied hard drive after the defendant withdraws consent. The State also asserts that, in United States v. Thomas, 818 F.3d 1230, 1242 (11th Cir. 2016), the Eleventh Circuit affirmed the validity of consent to the copying of files from the defendant's computer with the use of a forensic tool and law enforcement's reliance on the copy where the copy was made before consent was withdrawn but the examination occurred afterward.

The State contends that, because a warrantless search under the consent exception is legitimate only within the scope of the consent, we should assess the scope of Mr. McDonnell's consent based on an objective standard of what a reasonable person would have understood the consent to include. According to the State, "[n]o reasonable person would let the government search their digital information, then expect to retain a privacy

[8]The State cites United States v. Megahed, No. 8:07-cr-342-T23-MAP, 2009 WL 722481 (M.D. Fla. Mar. 18, 2009) (unreported order); United States v. Thomas, No. 8:13-cr-462-T-33-TBM, 2014 U.S. Dist. LEXIS 33443 (M.D. Fla. Feb. 14, 2014) (unreported report and recommendation); United States v. Sharp, No. 1:14-cr-229-TCB, 2015 WL 4641537 (N.D. Ga. Aug. 4, 2015) (unreported order), contending that, under our precedent, although such citation "'ordinarily is not appropriate,'" it is permissible in the face of a lack of authority on the issue. (Quoting Clancy v. King, 405 Md. 541, 558 n.17, 954 A.2d 1092, 1102 n.17 (2008)).

interest in copies that the government made *with their consent*." (Emphasis in original). The State contends that, in this case, Mr. McDonnell lost any reasonable expectation of privacy when he signed a form consenting to the seizure, search, and copying of his laptop's hard drive, and disclaiming his possessory and privacy interests in the copy.

The State asserts that this Court's holding in Varriale, 444 Md. at 418-19, 423-24, 119 A.3d at 835, 838-39, supports its position because, in that case, we held that, by consenting to the use of his DNA in a rape investigation and any future criminal prosecution, without placing any constraints on its use, the defendant waived his expectation of privacy in the DNA sample with regard to the State's subsequent analysis that linked him to an unrelated crime. For the State, because Mr. McDonnell similarly did not limit his consent when he gave it, he lost any privacy interest he had in the data on his laptop's hard drive and the copy made while his consent remained in effect.

The State contends that the Appellate Court erred by concluding that Mr. McDonnell's withdrawal of consent after USACIDC copied his laptop's hard drive precluded subsequent examination of data on the copy. According to the State, Mr. McDonnell's withdrawal of consent after the copy was made did not change USACIDC's ability to examine the copy, as the copy was USACIDC's property. The State asserts that the language on the consent form indicating that Mr. McDonnell could withdraw his consent at any time is not applicable, because, according to the form, once the copy was made, Mr. McDonnell had no privacy interest in the data on the copy.

The State contends that the Appellate Court improperly applied the holding of the Supreme Court of the United States in Riley, which the State distinguishes as being focused

on the privacy interest implicated in a search of a cell phone's data and not answering the question of whether law enforcement's examination of a copy of digital data constitutes a search. The State asserts that Riley's emphasis on a person's privacy interest in the digital contents of a cell phone does not support the proposition that a person "always retains identical expectations of privacy in all copies of one's digital data."

The State acknowledges that there is another view, as expressed by law professor Orin Kerr, that "[c]ourts should apply identical rules regardless of whether the data analyzed is the original version or a government-generated copy." (Quoting Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 563 (2005)). The State acknowledges that the Supreme Court of Illinois determined that this was the appropriate approach in People v. McCavitt, 185 N.E.3d 1192, 1207 (Ill. 2021), where the Court observed that the defendant had an informal privacy interest in his personal data and that this privacy interest extended to an image copy. According to the State, in McCavitt, after a defendant had been acquitted in a criminal case, a law enforcement officer re-examined a copy of the defendant's computer that had been previously obtained pursuant to a search warrant and new charges were brought against the defendant. The State distinguishes McCavitt from this case, however, on the ground that, here, Mr. McDonnell consented to USACIDC copying the hard drive and, according to the State, treating it as USACIDC's own property, thereby affirmatively relinquishing his privacy interest in it.

In sum, the State asserts that, pursuant to the consent form signed by Mr. McDonnell, the copy of the hard drive was USACIDC's property and, therefore, Mr. McDonnell had no privacy interest in the data on it at any time. The State argues that the

forensic analysis of the copy was therefore not a search. The State contends that, under a reasonableness analysis, in signing the consent form, Mr. McDonnell disclaimed any privacy interest in the data on the copy of the hard drive.

Mr. McDonnell responds that he "had a reasonable expectation of privacy in his digitally-stored personal information[.]" (Cleaned up). Mr. McDonnell asserts that, under Riley, 573 U.S. at 386, 393-94, a search of such information must be independently justified apart from any legal seizure of the physical apparatus containing the information or data, because searches of a cell phone or computer "bear 'little resemblance' to searches of containers like bags, which are 'limited by physical realities'" or boundaries. Mr. McDonnell contends that the Supreme Court of the United States reinforced the distinction between a privacy interest in digital information and its physical storage apparatus in Carpenter, 138 S. Ct. at 2213, 2219-20, by holding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell site location information,]" collected and stored by a third party. According to Mr. McDonnell, recognizing this distinction, the Supreme Court therefore concluded that "the Government's acquisition of the cell[]site records is a search and seizure within the meaning of the Fourth Amendment." (Cleaned up).

Mr. McDonnell contends that, in Richardson, 481 Md. at 472, 282 A.2d at 126, this Court took the same approach by holding that an abandoned backpack could legitimately be searched without a warrant, but a warrant authorizing a search of information on a cell phone found therein did not satisfy the particularity requirement for search warrants. Mr. McDonnell argues that our holding in Richardson "necessarily recognizes an independent

expectation of privacy in information as distinguished from the digital media on which it is stored[.]" Mr. McDonnell asserts that, because he had a reasonable expectation of privacy in the information on his laptop, and because USACIDC did not examine the information before he withdrew his consent, the examination of the data thereafter was a search for which a warrant was required. Mr. McDonnell argues that the USACIDC agents' possession of the copy of his hard drive after he withdrew consent left them "in the same position as the officers in *Riley* and *Richardson*, who had lawfully seized the cell[ ]phones at issue but did not yet have authorization to search the information stored thereon."

Mr. McDonnell argues that forensic copies enjoy the same Fourth Amendment protections as originals and asserts that Katz v. United States, 389 U.S. 347, 352-53 (1967), and Walter v. United States, 447 U.S. 649, 652-54 (1980) (plurality opinion), stand for the proposition that, to have a reasonable expectation of privacy in a searched item, an individual need not have a possessory or property interest in the item. Mr. McDonnell contends that the Supreme Court applied this concept to the electronic and digital realm in United States v. Karo, 468 U.S. 705, 714-15 (1984), and Carpenter, 138 S. Ct. at 2219-20, by recognizing the defendants' privacy interests in their data or personal information despite their lack of a "property interest in the devices and media used to collect their personal information[.]" At bottom, Mr. McDonnell asserts, these cases instruct "that if an individual has a reasonable expectation of privacy in his personal information," the person "retains that expectation regardless of where that information is stored[,]" *i.e.*, the original hard drive or the copy of the hard drive.

For Mr. McDonnell, the act of copying, without accessing, the hard drive does not remove his privacy interest in the data on the hard drive. Mr. McDonnell contends that, in McCavitt, 185 N.E.3d at 1206, the Supreme Court of Illinois came to the same conclusion where a hard drive was copied pursuant to a search warrant. Mr. McDonnell asserts that this approach is consistent with the principle reflected in a number of cases, including Richardson, that the justification needed for seizing an electronic device is distinct from the justification needed to search its digital contents.

Mr. McDonnell contends that the State erroneously relies on opinions treating a copy of a hard drive like a copy of a piece of paper, because "[t]he U.S. Supreme Court has already rejected the false equivalency between physical documents and digital media." Mr. McDonnell asserts that, in Riley, 573 U.S. at 393, the Supreme Court dispositively ruled out the idea that searches of a cell phone's digital contents and physical containers are "materially indistinguishable" because the breadth of information contained in a cell phone merits "privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." Mr. McDonnell points out that the Fourth Amendment's "touchstone" is reasonableness and argues that it is unreasonable "to categorically equate digital media with paper documents" due to the difference in sophistication between the two, particularly because "a forensic copy of a personal device gives insight into 'many distinct types of information' that can 'reveal much more in combination than any isolated record[,]' *Riley*, 573 U.S. at 394[,]" in a way that copies of paper documents do not.

Mr. McDonnell argues that, while his signing of the consent form made the seizure of his laptop reasonable under the Fourth Amendment and any search of it reasonable while

his consent was effective, by withdrawing his consent, he preserved a reasonable expectation of privacy in his unexamined digital data. Mr. McDonnell contends that consent can be withdrawn at any time and "does not extinguish the individual's reasonable expectation of privacy[.]" Mr. McDonnell argues that his revocation of consent nullified the consent provided to USACIDC, including the disclaimer in the consent form of any "privacy or possessory interest in the copy" of his laptop. Mr. McDonnell maintains that accepting the State's contention otherwise would allow consent to become permanent when framed as a "disclaimer" and that this would contravene the principle that consent can be withdrawn at any time. Mr. McDonnell points out that the consent form itself in this case instructed that he could withdraw his consent "at any time." In addition, Mr. McDonnell contends that this Court's holding in Varriale is not dispositive because it did not involve a withdrawal of consent.

B. Standard of Review

"The validity of a suppression ruling is a mixed question of law and fact." Richardson, 481 Md. at 444, 282 A.3d at 110 (citation omitted). We consider only the record from the suppression hearing, which we assess in the light most favorable to the prevailing party, and we accept the trial court's factual findings absent clear error. See id. at 444-45, 282 A.3d at 110. However, when assessing the constitutionality of a search or seizure, we conduct "an independent constitutional evaluation . . . applying the law to the facts found in each particular case." Id. at 445, 282 A.3d at 110 (cleaned up). We review *de novo* any legal conclusions about the constitutionality of a search or seizure. See id. at 445, 282 A.3d at 110.

C. Fourth Amendment Protections

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. The Fourth Amendment[9] does not prohibit all searches and seizures, just unreasonable ones. See United States v. Sharpe, 470 U.S. 675, 682 (1985). "A search compromises the individual interest in privacy; a seizure deprives the individual of dominion over his or her person or property." Horton v. California, 496 U.S. 128, 133 (1990) (citation omitted). "The touchstone of the Fourth Amendment is reasonableness." Florida v. Jimeno, 500 U.S. 248, 250 (1991).

Two tests can determine whether government action constitutes a search that implicates the Fourth Amendment. The first approach, set forth in Katz, 389 U.S. at 351, focuses on "people, not places[.]" Under this test, "[w]hen an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable, . . . official intrusion into that private sphere generally qualifies as a search[.]" Carpenter, 138 S. Ct. at 2213 (cleaned up). The burden is on the defendant asserting Fourth Amendment protection to "demonstrate that a government actor infringed

[9]The Fourth Amendment is applicable to the States through the Fourteenth Amendment. See Varriale, 444 Md. at 411, 119 A.3d at 831. Additionally, we interpret Article 26 of the Maryland Declaration of Rights *in pari materia* with the Fourth Amendment, such that it provides the same protections. See King v. State, 434 Md. 472, 482, 76 A.3d 1035, 1041 (2013).

upon his or her actual, subjective expectation of privacy in an item or place searched and that the expectation of privacy is one that society is prepared to recognize as reasonable." In re Russell, 464 Md. 390, 406, 211 A.3d 426, 435 (2019) (cleaned up). The second prong of this test requires that the defendant show an objectively reasonable expectation of privacy, "either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society[.]" Williamson v. State, 413 Md. 521, 535, 993 A.2d 626, 634 (2010) (cleaned up).

Next, because the amendment's text "reflects its close connection to property," historically, "the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates." Jones, 565 U.S. at 405-06 (footnote omitted). This property-focused approach related to "common-law trespass[.]" Carpenter, 138 S. Ct. at 2213 (cleaned up). Under this test, government action that causes "physical intrusion" on "private property" constitutes a search, such as attaching a GPS device to a person's car. Jones, 565 U.S. at 404-05.

Generally, there is no bright-line rule for determining the reasonableness of a search. See Ohio v. Robinette, 519 U.S. 33, 39 (1996). Instead, courts apply a totality of the circumstances analysis, based on the unique facts and circumstances of each case. See Missouri v. McNeely, 569 U.S. 141, 150 (2013). The nature of the intrusion, whether severe or "negligible[,] is of central relevance to determining reasonableness[.]" Maryland v. King, 569 U.S. 435, 446 (2013); see also Riley, 573 U.S. at 396 (quoting Judge Learned Hand's observation in United States v. Kirschenblatt, 16 F.2d 202, 203 (2d Cir. 1926), "that it is 'a totally different thing to search a man's pockets and use against him what they

contain, from ransacking his house for everything which may incriminate him'"); Richardson, 481 Md. at 453, 282 A.3d at 115 ("Without understating the problem posed by a general warrant to search someone's home prior to the digital age, a general warrant to search a computer or a smartphone today magnifies that problem exponentially."). Another consideration is whether any facts reduced or heightened the defendant's expectation of privacy. See King, 569 U.S. at 462 (discussing a person's diminished expectation of privacy as a student at school, an employee on the job, or a person in custody of law enforcement). An additional factor is the governmental interest or need that allegedly justifies the intrusion. See McNeely, 569 U.S. at 152 (concluding that a warrantless blood-alcohol test is unreasonable when the facts show that "police officers can reasonably obtain a warrant before a blood sample can be drawn without significantly undermining the efficacy of the search").

The contours of the privacy protected by the Fourth Amendment are "informed by historical understandings" at the time of its adoption regarding what constituted unreasonable searches or seizures. Carpenter, 138 S. Ct. at 2213-14. The "basic guideposts" for such an analysis, as described by the Supreme Court of the United States, include the amendment's goals of guarding "the privacies of life against arbitrary power" and "plac[ing] obstacles in the way of a too permeating police surveillance." Id. at 2214 (cleaned up). The Supreme Court has "kept this attention to Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools." Id. "As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," courts should seek to preserve the "degree of privacy

against government that existed when the Fourth Amendment was adopted." Id. (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)) (internal quotation marks omitted). The Supreme Court has been particularly concerned with "th[e] power of technology to shrink the realm of guaranteed privacy." Kyllo, 533 U.S. at 34.

1. Consent

A search conducted without a warrant is presumed to be unreasonable, but a warrantless search can still be reasonable, such as when "conducted pursuant to valid consent[.]" Jones v. State, 407 Md. 33, 51, 962 A.2d 393, 403 (2008) (citations omitted). The consent must be voluntary, see Robinette, 519 U.S. at 40, and the search must remain within the scope of the consent, see Jimeno, 500 U.S. at 252. Courts examine the scope of consent objectively: "what would the typical reasonable person have understood by the exchange between the officer and the suspect?" Id. at 251 (citations omitted). "The scope of a search is generally defined by its expressed object." Id. (citing United States v. Ross, 456 U.S. 798 (1982)). One who gives consent for the search of a particular area or items may subsequently narrow the scope of the consent given or withdraw consent entirely. See, e.g., State v. Reum, 313 P.3d 1156, 1164 (Wash. 2013) (*en banc*) ("A person consenting to a search has the right to restrict or revoke that consent at any time." (Citations omitted)). If consent is withdrawn, thereafter, the government must have other justification to make the search reasonable. See, e.g., United States v. Williams, 898 F.3d 323, 330 (3d Cir. 2018). That is, if the person withdraws consent before "the search is completed, then the police may not thereafter search in reliance upon the earlier consent." United States v. Lattimore, 87 F.3d 647, 651 (4th Cir. 1996) (*en banc*) (citations omitted). In the context

of the taking, testing, and matching of a DNA sample, this Court has held that consent that is neither limited beforehand nor withdrawn permits the government to use the sample consistent with the reasonable understanding of the consent, including in unrelated investigations. See Varriale, 444 Md. at 423-25, 119 A.3d at 838-39.

In Varriale, id. at 425, 119 A.3d at 839, this Court held that, under the circumstances of the case, "the Fourth Amendment [did] not preclude the police from retaining and using a suspect's DNA profile created from a DNA sample lawfully obtained by consent." Varriale consented to provide samples for DNA testing in relation to an investigation into a rape. See id. at 404-05, 119 A.3d at 827. After the testing ruled Varriale out as a suspect in the rape, the police uploaded his DNA profile to county and State databanks and compared it to "unidentified DNA profiles developed from crime scene evidence" in other unsolved cases, leading to a match to a profile associated with a burglary. Id. at 406, 119 A.3d at 827-28. When Varriale was prosecuted for that crime, he challenged the use of his DNA as an unauthorized search, but it was not suppressed. See id. at 403-04, 119 A.3d at 826.

This Court concluded that the database search was not beyond the scope of Varriale's consent, because there was no express limitation on his consent, and it was objectively reasonable for the police to retain and compare his DNA profile against the cold case evidence. See id. at 418-19, 119 A.3d at 835. We determined "that DNA profiles are like fingerprints, which police routinely catalog and compare in the course of criminal investigations" and, therefore, when police validly have such an identifying profile in their possession, "[n]o further Fourth Amendment authorization is required" to indefinitely store

and reuse them to "identify criminals." Id. at 416, 119 A.3d at 833-34 (citations omitted). In other words, this Court held that, once police lawfully obtain a person's DNA sample during an investigation, the person no longer has any expectation of privacy in that sample. See id. at 423, 119 A.3d at 838.

2. Digital Information

The Supreme Court has recognized the important distinctions between digital media and the physical targets of searches, observing that smartphones, for example, have "immense storage capacity" and "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." Riley, 573 U.S. at 393-94. Searches of computers, cell phones, and the like can reveal the "sum of an individual's private life" and bear "little resemblance" to searches of containers like bags, which are "limited by physical realities." Id. at 386, 393-94. Data stored on electronic devices is both qualitatively and quantitatively different from physical analogues because a search of cell phone or computer data "would typically expose to the government far *more* than the most exhaustive search of a house[.]" See id. at 396 (emphasis in original). A device's hard drive "not only contains in digital 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—unless the [device] is." See id. at 396-97.

The remarkable ability of digital information in the modern age to permit "official intrusion" into an individual's "private sphere" requires "special solicitude" for this information. Carpenter, 138 S. Ct. at 2213, 2219. The unique nature and scope of digital

information warrants particular limits on the government's ability to access it, such as determining that cell site location information requires a warrant or other authorization despite it being collected and held by third parties, whereas in other contexts "the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections" because a person usually has no reasonable expectation of privacy in information shared with third parties. Id. at 2216, 2223.

Riley, 573 U.S. at 378, required the Supreme Court to resolve "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." The Supreme Court noted the pervasiveness of cell phones and the "vast quantities of personal information" they contain. Id. at 385-86. The Court concluded that the rationales justifying searches incident to arrest—officer safety and preventing evidence destruction—did not justify a search of digital data on an arrestee's cell phone. See id. at 386. Citing the quantity and quality of information stored on cell phones, the Court determined that the warrantless examination of the digital contents of a phone implicates greater privacy interests than a search of an arrestee. See id. at 386. Thus, the Court held that "a warrant is generally required" before "a search" of a cell phone's digital contents, even if the cell phone was lawfully "seized incident to arrest." Id. at 401.

In Richardson, 481 Md. at 434, 282 A.3d at 104, this Court reiterated "[t]he privacy concerns implicated by cell phone storage capacity and the pervasiveness of cell phones in daily life" and pointed out that these concerns "do not fade away when police obtain warrants to search cell phones." The defendant's abandonment of his backpack provided

justification for the warrantless search of it, but this Court explained that the government needed separate justification to search the contents of the cell phone found inside. See id. at 435-36, 282 A.3d at 105. We held that the search warrant at issue failed to comply with the particularity requirement of the Fourth Amendment because it lacked any limitations on the authority to search the contents of the phone. See id. at 472, 282 A.3d at 126. Because "[t]he particularity requirement is arguably of even greater importance in the context of computers and smartphones than it is in the physical world," we concluded that it must be enforced to realize the "meaningful constraints" on government power required under Riley. Richardson, 481 Md. at 452, 282 A.3d at 114-15 (cleaned up).

To date, relatively few courts have grappled with the effect of governmental copying of a hard drive from a computer or cell phone on a person's privacy interest in the information stored therein. Some State high courts have rejected the argument that a defendant does "not have a legitimate expectation of privacy in" a copy of a hard drive from the defendant's computer because the defendant "did not create, own, or have lawful access to it." McCavitt, 185 N.E.3d at 1206 (citation omitted); see also People v. Hughes, 958 N.W.2d 98, 115 (Mich. 2020) (holding that search and extraction of data from a cell phone pursuant to a search warrant in a drug trafficking investigation did not permit law enforcement officers to later search the data for evidence of unrelated crimes without a warrant). In contrast, some trial and intermediate appellate courts in other jurisdictions have concluded that a copy of a computer hard drive is analogous to a photocopy of a paper document, which the government may freely examine so long as the copy was lawfully obtained. See, e.g., United States v. Megahed, No. 8:07-cr-342-T23-MAP, 2009 WL

722481, *3 (M.D. Fla. Mar. 18, 2009) (unreported order). These courts have relied on opinions like Ponder, 444 F.2d at 818-19, for the proposition that "a valid consent to search . . . carries with it the right to examine and photocopy" and that withdrawal of consent does not limit the government's ability to examine copies made prior to that withdrawal. See Megahed, 2009 WL 722481, at *3.

In McCavitt, 185 N.E.3d at 1198-99, the Illinois State Police seized the defendant's computer and created a copy of the hard drive under a warrant that the defendant did not challenge. The warrant permitted law enforcement to search for digital evidence of two unrelated crimes. See id. at 1196. The defendant was acquitted of one offense before the second offense was investigated. See id. After the defendant's acquittal, without seeking a new warrant, a different police department, the Peoria Police Department, acquired a copy of the hard drive, searched it, and uncovered evidence of child pornography, which was not a crime mentioned in the warrant. See id. The defendant was charged and convicted of possession of child pornography. See id.

The Supreme Court of Illinois concluded that the defendant's privacy interest in his computer's contents extended to the copy of the hard drive made by law enforcement after seizing the computer pursuant to the search warrant. See id. at 1206. The Court was unconvinced by the government's emphasis on the "defendant's lack of a formal property interest in the [copy] itself" because the government's theory disregarded the "defendant's informal privacy interest in his personal data." Id. The Court was persuaded by the defendant's argument that police examination of the copy was the same as an examination of the original, because its "evidentiary value . . . resides in the data itself, not in the

medium on which it is stored." Id. According to the Court, the idea that the "defendant lacked an expectation of privacy in the contents of his personal computer because those contents were copied to another medium contravene[d] the requirement of reasonableness[.]" Id. (citation omitted). In concluding that "[t]reating a digital copy as the original recognizes that the key to fourth-amendment reasonableness is the access to data, regardless of whether the data is copied, transferred, or otherwise manipulated[,]" the Supreme Court of Illinois found insight in the opinion of a key legal scholar on the topic. Id. (citing Kerr, Searches and Seizures, supra, 119 Harv. L. Rev. at 564). The Court ultimately held, however, that the defendant's appeal turned on his privacy interest in light of the warrant and the reasonableness of the examination of the copy after his acquittal and concluded that the examination was reasonable under the circumstances of the case. See id. at 1214.

In his law review article, Professor Kerr wrote that "important differences exist between the mechanisms of physical and digital evidence collection[,]" which create a "thorny issue" with respect to the Fourth Amendment's application to searches of computers and other electronic devices. Kerr, Searches and Seizures, supra, 119 Harv. L. Rev. at 532-33. Professor Kerr proposed that, for Fourth Amendment purposes, "a search of data stored on a hard drive occurs when that data, or information about that data, is exposed to human observation." Id. at 548. Under this approach, every "observable retrieval of information stored on a computer hard drive, no matter how minor, should be considered a distinct Fourth Amendment search[,]" which requires authorization from a warrant or an exception to the warrant requirement. Id. This emphasis on data, rather than

the hard drive as physical property, led Professor Kerr to the conclusion that "the same Fourth Amendment rules that apply to searching a suspect's computer should also apply to searching the government's [] copy." Id. According to Professor Kerr, treating the digital original and the copy as the same is consistent with the circumstance that generating a copy is normally a requisite step before searching the data stored in a hard drive, that "[a]ll computer data is a copy[,]" and that "the key is access to the data." Id. at 564.

On the other side of the ledger, in Megahed, 2009 WL 722481, *1, the United States District Court for the Middle District of Florida declined to suppress the internet history uncovered on a copy that the government had made of the hard drive of a computer seized from the Megahed family residence. The defendant's father had consented to the seizure and search of the computer, but later the defendant and his parents withdrew the consent. See id. at *1, *3. Although the Court held the suppression motion was untimely and moot, it also addressed the merits and reasoned that the defendant had no "reasonable expectation of privacy in the mirror image copy that the FBI had obtained already with [the defendant's father's] consent and had begun already to search." Id. In reaching this conclusion, the Court relied on Ponder, 444 F.2d at 818, and Mason v. Pulliam, 557 F.2d 426, 429 (5th Cir. 1977), cases in which the Fifth Circuit concluded that, when the government has obtained consent to seize and search paper documents, it may photocopy them, and if the defendant withdraws consent, the government may retain and continue to examine any

copies made while the consent was operative. See Megahed, 2009 WL 722481, at *3.[10]

In United States v. Thomas, No. 8:13-cr-462-T-33-TBM, 2014 U.S. Dist. LEXIS 33443, at *1-2, *17 (M.D. Fla. Feb. 14, 2014) (unreported report and recommendation), a case cited by the State, the defendant sought to suppress evidence gathered by law enforcement from a computer that he shared with his wife, which officers accessed for a brief period with his wife's consent. Initially, the defendant also consented, but then withdrew his consent. See id. at *17. During approximately 50 minutes of access, police viewed (and photographed) websites that the defendant had allegedly visited on the computer, which included images of "child erotica" and links that officers considered "indicative of child pornography." Id. at *3-4, *18 (footnote omitted). Law enforcement also scanned the computer with a "forensic preview tool for searching live active files [that] allows the user to scan the computer's registry including internet history, and to scan for images of child pornography or child erotica." Id. at *10. Once the defendant withdrew his consent, the police stopped the scan and later secured a warrant to further search the computer based on examination of the results of the initial scan. See id. at *12-14. The additional search pursuant to the warrant revealed images of child pornography, which the defendant sought to suppress. See id. at *14-15.

The United States District Court for the Middle District of Florida did not suppress the evidence, reasoning that "revocation of consent does not require the suppression of

[10]Decisions of the Fifth Circuit prior to the creation of the Eleventh Circuit are binding precedent for the Eleventh Circuit's courts. See Bonner v. City of Prichard, Ala., 661 F.2d 1206, 1209 (11th Cir. 1981) (*en banc*).

evidence already lawfully obtained." Id. at *18 (citing Megahed, 2009 WL 722481, at *3). The Court agreed with the government's position that "a valid consent to search carries with it the right to examine and photocopy." Id. at *20 (citing Ponder, 444 F.2d at 818). Because "the initial search . . . was supported by valid consent," the Court concluded that the police were "free to copy the data obtained by use of the" forensic tool "for further review without the necessity of obtaining a warrant to authorize such." Id. at *19-20.

On appeal, the defendant contended that his wife "did not have the authority to consent to a *forensic* search of the [] computer," and that the lack of consent made the search unlawful, as well as everything that flowed from it, including the warrant. See Thomas, 818 F.3d at 1239 (emphasis in original). The Eleventh Circuit disagreed, holding that the wife had the authority to consent and that, in getting the warrant, the police "relied on information obtained *before* Thomas even objected and attempted to revoke" that consent. Id. at 1241 (emphasis in original) (citation omitted). The Eleventh Circuit did not address the District Court's treatment of the forensic scan results as akin to a photocopy, but concluded that the warrant was valid because "the only information" utilized "in obtaining the search warrant was data collected prior to Thomas's objection." Id. at 1242.

D. Application of Above Principles to This Case

After careful examination of relevant authority, we hold that Mr. McDonnell had a reasonable expectation of privacy in the digital data stored on his laptop, and, as such, in the data stored on USACIDC's copy of his laptop's hard drive. Mr. McDonnell's reasonable expectation of privacy was not eliminated by the making of a copy of his hard

drive because the data was not searched or exposed prior to his revocation of consent.[11] Central to this holding is our conclusion that Mr. McDonnell's privacy interest is in the data on his hard drive, not just the particular computer or apparatus on which the data is stored (his original or USACIDC's copy). To accept the State's stance—*i.e.*, that Mr. McDonnell irrevocably lost all privacy interest in the data on his hard drive when he allowed USACIDC to copy it—would be to permit a limitless search through vast quantities and a varied array of personal data that the Supreme Court of the United States has characterized as consisting of more information than would be found in an exhaustive search of a person's home. See Riley, 573 U.S. at 396. Absent a warrant supported by probable cause or an exception to the warrant requirement, the Fourth Amendment does not permit such an unfettered governmental intrusion of a person's "private sphere[.]" Carpenter, 138 S. Ct. at 2213, 2221 (citation omitted).

Like the Supreme Court of Illinois, we focus on the data as the significant factor here, not the fact that USACIDC lawfully made a replica of Mr. McDonnell's hard drive. See McCavitt, 185 N.E.3d at 1206. We agree that Mr. McDonnell has a privacy interest in the data itself. "The evidentiary value of data resides in the data itself, not in the medium on which it is stored." Id. This conclusion flows logically from our explanation in Richardson that the defendant's abandonment of his cell phone made its seizure lawful, but did not permit the government, without a particularized warrant, to search the data stored on it. See Richardson, 481 Md. at 435-36, 282 A.3d at 105. So, too, here: Mr. McDonnell's

[11]Neither the voluntariness of Mr. McDonnell's consent nor the validity of his withdrawal of it is disputed.

consent made the creation and retention of the copy of his hard drive lawful, but after withdrawal of his consent, USACIDC needed additional authority to search the data on the copy. For the duration of Mr. McDonnell's consent, USACIDC had the authority to examine the data; once the consent was withdrawn, the authority to examine went with it. Likewise, Riley, 573 U.S. at 386, dictates that law enforcement's justification for a search of the data stored on an electronic device must be assessed independently from the justification for seizure of the device. Therefore, copying the same data to a different device that law enforcement officers have legal authority to possess makes no difference in the Fourth Amendment analysis.[12]

Because making a copy of a hard drive is usually the first step in performing a forensic analysis, if making a copy itself divested a person of a reasonable expectation of privacy in the data, people would lose all expectation of privacy in the entirety of the data on any device the moment the government made a copy of the device's hard drive. That would permit precisely the kind of unlimited rummaging through a person's private domain that the Fourth Amendment was designed to prohibit. See Riley, 573 U.S. at 386. The legitimate subjective and objective reasonable expectation of privacy that people have in their electronically stored data should not be so easily defeated. Focusing on the data in

[12]The logistics of digital storage also support this conclusion because data saved on a computer is automatically copied multiple times in the course of using a computer. See Kerr, Searches and Seizures, supra, 119 Harv. L. Rev. at 562. In addition, digital information is often deliberately or automatically copied to remote servers to be stored "in the cloud." Riley, 573 U.S. at 397 ("Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference." (Citation omitted)). Yet, the owners of such data, regardless of where it is copied and stored, have a reasonable expectation of privacy in the information.

question rather than on the possession of an apparatus containing a copy of the data "recognizes that the key to fourth-amendment reasonableness is the access to data, regardless of whether the data is copied, transferred, or otherwise manipulated." McCavitt, 185 N.E.3d at 1206 (citing Kerr, Searches and Seizures, supra, 119 Harv. L. Rev. at 564).

Obviously, in this case, if any data had been revealed prior to the revocation of Mr. McDonnell's consent, that data would have lost any reasonable expectation of privacy that was previously attached to it. That is because, as to that data, Mr. McDonnell's privacy interest would have been eliminated. And lawfully so, because USACIDC had the authority, while Mr. McDonnell's consent was in effect, to search and examine his data. In such a scenario, the cat could not be put back into the bag.

As to data that was not exposed before the withdrawal of consent, however, Mr. McDonnell retained an expectation of privacy. By way of analogy, if Mr. McDonnell had stood on a street corner and offered passersby the opportunity to read his diary, but no one took him up on it, his reasonable expectation of privacy would not be lost. The threat of an invasion of privacy is not an invasion at all. See Karo, 468 U.S. at 712. In this way, the creation of the copy was akin to the placement of the tracking device in Karo, id.,[13] because with the making of the copy, USACIDC created only the "potential for an invasion

[13]In Karo, 468 U.S. at 712, the Supreme Court held:

> The mere transfer to Karo of a can containing an unmonitored beeper infringed no privacy interest. It conveyed no information that Karo wished to keep private, for it conveyed no information at all. To be sure, it created a potential for an invasion of privacy, but we have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment.

of privacy" rather than an actual invasion of the subjective and objective expectation of privacy in Mr. McDonnell's data. It would be objectively reasonable to believe that data *could* be exposed to law enforcement through an owner's consent to copy a laptop's hard drive and *could* lose its private nature if examined—but, absent an enforceable waiver to the contrary, if law enforcement had not already become privy to the data, upon withdrawal of consent to access the data, the data remains private, *i.e.*, the owner retains a reasonable expectation of privacy in the data by withdrawal of consent.

1. The Consent Form

The quintessential test or criterion for determining the applicability of the Fourth Amendment's protection is one of "reasonableness." Riley, 573 U.S. at 381 (cleaned up). In the absence of a warrant, a search is reasonable only where it falls within an exception to the warrant requirement. See id. at 382. It is well settled that "[a]n individual may waive [] Fourth Amendment rights by giving voluntary and intelligent consent to a warrantless search of his person, property, or premises." United States v. Cormier, 220 F.3d 1103, 1112 (9th Cir. 2000) (cleaned up). In this case, we must assess the reasonableness of the search of data on the copy of the hard drive in light of the content of the consent form.

The terms of the consent form guide our assessment of the reasonableness of the search. Per the terms of the consent form, Mr. McDonnell authorized a Special Agent or other person designated by USACIDC to conduct a complete search of all "digital media including cell[ ]phones, thum[b]drive[s], hard disk drives, laptops & any other media relevant to this investigation." (Capitalization omitted). According to the language of the form, among other things, Mr. McDonnell relinquished his constitutional right to privacy

in his electronic devices and all of the information stored on them, and "authorize[d] USACIDC to make and keep a copy of any information stored on [his] devices." The form stated that Mr. McDonnell understood that any copy made by USACIDC would be the property of USACIDC and that he would have no privacy or possessory interest in the copy. Critically, a sentence at the bottom of the form stated without qualification: "I understand that I may withdraw my consent at any time."

Using the reasonableness approach discussed by the Supreme Court of the United States in Riley and Carpenter, and used by this Court in Varriale for that matter, we conclude that it was not reasonable for USACIDC to examine the data on the copy of Mr. McDonnell's hard drive after he withdrew his consent and that the examination was a search. It would have been objectively reasonable for Mr. McDonnell, or anyone else, to believe that the final sentence of the form advising of the ability to withdraw consent at any time applied to all of the language in the form, *i.e.*, that the withdrawal of consent applied to all of the matters agreed or consented to earlier in the form. See Riley, 573 U.S. at 386 (determining that it would be unreasonable to apply the search incident to arrest exception to permit a warrantless search of a cell phone because the rationale for the exception's application to physical objects did not extend to the digital contents of a cell phone); Carpenter, 138 S. Ct. at 2217-20 (determining that it would be unreasonable to apply the third-party doctrine to permit a warrantless search of 127 days' worth of cell site location records because society does not expect law enforcement to secretly track an individual's every movement without a warrant); Varriale, 444 Md. at 418-19, 119 A.3d at 835 (determining that it was reasonable for the State to retain and compare a defendant's

DNA sample to samples from cold cases under the totality of the circumstances of the consent to the taking of the sample). In this case, it would not be reasonable, under the totality of the circumstances, to interpret the consent form to mean that the withdrawal of consent applied only to certain language on the form and not to the entire document.

The State focuses on language on the form stating "I understand that any copy made by USACIDC will become the property of USACIDC and that I will have no privacy or possessory interest in the copy." The State refers to this language as a disclaimer and argues that the language could not be rendered ineffective by Mr. McDonnell's withdrawal of consent. We disagree. No language in the form states or even suggests that the acknowledgement of having no privacy or possessory interest in any copy made by USACIDC is irrevocable and not subject to withdrawal of consent at any time as provided by the language at the bottom of the consent form. The language setting forth the alleged disclaimer is contained in the fifth paragraph of the seven-paragraph form and is in no way distinguished from the other language of the form. It is included in the same paragraph in which Mr. McDonnell relinquished his right to privacy in his laptop itself, and, as the State agrees, the withdrawal of consent precluded further examination of the laptop. The paragraph is stylistically identical to every other paragraph in the document. In no way does the purported disclaimer stand out. Neither its express terms nor its appearance would suggest to a reasonable person that the last sentence of the fifth paragraph of a seven-paragraph document should be treated differently than the other language of the form with respect to the withdrawal of consent, as the State contends.

The language in the consent form did not convey that Mr. McDonnell relinquished for all time a privacy and possessory interest in the data on his laptop. Instead, the language sought to establish that Mr. McDonnell had no privacy or possessory interest in the copy of his data made by USACIDC based on the copy being property of USACIDC. But that cannot be. The copying of the data, without the data being examined, did not vitiate Mr. McDonnell's privacy interest in the data itself. As explained, a person has an independent privacy interest in the data on a laptop or hard drive, no matter where the data may be stored. See McCavitt, 185 N.E.3d at 1206. Due to the personal content and far-reaching consequences of allowing access to such data, the data on a laptop, like the digital information on a cell phone, warrants its own discrete privacy interest. See Riley, 573 U.S. at 386; Richardson, 481 Md. at 434, 452, 282 A.3d at 104, 115. Under the terms of the consent form, Mr. McDonnell never agreed to permanently relinquish a privacy interest in his data, and, as discussed above, the consent form, on its face, provided an unqualified right to withdraw consent at any time. This necessarily included the right to withdraw consent to a search of the data.[14]

[14]On brief and at oral argument, counsel for Mr. McDonnell asserted that even if the disclaimer had been written to accomplish what the State claimed it did, Mr. McDonnell retained a constitutional right to withdraw consent. This contention has significant rational force, as a person has a constitutional right to not consent in the first instance, and, as Mr. McDonnell points out, at least one court in another jurisdiction has so held. See United States v. McWeeney, 454 F.3d 1030, 1035 (9th Cir. 2006) (concluding defendants "had a constitutional right to modify or withdraw their general consent at any[ ]time"). Nothing in this opinion should be construed to mean that clauses in consent forms purporting to irrevocably waive the right to consent are enforceable. However, because the language in the consent form did not purport to irrevocably waive Mr. McDonnell's privacy or possessory interest in his data, we need not address the issue to resolve this case. See

The State argues that Mr. "McDonnell's reading would treat the disclaimer as meaningless[,]" but the State's treatment of the consent form's language regarding the copy would render a different portion of the document meaningless: Mr. McDonnell's right to withdraw consent "at any time." Mr. McDonnell's agreement that USACIDC could search his hard drive at any time was limited by his right to withdraw consent at any time. Based on the language of the consent form, it would not be reasonable to believe that, by consenting to the government's searching the laptop and making of a copy of its hard drive, a person could not withdraw consent before the search occurred and prevent the government from examining anything that had not yet been searched.[15]

When Mr. McDonnell revoked his consent to the search of the laptop, he retained a reasonable expectation of privacy in any data that had not been exposed. Because

---

Robinson v. State, 404 Md. 208, 217, 946 A.2d 456, 461 (2008) ("[I]t is this Court's established policy to decide a constitutional issue only when necessary." (Citations omitted)).

[15]As an alternate basis for affirming the Appellate Court's decision, Mr. McDonnell argues that he "enjoys a protectable property interest in his digitally-stored personal information, which was not extinguished by his transient consent or the agents' making of a forensic copy." (Emphasis omitted). Mr. McDonnell contends that the reasonable expectation of privacy analysis from Katz did not displace "property-based conceptions of Fourth Amendment rights." (Citations omitted). Due to our decision under the Katz reasonable expectation of privacy analysis, however, we need not reach the issue.

In addition, in a reply brief, the State contends that Mr. McDonnell's "property-based rationale" for the alleged Fourth Amendment violation is not properly before this Court because he did not raise the argument before the circuit court. We agree with the State that Mr. McDonnell raised only the reasonable expectation of privacy analysis before the circuit court. The record reflects that Mr. McDonnell did not raise the property-based theory of unlawful search before the circuit court, nor did that court address such an approach in denying the motion to suppress. Likewise, Mr. McDonnell failed to present the argument to the Appellate Court of Maryland, and that Court relied solely on the reasonable expectation of privacy analysis in its decision. See McDonnell, 256 Md. App. at 296, 286 A.3d at 120.

USACIDC did not search or examine *any* of his data prior to the withdrawal of consent, Mr. McDonnell continued to retain a privacy interest in the entirety of his data on his laptop's hard drive and the copy thereof. Lacking Mr. McDonnell's consent, USACIDC needed another justification for the examination of the data on the copy of the hard drive, such as a warrant. But because USACIDC did not obtain a warrant or have any other justification for the search, the search of the data on the copy of the hard drive was unlawful and the evidence obtained as a result of the search should have been suppressed.

Government action in consent searches is restrained in two ways: by limits placed on the scope of consent, see Varriale, 444 Md. at 412, 119 A.3d at 831, and withdrawal of the consent, see Williams, 898 F.3d at 330. Here, Mr. McDonnell provided his consent for USACIDC to seize, search, and copy his hard drive, limited by the scope of the investigation. Anything uncovered in the course of that consent would have been lawfully in USACIDC's possession. But once he withdrew his consent, a right he always had and which the consent form that he signed confirmed, USACIDC's authority to search ended. USACIDC could keep the copy, as Mr. McDonnell had consented to its creation; he could not un-ring that bell.

However, because USACIDC had not examined the data on the copy of the hard drive in any way while Mr. McDonnell's consent was in effect, it could not claim the right to search his data under the authority of his consent after his consent was withdrawn. This case involves the undifferentiated copying of the entirety of a hard drive before the examination of any data on it, which distinguishes it from those in which recipients consensually share with government actors emails or text messages, or law enforcement

gains access through other means to items with readily visible content. See United States v. Barber, 184 F. Supp. 3d 1013, 1016 (D. Kan. 2016); State v. Carle, 337 P.3d 904, 910 (Or. Ct. App. 2014).[16] In this case, the copying process exposed none of the data on the laptop's hard drive and the process did not differentiate between data that might have implicated child pornography and data that did not. Prior to his withdrawal of consent, USACIDC had not yet intruded upon Mr. McDonnell's privacy interest in the data on the copy of the hard drive; that bell was never rung, and upon the withdrawal of his consent, Mr. McDonnell retained a reasonable expectation of privacy in the data.

2. Consent and Digital or Electronic Data

As with a warrant for a search of electronic data, respect for the limits of consent "is arguably of even greater importance in the context of computers and smartphones than it is in the physical world, given the[ir] ability . . . to store 'millions of pages of text, thousands of pictures, or hundreds of videos[.]'" Richardson, 481 Md. at 452, 282 A.3d at 115 (quoting Riley, 573 U.S. at 394).[17] The difference between a photocopy of a paper

[16]For similar reasons, the State's argument that different iterations of data can have different reasonable expectations of privacy does not hold up when no data was examined or revealed before or during the copying of the laptop's hard drive, unlike the viewing of a physical copy of a digital photo. Because different facts could support the loss of a reasonable expectation of privacy in data on a hard drive, there may, of course, be other circumstances under which a forensic copy of a hard drive may not maintain the same Fourth Amendment protections as an original.

[17]As noted by *amici*, the American Civil Liberties Union and the ACLU of Maryland, electronic storage capacities have grown dramatically since Riley, as forecast by the Supreme Court. See Riley, 573 U.S. at 394. The maximum storage capacity of a cell phone todays is more than 15 times what it was when Riley was decided. Compare id. (describing the "top-selling smart[]phone" as having a storage capacity of "up to 64 gigabytes"); with Apple Inc., iPhone 14 Pro, https://www.apple.com/iphone-14-pro/specs

document and a copy of a hard drive is obvious in this context, and therefore we do not find that analogy persuasive, despite the decisions of courts in other jurisdictions cited by the State. With paper documents, law enforcement officers may first search the documents, *i.e.*, review the data contained in them, and then seize only the relevant ones (and likely copy them). However, the differences between papers and digital data, including the need to maintain the integrity of the digital evidence, the vast quantity of digital data or information involved, and the time necessary to conduct the search, require a different approach for hard drives. First, the laptop or computer is seized and the hard drive copied, and then, the search is conducted. So, whereas paper copies may have already been examined "to determine whether they are, in fact, among those papers authorized to be seized[,]" Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976), copying a hard drive does not expose any information about its contents to the government.

To the extent that there are cases such as Ponder from other jurisdictions that permit law enforcement officers after consent has been withdrawn to examine copies where papers have been bulk copied or copied without having been reviewed, this Court has not addressed the issue and adopted that approach. It may well be that if, or when, the issue is before us, this Court will conclude that, as with digital data, where law enforcement officers

---

[https://perma.cc/KUW9-6AKG] (listing smartphones with available capacity of one terabyte). A terabyte is equivalent to 1,000 gigabytes, which can store more than 83.3 million pages of text. See Univ. of Alaska Anchorage, How many files can I store? (July 13, 2022), https://service.alaska.edu/TDClient/36/Portal/KB/ArticleDet?ID=95 [https://perma.cc/4KE7-PVYA]. Contemporary laptops have even greater storage space. See, e.g., Apple Inc., Which Mac is right for you?, https://www.apple.com/mac [https://perma.cc/B9BA-HE4J] (listing laptops with available capacity of 8 terabytes).

have not reviewed or examined paper copies before a withdrawal of consent, the examination of the copies would be precluded if consent is withdrawn.

But, even if, for argument's sake, we were to apply the reasoning of cases like Ponder and its progeny, and the information in a thousand-page paper document was not entirely examined by the government prior to or in the course of photocopying the pages, such a copy would not begin to approximate a copy of a hard drive, which allows "[t]he sum of an individual's private life [to] be reconstructed[.]" Riley, 573 U.S. at 394. A copy of a paper document does not give access to the "many distinct types of information" found in a copy of a hard drive, which can reveal much more than any isolated record. Id.[18] A copy of a hard drive, the search of which "would typically expose to the government far *more* than the most exhaustive search of a house[,]" has as much in common with a

[18]For comparison, in the cases cited by the State for the proposition that consent includes the right to copy and thereafter examine the copies, the paper documents that were copied while consent was operative were far less voluminous than the amount of digital data that may be contained on a copy of a hard drive. In Ponder, 444 F.2d at 818 n.3, documents that the government copied

> consisted of a 'Receipts Book' which was photocopied, admitted in evidence, and its contents used against Ponder; and numerous deposit records shown on check stubs giving names of those who paid him and amounts of settlements on claims of clients, not introduced in evidence, but which were used as sources for leads.

Approximately "600 pieces of documentary evidence" were in evidence per the Fifth Circuit, which did not distinguish between those that were contested copies and those that were not. See id. at 818. In Ward, 576 F.2d at 244, the defendant consensually gave an agent of the Internal Revenue Service four boxes of records, which were not copied in their entirety until after he withdrew consent five days later. Despite the obvious privacy interest of the defendant in such financial documents, it cannot be said that accessing data on a hard drive would be an equivalent and, therefore, permissible level of intrusion into a person's personal or private affairs.

photocopy of paper documents as "a flight to the moon" has in common with "a ride on horseback[.]" Riley, 573 U.S. at 393, 396 (emphasis in original).[19]

With respect to digital information or data on a hard drive, and perhaps even photocopies for that matter, withdrawal of consent after copying but before analysis is like interruption of a consented-to search of a home by withdrawal of consent—police would have to promptly leave the home and seek a warrant, or other authorization, in order to further search.[20] The copying of Mr. McDonnell's hard drive was a precursor to a search, or perhaps a step in preparation, but it was not the search. An inexact comparison could be made to police securing a house, with the owner's consent, as precursor to a consent search. If the person were to withdraw consent after the securing but before the search, the search of the house would not occur and the owner would have lost a reasonable expectation of privacy only to the extent of what the officers may have observed before the consent was withdrawn. The advancement of technology that allows the digital equivalent

[19]As such, we decline to adopt the reasoning of courts in other jurisdictions that a forensic copy of a hard drive is akin to a photocopy of a paper document that, if made while consent was effective, can still be examined after consent is withdrawn. See, e.g., Lutcza, 76 M.J. at 702; Campbell, 76 M.J. at 658; Megahed, 2009 WL 722481, at *3; Thomas, 2014 U.S. Dist. LEXIS 33443, at *20.

[20]In some of the cases relied on by the State for the proposition that a copy of a hard drive is no different from a photocopy of a paper document, law enforcement officials had already begun to examine data on the hard drives in question prior to the revocation of consent. See Thomas, 2014 U.S. Dist. LEXIS 33443 at *4, *9-10, *18 (during approximately 50 minutes of consensual access to the defendant's computer, police viewed and photographed websites on the computer that the defendant had allegedly visited and scanned the hard drive for images of child pornography or erotica); Lutcza, 76 M.J. at 702 n.2 ("We recognize that in *Megahed*, unlike the instant case, the investigators began the actual review of the copied data prior to the revocation of consent."). This factual distinction further dilutes those opinions' persuasive value here.

of making a copy of a person's home and all its contents, see Riley, 573 U.S. at 396, should not permit invasion of a privacy interest that otherwise would be prohibited, see Kyllo, 533 U.S. at 34.

In this case, there is no indication in the record that law enforcement could not have sought a warrant to search the copy, once consent was withdrawn. The copying of the hard drive effectively preserved the evidence, just as police may secure a location while obtaining a warrant. See Illinois v. McArthur, 531 U.S. 326, 332 (2001). In this case, the fact that weeks passed between the completion of the copying and the start of the examination of the data shows that time was not of the essence. This contributes to the unreasonableness of the search after Mr. McDonnell withdrew his consent. See McNeely, 569 U.S. at 152 ("[W]here police officers can reasonably obtain a warrant before a blood sample can be drawn without significantly undermining the efficacy of the search, the Fourth Amendment mandates that they do so." (Citation omitted)).

Additional support for our conclusion comes from the Supreme Court's discussion in Carpenter, 138 S. Ct. at 2219, differentiating between physical and digital information in the context of another exception to the warrant requirement, the third-party doctrine. In Carpenter, id. at 2216, the Supreme Court stated that it has held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." (Cleaned up). The Supreme Court explained, though, that given the unique nature of cell phone location records, the fact that the information was held by a third party did not alone overcome the user's claim to Fourth Amendment protection. See id. at 2217.

Likewise, the "qualitatively different" nature of "detailed, encyclopedic, and

effortlessly compiled" digital information merits a different analysis than that applied to physical records. Id. at 2216-17. Similar to a person's retention of a reasonable expectation of privacy in the unique and unprecedented information held in cell site location records, despite the data's collection by cell phone companies, see id. at 2223, a person maintains a reasonable expectation of privacy in the information stored on a hard drive even when the government creates a copy. Just as the cell site location information's creation "for commercial" purposes did "not negate Carpenter's anticipation of privacy in his physical location[,]" id. at 2217, the creation of the copy, without more, did not negate Mr. McDonnell's expectation of privacy in the data in his hard drive. Like the detailed records of a person's movements in Carpenter, the data at issue here contains unique information of unprecedented comprehensiveness and breadth, including information that was previously unknowable, and deserves "special solicitude[.]" See id. at 2219.

The State's argument that the copy of the hard drive is like abandoned property is even less persuasive because a warrantless search of an electronic device lawfully within the government's custody is unreasonable, unless the government has authority to search the data specifically. See Riley, 573 U.S. at 386; Richardson, 481 Md. at 435-36, 282 A.3d at 105. Put simply, our case law and that of the Supreme Court of the United States leads to the conclusion that Mr. McDonnell had a reasonable expectation of privacy in his data, regardless of whether the data was stored on his laptop's hard drive or a copy of the hard drive, and, with the withdrawal of his consent, he maintained a reasonable expectation of privacy in the data, as it had not yet been examined.

3. Varriale

Just as we decline the State's invitation to treat copies of digital data as equivalent to copies of paper documents, we do not see cases involving consented-to blood and DNA sampling as controlling here. Although this Court has held that it may be objectively reasonable for police to indefinitely retain a DNA profile created with consent and use it in subsequent investigations, see Varriale, 444 Md. at 415-16, 119 A.3d at 833, the same cannot be said of a copy of a person's laptop hard drive. Moreover, this Court has not determined that it is objectively reasonable for law enforcement to retain and use a consented-to blood or DNA sample after consent has been withdrawn. Varriale did not involve an attempt by the defendant to withdraw consent to the testing or use of a previously consented-to sample. Rather, in Varriale, id. at 403, 119 A.3d at 826, the State used a DNA profile obtained from the consented-to sample in a different investigation than the one in which consent had been given for testing. This Court held that, given that there was no express limitation on the consent, the use of the DNA profile did not exceed the scope of consent and it was objectively reasonable for the police to retain and compare the DNA profile against evidence in another case. See id. at 418-19, 119 A.3d at 835. We likened the retention and use of the DNA profile to fingerprints, which law enforcement agencies "routinely catalog and compare[.]" Id. at 416, 119 A.3d at 833 (citations omitted).

Unlike a DNA profile that is held exclusively for identification purposes, a copy of a hard drive is not "like fingerprints," and police do not "routinely catalog and compare" copies of hard drives "in the course of criminal investigations." Id. at 416, 119 A.3d at 833 (citations omitted). A copy of a person's hard drive contains vast troves of personal data

that go far beyond serving to identify the owner, which has been the focus of this Court and others when assessing the use of DNA samples or similar evidence, like fingerprints. See id. at 416, 119 A.3d at 834; see also King, 569 U.S. at 461.

To be sure, there is an appealing simplicity to treating the seizure and copying of a hard drive within the framework of cases viewing "the collection and testing of blood" or other bodily fluids as "a single event for [F]ourth [A]mendment purposes[.]" People v. Woodard, 909 N.W.2d 299, 306 (Mich. Ct. App. 2017) (cleaned up). Both involve invasion of "an individual's most personal and deep-rooted expectations of privacy[,]" McNeely, 569 U.S. at 148 (cleaned up), and the outcome of a blood sample test is just as incomprehensible or unknown prior to testing as the data on a copy of a hard drive is prior to searching.

But the similarity stops there. Government examination of a copy of a hard drive would potentially violate far more of a person's "private sphere" than the testing of a blood sample. Carpenter, 138 S. Ct. at 2213 (citation omitted). As with a DNA sample held and analyzed for the purpose of identification, a blood test could reveal only so much or a limited sphere of information about a person's "privacies of life." Id. at 2214 (cleaned up). Most commonly, a blood sample is used to identify a person, via DNA, or to detect the presence of alcohol or other substances in a person's system, although other important information could also be revealed by certain tests if authorized, such as medical

conditions.[21] See Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 658 (1995) (concluding that a "significant" factor in the reasonableness of compulsory drug testing of student athletes was "that the tests at issue here look only for drugs, and not for whether the student is, for example, epileptic, pregnant, or diabetic" (citation omitted)). That this Court held, in Varriale, 444 Md. at 418-19, 119 A.3d at 835, that the use of the results of a consented-to DNA sample for an identification match in an unrelated case was reasonable, where there was no express limitation on the consent, does not by analogy make the examination of data on a copy of a hard drive reasonable, after the owner withdraws consent.[22]

4. Public Policy and Consent Searches

Undeniably, there are significant governmental interests in conducting consent searches generally and consent searches of computer hard drives containing digital

[21]Although the examination of Mr. McDonnell's data here sought only to locate images or data related to child pornography, this was not the kind of binary search that would give only a positive or negative result (*e.g.*, an identification match or lack thereof, or the presence or absence of alcohol). Instead, law enforcement would need to examine and assess each piece of data to see if it did in fact constitute or relate to child pornography. In the process, such a search could reveal a significant amount of innocuous information that would invade Mr. McDonnell's privacy in a way that a test for a DNA match or alcohol could not.

[22]The better analogy, though still imperfect, is between a hard drive lawfully copied but unexamined and cases involving the government's ability to examine the contents of packages lawfully obtained. The government's lawful possession of a package of undeveloped film does not permit examination of the film without a warrant or warrant exception, see Walter, 447 U.S. at 651-52, 654 (plurality op.), whereas the government can freely examine the contents of a package that has already been inspected by Federal Express employees before the package was provided to the government, because the government would "learn nothing that had not previously been learned during the private search[,]" United States v. Jacobsen, 466 U.S. 109, 111, 120 (1984) (footnote omitted). The previously uninspected data on the copy of Mr. McDonnell's hard drive is like an undeveloped roll of film, not a package's already-examined contents.

information in particular. Allowing officers to search based on a person's consent promotes the important social goal of cooperation between law enforcement and the public. See United States v. Drayton, 536 U.S. 194, 207 (2002). Further, a consent search "may result in considerably less inconvenience for the subject of the search" and may "be the only means of obtaining important and reliable evidence." Schneckloth v. Bustamonte, 412 U.S. 218, 227-28 (1973) (footnote omitted). But allowing the State to examine the data on a copy of a person's hard drive after a person has withdrawn consent would permit severe intrusions into one of the single most comprehensive repositories of a person's private information.

On the other hand, requiring law enforcement officers to get a warrant in this situation would increase the likelihood that people may consent to a search of a laptop or computer, as a person would not fear that the copying of a hard drive as part of the search would result in unfettered governmental access to their data in the future. Nor would the requirement of a warrant to search data where consent is withdrawn after copying of a hard drive necessarily cause inconvenience to law enforcement officers or impede investigations. To the contrary, it would incentivize law enforcement to act more expediently after obtaining consent to search the contents of a hard drive, *i.e.*, such a requirement would minimize delay.

E. Conclusion

The unique nature of digital information presents new challenges for the application of the Fourth Amendment's requirements concerning concepts such as the particularity of warrants, reasonableness of searches, and withdrawal of consent. See Richardson, 481 Md.

at 452-53, 282 A.3d at 115. Modern computers, cell phones, and other devices contain vast and varied types of personal information yet lack the inherent physical boundaries of other searchable items, such as backpacks or cars, thus requiring courts to find new ways to address the potential intrusion into privacy interests by unauthorized searches. See Riley, 573 U.S. at 393-97; Kerr, Searches and Seizures, supra, 119 Harv. L. Rev. at 556.

In this case, we hold that Mr. McDonnell had a reasonable expectation of privacy in his digital data, regardless of whether the data was electronically stored on his laptop's hard drive or USACIDC's copy of the hard drive, made with his consent. USACIDC's creation of a copy of the laptop's hard drive with his consent, in order to search it, did not annul Mr. McDonnell's reasonable expectation of privacy in the data, given that the examination of the data did not occur while the consent was effective. In light of Mr. McDonnell's withdrawal of consent, USACIDC's examination of the data on the copy was a search and was unreasonable in the absence of a warrant supported by probable cause or an exception to the warrant requirement.

JUDGMENT OF THE APPELLATE COURT OF MARYLAND AFFIRMED. ANNE ARUNDEL COUNTY TO PAY COSTS.

The correction notice(s) for this opinion(s) can be found here:

https://mdcourts.gov/sites/default/files/import/appellate/correctionnotices/coa/36a22cn.pdf