RECEIVED
03-04-2021
CLERK OF WISCONSIN
SUPREME COURT

IN THE SUPREME COURT OF WISCONSIN

STATE OF WISCONSIN
Plaintiff-Respondent,

Appeal No.
2019-AP-1404-CR

v.

GEORGE STEVEN BURCH,
Defendant-Appellant.

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION FOUNDATION, AMERICAN CIVIL LIBERTIES UNION OF WISCONSIN FOUNDATION, ELECTRONIC FRONTIER FOUNDATION, AND ELECTRONIC PRIVACY INFORMATION CENTER

Laurence J. Dupuis (WBN 1029261)
American Civil Liberties Union of
Wisconsin Foundation
207 E. Buffalo Street, Suite 325
Milwaukee, WI 53202
Telephone: (414) 272-4032, ext. 212
Email: ldupuis@aclu-wi.org

Jennifer Granick, admitted *pro hac vice*
American Civil Liberties
Union Foundation
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 343-0758
Email: jgranick@aclu.org

Jennifer Lynch, admitted *pro hac vice*
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 435-9333
Email: jlynch@eff.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

STATEMENT OF INTEREST OF AMICI

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to defending the principles embodied in the Federal Constitution and our nation's civil rights laws. The ACLU of Wisconsin Foundation is the local affiliate of the ACLU. The ACLU and the ACLU of Wisconsin have frequently appeared before courts—including this one—throughout the country in Fourth Amendment cases, both as direct counsel and as amici curiae.

The Electronic Frontier Foundation ("EFF") is a member-supported, nonprofit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for nearly thirty years. With roughly 35,000 active donors, including donors in Wisconsin, EFF represents technology users' interests in court cases and broader policy debates. EFF regularly participates both as direct counsel and as amicus in the Supreme Court, the Seventh Circuit Court of Appeals, this Court, and other state and federal courts in cases addressing the Fourth Amendment and its application to new technologies.

The Electronic Privacy Information Center ("EPIC") is a public-interest research center in Washington, D.C. established to focus public attention on emerging privacy and civil liberties issues in the information age. EPIC participates as amicus curiae before courts across the country in cases involving constitutional rights and emerging technologies.

Amici have, alone or together, appeared as either counsel or amicus in the following cases: *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014); *United States v. Jones*, 565 U.S. 400 (2012); *United States v. Miller*, 982 F.3d 412 (6th Cir. 2020), *petition for cert. filed*, (U.S. Feb. 25, 2021) (No. 20-1202) (Google's use of a proprietary algorithm to automatically search user data and refer to law enforcement); *State v. Sveum*, 2010 WI 92, 328 Wis. 2d 369, 787 N.W.2d 317 (warrantless GPS tracking of vehicles); *Belleau v. Wall*, 811 F.3d 929 (7th Cir. 2016)

(GPS bracelets); *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (en banc); *United States v. Patrick*, 842 F.3d 540 (7th Cir. 2016), *reh'g denied* (7th Cir. May 9, 2017) (cell-site simulators); *People v. Hughes*, No. 158652, 2020 WL 8022850 (Mich. 2020) (police searched cell phone data obtained in one investigation for evidence of a different crime).

Given this expertise, amici's participation may be helpful to this Court. The Court granted leave to file this brief on February 9, 2021. Order Granting Amici's Mot. to File a Non-Party Br.[1]

[1] Amici wish to thank Rachel Maremont, a student at New York University School of Law, and Melodi Dincer, a legal fellow at EPIC, for their contributions to this brief.

INTRODUCTION

The "central concern underlying the Fourth Amendment" is to avoid "giving police officers unbridled discretion to rummage at will among a person's private effects." *Arizona v. Gant*, 556 U.S. 332, 345 (2009). Yet, the State's position in this case—that it is authorized to indefinitely retain all of Burch's cell phone data and search it for any reason—opens the door to just such "general, exploratory rummaging" as the "'general warrant' abhorred by the colonists." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). Under the State's proposed rule, no one—including suspects, witnesses, and victims—who consents to a search of their digital device in the context of one investigation could prevent law enforcement from storing a copy of their *entire* device in a database and "min[ing] [it] for information years into the future." *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). Such a rule would enable the State to rummage at will among a person's most personal and private information whenever it wanted, for as long as it wanted. *See Riley v. California*, 573 U.S. 373, 399 (2014) (requiring greater protections for searches of digital data because "[t]he sources of potential pertinent information are virtually unlimited"). The Constitution does not grant the police such power.

For the reasons set forth below, amici answer this Court's questions presented as follows:

1. A reasonable person would consider the scope of consent to search a cell phone to be limited by the discussion with police identifying specific categories of data, and would believe that a download of "the information" referred to the categories of information discussed, not to a forensic download and search of the phone's entire contents.

2. Vague consent forms such as the one in this case cannot override more explicit oral statements and assurances about the scope of consent.

3. After police downloaded information from the cell phone, they could have retained and searched only the information Burch consented to share—his text messages from the night before the hit-and-run. See R. 234:9–10, App'x at 108–09. Any search of

that data also had to be limited to the context in which consent was given—the investigation of the hit-and-run.

4. The ongoing retention of information the police were permitted to access became unreasonable once police determined Burch was no longer a suspect in the hit-and-run investigation.

5. That Burch was no longer a suspect in the original investigation is a strong indication that continued retention of his data was unlawful.

6. Police first had an obligation to immediately return to Burch material outside the scope of consent, because it should never have been seized. Second, after officers completed their search by creating a report containing communications potentially relevant to the hit-and-run investigation, the remainder of Burch's data, which was non-responsive, should have been returned. Finally, when police determined that Burch was no longer a suspect, all his information should have been returned.

ARGUMENT

I. CELL PHONES GENERATE, STORE, AND PROVIDE ACCESS TO VAST QUANTITIES OF SENSITIVE PERSONAL INFORMATION THAT REQUIRE HEIGHTENED CONSTITUTIONAL PROTECTIONS AGAINST WARRANTLESS EXTRACTION, ANALYSIS, AND STORAGE.

Modern cell phones contain a wealth of sensitive information that would never have been accessible to law enforcement before. Today, government agencies have advanced forensic tools that can extract and analyze all of the data stored on a cell phone, including data that the user might not even know exists. When law enforcement obtains and analyzes an individual's cell phone data, it invades that individual's expectation of privacy protected by the Fourth Amendment, and it must obtain a warrant or an exception to the warrant requirement must apply.

A. Cell phone searches raise significant privacy concerns because they provide access to vast amounts of personal information.

A smartphone is a palm-sized portal into an individual's personal life. Smartphones "place vast quantities of personal information literally in the hands of

individuals." *Riley*, 573 U.S. at 386. The more than eighty percent[2] of Americans who own smartphones "keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate." *Riley*, 573 U.S. at 395.

In *Riley*, the U.S. Supreme Court recognized that cell phone searches "implicate privacy concerns far beyond those implicated" by the search of any other object and thus require heightened constitutional protections. *Id.* at 393. This is partly because "cell phones have become [a] pervasive and insistent . . . part of daily life"—so much so that they appear almost "as an important feature of human anatomy." *Id.* at 385; *see also* Alan Butler, *Get a Warrant: The S. Ct.'s New Course for Digit. Privacy Rights After* Riley v. California, 10 Duke J. Const. L. & Pub. Pol'y 83, 89–91 (2014).

Cell phone searches involve a quantitatively different privacy intrusion as compared to searches of physical items because of cell phones' "immense storage capacity." *Riley*, 573 U.S. at 385. In 2014, when the Supreme Court decided *Riley*, the top-selling smartphone could store sixteen gigabytes of data. *Id.* at 394.[3] The minimum storage on Apple's current line of iPhones is sixty-four gigabytes.[4] Some Android models offer one terabyte of storage, roughly sixty-four times more than a *Riley*-era phone.[5] And off-device cloud storage services expand capacity even further.[6] Storage capacities increase every year, as does the sheer volume of personal data stored on—and accessible from—cell phones.

Cell phones are also qualitatively different from other objects because they "collect[] in one place many distinct types of information—an address, a note, a

---

[2] Pew Rsch. Ctr., *Mobile Fact Sheet* (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile/.

[3] Sixteen gigabytes equals about 3,680 songs, 8,672 digital copies of *War and Peace*, 9,520 digital photos, or eight feature-length movies. *See* iClick, *How Big is a Gig?* (2013), https://www.iclick.com/pdf/02_howbigisagig_infographic.pdf.

[4] Apple, *Compare iPhone Models*, https://perma.cc/A7G9-AJQX (last visited Mar. 3, 2021).

[5] Samsung, *Galaxy S10+ 1TB (Unlocked)*, https://perma.cc/8BJ4-EP9W (last visited Mar. 3, 2021).

[6] Apple, *iCloud* (2021), https://perma.cc/5UMQ-NV3K (last visited Mar. 3, 2021) (providing up to 2TB of remote storage).

prescription, a bank statement, a video—that reveal much more in combination than any isolated record." *Riley*, 573 U.S. at 394. Along with more traditional data like text messages, phone calls, and emails, the proliferation of smartphone apps[7] for social media, health and activity, dating, video streaming, mobile shopping, banking, and password storage have created novel types of records that can "reveal an individual's private interests or concerns." *Riley*, 573 U.S. at 395. Location information in particular is "detailed, encyclopedic, and effortlessly compiled" by most apps whenever a "cell phone faithfully follows its owner . . . into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Carpenter v. United States*, 138 S. Ct. 2206, 2216, 2218 (2018).

B. Law enforcement increasingly extracts, analyzes, and stores the entire contents of cell phones using advanced forensic tools—often without a warrant.

In recent years, law enforcement agencies across the country have acquired powerful new tools, like the technology used in this case, to conduct detailed forensic searches of cell phones. These forensic search techniques are problematic because of how much personal information the searches can reveal when all of the data from a phone is extracted, organized, and categorized in unexpected ways, stored indefinitely, combined with other data, and used to generate leads in cases completely unrelated to the original search. There is simply no physical analog to the type of detailed information that law enforcement can obtain from a forensic cell phone search.

Mobile device forensic tools ("MDFTs") enable law enforcement to first extract and then analyze a complete copy of a cellphone's contents. Upturn, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* (Oct. 2020),

[7] *See* App Annie, *State of Mobile 2021* (2020), https://www.appannie.com/en/go/state-of-mobile-2021/ (gathering the most popular apps of 2020).

https://perma.cc/7DCK-PGMQ [hereinafter Upturn Report].[8] MDFTs extract "the maximum amount of information possible" from a phone, including a user's contacts, call logs, text conversations, photos, videos, saved passwords, GPS location records, phone usage records, online account information, and app data. *Id.* at 10, 16. MDFTs can access data stored remotely in the cloud and even data the user previously deleted. *Id.* at 16–17, 21–23. MDFTs can also use login credentials stored on a phone to extract data from apps and services that are otherwise password-protected. *Id.* at 17–20.

MDFTs enable law enforcement to organize and draw connections in extracted data. They can aggregate data from different apps and sort it by GPS location, file type, or the time and date of creation, enabling police to view the data in ways a phone user cannot, and to gain insights that would be impossible if the data were siloed by application. *Id.* at 12. Police can use a MDFT's data-sorting capability to make sense of reams of data and tell a particular story about a person, including by revealing where they were (and what they were doing), when, with whom, and even why.

An individual who gives police permission to take a quick look at their phone would be astounded at what the officers can learn when they use a MDFT, as the officers did in this case. Police can tell where and when somebody went to their place of worship. They can learn that a person has several joint bank accounts with a person of the same gender who is also tagged in hundreds of their photos. Police can also see that a person was at a recent protest where law enforcement made mass arrests, can read the person's deleted texts, and can download deleted photos from the event to analyze the faces of others present. They can even download the person's contacts from multiple apps, combine the data with contacts from other phones, and reveal the person's place in an extended network of individuals.

[8] Upturn is a 501(c)(3) organization that works in partnership with many of the nation's leading civil rights and public interest organizations to promote equity and justice in the design, governance, and use of digital technology.

Today, law enforcement agencies of all sizes in all fifty states and the District of Columbia have access to these powerful data extraction and analysis tools and use them frequently, placing "[e]very American [ ] at risk of having their phone forensically searched by law enforcement." *Id.* at 32. At least 2,000 law enforcement agencies have purchased MDFTs, while agencies without their own MDFTs often access them through partnerships with MDFT-equipped departments or through federal forensic laboratories. *Id.* at 32, 35, 39. Many police departments readily admit that they consider MDFTs a standard investigatory tool and use them daily. *Id.* at 47. At least 50,000 cell phone extractions took place between 2015 and 2019 among the forty-four agencies that reported statistics to Upturn. *Id.* at 41. This is a "*severe undercount*" of the national number, as the vast majority of the agencies that currently use MDFTs did not respond to Upturn's inquiries or did not track MDFT use statistics for the full period covered in the report. *Id.*

Despite the outcome of *Riley*, 573 U.S. at 386, many MDFT searches occur without warrants. Upturn's recent report shows that police frequently conduct detailed, warrantless forensic searches of cell phone data based on users' purported consent. Upturn Report at 46–47.[9] Some examples are striking: of the 1,583 cell phones on which the Harris County, Texas Sheriff's Office performed extractive searches from August 2015 to July 2019, 53 percent were consent searches or searches of "abandoned/deceased" phones. *Id.* at 46. Of the 497 cell phone extractions performed in Anoka County, Minnesota between 2017 to May 2019, 38 percent were consent searches. *Id.* at 47.

Once law enforcement extracts cell phone data, it has the technological capability to store the data forever and search it at will. The agency thus possesses massive amounts of information about a person that, unless subject to legal limitations, could be retained

[9] Consent has become an increasingly common justification for searches of physical evidence as well. *See, e.g.*, Ric Simmons, *Not "Voluntary" but Still Reasonable: A New Paradigm for Understanding the Consent Searches Doctrine*, 80 Ind. L. J. 773 (2005) (more than 90 percent of warrantless searches are accomplished through the use of consent).

indefinitely and searched at a later date. This is an unreasonable power for police to wield without strict constitutional review and independent judicial oversight.

II. CONSENT-BASED SEARCHES OF DIGITAL DATA MUST BE NARROWLY SCOPED IN CATEGORY AND PURPOSE TO THE OWNER'S EXPLICIT PERMISSION.

Both consent searches and warrant-based searches are "limited by the terms of [their] authorization." *Walter v. United States*, 447 U.S. 649, 656 (1980). This requirement helps avoid the indiscriminate searches and seizures that were the "immediate evils" motivating adoption of the Fourth Amendment. *Id.* at 657 (citing *Payton v. New York*, 445 U.S. 573, 583 (1980)). Further, as this Court has held, searches and seizures conducted on the basis of consent are reasonable only if conducted within the scope of the consent. *See State v. Randall*, 2019 WI 80, ¶ 10, 387 Wis. 2d 744, 930 N.W.2d 223. Given that cell phone searches can reveal voluminous amounts of people's most sensitive information through advanced forensic tools and the enormous privacy implications of allowing broad law enforcement access to this data, courts should narrowly interpret the scope of consent when a cell phone search is in question.

A reasonable person in Burch's position would consider their consent to search a cell phone to extend only to categories of data explicitly discussed with law enforcement in lay terms—not a forensic search of the phone's entire contents. A reasonable person would not expect a vague consent form to override previously limited verbal consent. Moreover, just as a warrant limits the scope of a search to the crime supported by probable cause, a reasonable person would also consider their consent to extend only to a search for evidence of the crime under investigation, and not to indefinite storage and use of their data to develop leads for investigations of other crimes.

Given the breadth and sensitivity of data on cell phones—the exact kind of information the Supreme Court said required heightened constitutional protections in *Riley*, 573 U.S. 373—the risks of a consent search to the device owner are severe. Consent searches are especially problematic because they are conducted without judicial authorization or oversight. Allowing law enforcement's unfettered access to Burch's

complete cell phone data in this case and the subsequent searches that police conducted months after that data was collected, for purposes never contemplated at the time of consent, would mean that the government may invade any individual's privacy—including victims' and witnesses'—in a similar manner without due justification in future cases.

A. A reasonable person would understand consent to search their cell phone as limited to common-sense categories of relevant information, such as the text messages in this case, and not to include a full forensic download and analysis.

A reasonable person would not believe that giving consent to search the text messages on their cell phone, or even to "the information" stored there, would mean they were giving the police permission to perform a complete search of the phone or to use MDFTs to extract and store all of the phone's data. Consent searches have always been limited by the scope of the permission granted. *Florida v. Jimeno*, 500 U.S. 248, 252 (1991). Especially given the unique nature of digital data and the powerful tools law enforcement agencies now possess, it is objectively reasonable to define consent to search a cell phone as including only a limited, manual search, at least in the absence of clear and unambiguous evidence to the contrary. Otherwise, voluminous and intimate data would be readily subject to indiscriminate police review. The consent exception, which was largely developed prior to the advent of phones that store enormous amounts of data, should not be used to expand access to digital data, which the U.S. Supreme Court has held should be subject to more, not less, Fourth Amendment protection. *Riley*, 573 U.S. at 393.

Courts evaluate consent for Fourth Amendment search purposes by asking whether the search was "voluntary," which "is a question of fact to be determined from all the circumstances." *Schneckloth v. Bustamonte*, 412 U.S. 218, 248–49 (1973). "No single criterion controls [the] decision." *State v. Phillips*, 218 Wis. 2d 180, ¶ 26, 577 N.W.2d 794 (1998). "The State bears the burden of establishing, clearly and convincingly, that a warrantless search was reasonable and in compliance with the Fourth

Amendment." *State v. Matejka*, 2001 WI 5, ¶ 18, 241 Wis. 2d 52, 621 N.W.2d 891.

With that in mind, common intuition about how cell phones work would limit consensual access to particular categories of data found on a device, rather than the entire corpus. When a person looks for information on their own cell phone, they commonly open a particular app, such as text messages or email. They then search that specific category of data, either by scrolling through messages or by typing a query term in the search bar and pressing "Enter." The owner reasonably expects the same common-sense "search" when giving consent to police.

However, when police use a MDFT to search a phone, the individual "likely doesn't even have a rough idea of what's really about to happen to their phone." Upturn Report at 60. The public generally does not know that MDFTs exist, how they work, or that police departments use them to conduct forensic searches of phones. Before Upturn's report, there was essentially no public accounting of how often police use MDFTs, the broad range of investigations in which they do so, how much data they uncover, their analytic capabilities, and what happens with the data afterwards. If privacy experts are only beginning to pierce the veil of police MDFT use, ordinary citizens cannot be expected to understand and consent to extractive searches.

Under these circumstances, the layperson's common-sense understanding that consent applies to particular categories of data on a device, and not to all information, should rule. *United States v. Morton* illustrates this point. 984 F.3d 421 (5th Cir. 2021). In *Morton*, given the nature of the crime, the court determined that probable cause was sufficient to support a warrant to search only certain aspects of a phone—but not others. *Id.* at 426. Noting that the Supreme Court's decision in *Riley* rested in part on the observation that "a cell phone's capacity allows even just one type of information to convey far more than previously possible," the *Morton* court held that "*Riley* made clear that [ ] distinct types of information, often stored in different components of the phone, should be analyzed separately." *Id.* Just as "[c]onsent to search a garage would not implicitly authorize a search of an adjoining house," *Walter*, 447 U.S. at 656–57, consent

to search "information" on a phone is limited by the category of information made salient by the context of the consent.

This limitation on the categories of data that can be searched also applies to deleted information, information stored in the cloud, and data, such as incoming messages, that did not exist when law enforcement first received consent to search. Individuals generally do not give prospective consent to a search for information they did not know or expect to be on the phone. An ordinary person does not know that data they delete from their device is still "on" it and does not expect that anyone in possession of the phone can access deleted information. *See* Upturn Report at 21–22. Further, when a person deletes data from their phone, they clearly indicate that they do not want anyone, including law enforcement, to look at the data, thus excluding it from the scope of consent. Similarly, accessing data stored on the cloud and not actually resident on the device also dramatically expands the scope of a search. *Riley*, 573 U.S. at 397. As the *Riley* Court explained, "[t]reating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen." *Id.* (citations omitted). Finally, information received while the phone is in law enforcement's possession may change the individual's decision to consent and thus cannot be considered within the scope of the original consent.

Here, the evidence shows that Burch gave consent only to a limited search of his text messages. In response to Detective Bourdelais's inquiry about text messages that would corroborate his story that he was not in the neighborhood of the hit-and-run, Burch agreed that Detective Bourdelais could search those messages. *State v. Burch*, No. 2019AP1404-CR, at 3 (Wis. Ct. App. Oct. 20, 2020). Detective Bourdelais then inquired whether Burch would be willing to let the police download "the information" off the phone. *Id*. at 4. A reasonable person would have understood this to mean download "the information" they had previously discussed—the text messages.

B. Consent searches are also limited in scope to the purposes for which a reasonable person would understand their data is being examined.

When agreeing to a cell phone search, a reasonable person believes that they agree to a search for evidence of crimes related to the investigation at hand. Searches for evidence of unrelated crimes will generally be outside of the scope of consent and unconstitutional.

"The scope of a search is generally defined by its expressed object." *Jimeno*, 500 U.S. at 251. In *Jimeno*, the officer told the defendant that he wanted to search his car for narcotics and the defendant consented. That consent necessarily included permission to search containers in the car that might hold drugs. *Id*. The consent does not include searches of areas of the car or packages which could not contain narcotics. Similarly, Burch's consent to search his texts in connection with the hit-and-run does not cover different types of files, nor evidence of a different offense.

Inspections are "limited to the purposes contemplated by the [consenting] suspect." *United States v. Blocker*, 104 F.3d 720, 728 (5th Cir. 1997) (*quoting United States v. Bosse*, 898 F.2d 113, 115 (9th Cir. 1990)). Police are not allowed to misrepresent the purpose for consent. If they do, the consent is invalid. "A ruse entry when the suspect is informed that the person seeking entry is a government agent but is misinformed as to the purpose for which the agent seeks entry cannot be justified by consent." *Bosse*, 898 F.2d at 115. The searches here should have been limited to the purpose that Burch, or a reasonable person in his position, contemplated—evidence of the hit-and-run, and not some other crime.

C. Limitations on consent are particularly important because consent searches of cell phones raise unique concerns about law enforcement coercion.

People may feel coerced to offer consent when law enforcement seizes or threatens to search their cell phones. Scholars and practitioners have long criticized the consent exception to the Fourth Amendment's warrant requirement on policy grounds, often referencing the inherently coercive nature of law enforcement "requests." *See, e.g.*,

Marcy Strauss, *Reconstructing Consent*, 92 J. Crim. L. & Criminology 211, 236 (2002) ("most people would not feel free to deny a request by a police officer"); Janice Nadler, *No Need to Shout: Bus Sweeps and the Psych. of Coercion*, 2002 Sup. Ct. Rev. 153, 156 (2002) ("the fiction of consent in Fourth Amendment jurisprudence has led to suspicionless searches of many thousands of innocent citizens who 'consent' to searches under coercive circumstances"). Many have also observed that coercion is particularly present for people of color, and especially Black Americans, who may fear physical harm if they decline a request from a law enforcement officer. *See, e.g.*, Devon W. Carbado, *(E)Racing the Fourth Amend.*, 100 Mich. L. Rev. 946, 971, 972 & n.121, 973 (2002); *United States v. Washington*, 490 F.3d 765, 768–69 (9th Cir. 2007) (finding lack of consent after two incidents where white police officers shot African Americans during traffic stops).

In the cell phone context, people may feel additional coercion to consent to a search just to get their device back. Cell phones perform many essential functions, serving as prescription drug reminders,[10] and lifelines to app-based services such as Uber and Lyft. People who find themselves questioned by law enforcement may feel pressured to acquiesce to search requests to quickly regain access to the device, for example to call the babysitter and say that they've been delayed and will be home late.

D. Consent forms deserve little weight because they often fail to provide people facing an investigation sufficient information about their rights or about what a search means.

As the State concedes, "a general consent form can be overridden by more explicit statements." State Br. at 17. In practice, consent forms should get little weight in determining the scope of consent in the mind of a reasonable person. Research shows both that consent forms fail to inform people of their rights and that most people do not read consent forms. Police often use generic consent forms to authorize broad forensic

[10] J.D. Biersdorfer, *Getting Alerts from a Digital Pillbox*, N.Y. Times (June 5, 2017), https://perma.cc/M4DR-DABR. ("The App Store stocks several dozen pharmaceutical apps designed to organize your pills, schedule doses and remind you to take your medicine.").

phone searches. Most agencies' consent forms fail to specify how police search the phone, which tools they use, the scope of the search, how long they intend to retain the data, and the purposes to which that data may be put. Upturn Report at 60 & n.195. The form at issue in this case is a prime example. It purported to give "Officer Bourdelais or any assisting personnel permission to search my Samsung Cellphone." R. 234:12, App'x at 111; R. 78, App'x at 114. Consent forms that do not clearly describe the searches they supposedly authorize should not override evidence of a more limited scope of consent, such as the explicitly limited access to "text messages" that Burch gave in this case.

Further, a wide body of research shows that across different contexts, most people do not read consent forms. *See, e.g.*, Benjamin D. Douglas et al., *Some Rschs. Wear Yellow Pants, but Even Fewer Participants Read Consent Forms: Exploring and Improving Consent Form Reading in Human Subjects Rsch.*, 26 Psych. Methods 61 (2021) ("Participants do not thoroughly read, comprehend, or recall information in consent forms" in medical trials or procedures.). This is particularly true when the person is in police custody, under investigation, or otherwise confronted with the power of the state. "[A] consent form may do relatively little to improve a suspect's understanding of her rights, particularly when the suspect is poorly educated, frightened, or otherwise unable to understand the form." Nancy Leong & Kira Suyeishi, *Consent Forms and Consent Formalism*, 2013 Wis. L. Rev. 751, 753 (2013). Further, "once the suspect has been given the form, the inclination is merely to read it rather than to engage in a dialogue with the officer designed to clarify the meaning of the form." *Id.* at 789.

All of these factors mean written consent forms are not especially persuasive or binding evidence that a reasonable person consented to a particular search. Here, the existence of a signed consent form should not override Burch's limited verbal consent to search his text messages. The consent waiver Burch signed did not specify what areas of his phone would be searched, what tools would be used to conduct the search, or what would happen to his data following the search. *State v. Burch*, No. 2019AP1404-CR, at 4. Nor is there any indication in the record that Detective Bourdelais explained any of these things to Burch, which could have lent more weight to the form in a "totality of the

circumstances" analysis of the scope of consent. For these reasons, this Court should find that Burch's consent to search his cell phone extended no further than his text messages.

III. THE RETENTION OF BURCH'S CELL PHONE DATA VIOLATED THE FOURTH AMENDMENT.

The government's ongoing retention of Burch's cell phone data was unreasonable because it seized data outside of the scope of consent; it retained data that was non-responsive to the hit-and-run investigation;[11] and it retained the data after the State concluded that Burch was not a suspect in that investigation. At each of these points, the government had at most a limited interest in holding Burch's data. Burch's privacy interest in his own data dwarfed the State's interest. Therefore, the seizure of Burch's data was unreasonable and violated his Fourth Amendment rights.

A. Copying Burch's digital data constituted a seizure under the Fourth Amendment.

By copying data on Burch's phone, the Green Bay Police Department ("GBPD") effected a seizure within the meaning of the Fourth Amendment. "A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). As Justice Stevens wrote in *United States v. Karo*, "[t]he owner of property, of course, has a right to exclude from it all the world, including the Government, and a concomitant right to use it exclusively for his own purposes." 468 U.S. 705, 729 (1984) (Stevens, J., concurring in part and dissenting in part). Just as physical property may be "seized" within the meaning of the Fourth Amendment, so too may digital property. *See, e.g.*, *United States v. Werdene*, 883 F.3d 204, 212 (3d Cir. 2018) (government software "seized" information from defendant's computer); *United States v. Ganias*, 755 F.3d 199, 137 (2nd Cir. 2016) (en banc); *United States v. Comprehensive Drug Testing, Inc.*,

[11] "Responsive data" generally refers to information relevant to probable cause while "non-responsive data" means irrelevant information police were nevertheless permitted to overseize as a matter of administrative convenience. Here, we use "non-responsive data" to include information other than the text message data as well as any data on the phone that did not relate to the initial hit-and-run investigation.

621 F.3d 1162 (9th Cir. 2010) [hereinafter *CDT*] (en banc) (per curiam) (referring to the copying of electronic data as a seizure throughout the opinion).

When the GBPD copied the contents of Burch's phone, they deprived him of core possessory interests: the rights to exclude others from using his data and to dispose of his data as he saw fit. The Brown County Sheriff's Office ("BCSO") repeated these deprivations when it obtained another copy of the data from the GBPD. These acts of copying constituted two separate seizures under the Fourth Amendment.

B. It was unreasonable for the State to retain everything on Burch's phone.

The Supreme Court has made clear that "a seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution unreasonably infringes possessory interests protected by the Fourth Amendment[]." *Jacobsen*, 466 U.S. at 124. To determine whether a given seizure is reasonable under the Fourth Amendment, the Court looks to whether it "was reasonably related in scope to the circumstances which justified the interference in the first place." *Terry v. Ohio*, 392 U.S. 1, 20 (1968). Thus, in *United States v. Place*, for example, the Court held that although an initial seizure of luggage for the purpose of subjecting it to a "dog sniff" test was reasonable, prolonging that detention by ninety minutes was "sufficient to render the seizure unreasonable." 462 U.S. 696, 710 (1983); *see also Jacobsen*, 466 U.S. at 124 n.25 ("The seizure became unreasonable because its length unduly intruded upon constitutionally protected interests.").

The recognition that an initially justified seizure may become unreasonable solely due to ongoing detention is particularly important in cases involving the search of electronic devices. Because evidence on these devices may be intermingled with a large amount of irrelevant data, courts frequently permit the government to initially seize data beyond the scope of its authorization to facilitate later targeted searches. *See, e.g.*, *CDT*, 621 F.3d at 1177 (recognizing the "reality that over-seizing is an inherent part of the electronic search process"). But the government does not have an independent right to hold the data it gains through overseizure; that data is instead obtained through "a

courtesy that was developed for law enforcement." *People v. Thompson*, 28 N.Y.S.3d 237, 259 (N.Y. Sup. Ct. 2016); *see United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) ("[T]he wholesale *seizure* for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as 'the kind of investigatory dragnet that the [F]ourth [A]mendment was designed to prevent.'" (citation omitted)).

Thus, the Fourth Amendment does not allow the government to profit from its overseizure of digital data. *See CDT*, 621 F.3d at 1177 (declaring in context of search authorized by warrant "[t]he process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect."). When the government overseizes data as part of a device search, "[t]he potential for privacy violations occasioned by an [additional] unbridled, exploratory search . . . is enormous," *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013). As a result, the Fourth Amendment particularity requirement "assumes even greater importance" where digital evidence is concerned than it does in the physical evidence context. *Id.* at 446.

The U.S. Supreme Court has articulated a balancing test to determine when a seizure becomes unreasonable. Courts "must balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." *Jacobsen*, 466 U.S. at 125 (citation omitted). The same balancing test can be used to determine the reasonableness of the government's seizure and continued retention of individuals' digital data.

Because a person's privacy and possessory interests in the whole of the electronic data on a device are of the highest significance—these devices "hold for many Americans the 'privacies of life,'" *Riley*, 573 U.S. at 403 (citation omitted)—courts must apply intense scrutiny to the government's asserted interests and ensure the government intrusion is properly cabined. The government may have an interest in initially overseizing data so that, for example, it can later use the proper search tools and does not have to effectuate a targeted search on site. Here, the forensic investigator created a

report containing all communications back and forth after June 7. *See* State Br. at 11. Even if the GBPD were justified in initially overseizing Burch's data—for example, if this Court were to find that Burch's consent extended beyond his text messages—after the police generated the report, the agency's legitimate interests in retaining the rest of Burch's data were minimal. *See United States v. Metter*, 860 F. Supp. 2d 205, 212 (E.D.N.Y. 2012) (government's fifteen-month delay in reviewing seized electronic evidence and segregating non-responsive data was unreasonable).

The GBPD's interests in retaining Burch's data were diminished even further when he was no longer a suspect.[12] The State has offered no good reason for keeping the data contained in the hit-and-run report, never mind the entirety of the data. Because Burch was no longer a suspect and the data on his phone was irrelevant to the investigation of any other suspect, the State's argument that it needed to retain all of Burch's data to properly authenticate the download, State Br. at 22–24, fails. At that point, Burch's privacy and possessory interests in his data outweighed the government's interests, and any retention of data outside the scope of the first investigation—at least any data not included in the report—was unreasonable.

C. The Fourth Amendment requires that law enforcement purge or return unreasonably seized digital data.

To effectuate the Fourth Amendment's guarantee against unreasonable seizures, this Court should require that law enforcement purge unreasonably seized data. The rule is a straightforward application of the Supreme Court's decision in *Andresen v. Maryland*, 427 U.S. 463 (1976).[13] There, the Supreme Court affirmed that with respect to

[12] The State argues that the record does not clearly demonstrate whether or not the hit-and-run investigation was over. Even if true, the burden of justifying a warrantless search or seizure falls on the government, not on the defendant. *Kentucky v. King,* 563 U.S. 452, 474 (2011).

[13] This approach is also consistent with common understanding at the time of the Framers. A recent scholarly article establishes that the Framers understood that seized evidence had to be brought before a magistrate who then had the authority to return evidence seized outside of the scope of a warrant to the property owner. *See* Laurent Sacharoff, *The Fourth Amend. Inventory as a Check on Digit. Searches*, 105 Iowa L. Rev. 1643, 1687 (2020) ("[T]he original practice provides a surprisingly unambiguous picture of the central role the return played in England and the colonies, both as ordinary practice and as important rhetoric leading to the Fourth Amendment.").

papers that exceeded the scope authorized by the government's search warrant, "the State was correct in returning them voluntarily," *Id.* at 482 n.11. The same rule that covers paper records that the government has no right to hold—that they must be returned to the full control of their owner—applies also to digital data. Even the U.S. Department of Justice has recognized that the government has a duty to purge non-responsive files. *See Ganias*, 824 F.3d at 238 (Chin, J., dissenting) (government agent acknowledged he should have returned or destroyed non-responsive items after a "reasonable period" of off-site review). Lastly, several federal courts have drawn a purge requirement from the Fourth Amendment as they have denied warrant applications on the grounds that the government did not adequately establish a procedure to purge data beyond the scope of the authorization. *See In re Search of Black iPhone 4*, 27 F. Supp. 3d 74, 80 (D.D.C. 2014); *In re Search of Info. Associated with the Facebook Acct. Identified by the Username Aaron.Alexis That Is Stored at Premises Controlled by Facebook, Inc.*, 21 F. Supp. 3d 1, 10 (D.D.C. 2013); *In the Matter of the Search of Premises Known as a Nextel Cellular Tel.*, No. 14-MJ-8005-DJW, 2014 WL 2898262, at *10 (D. Kan. June 26, 2014); *Matter of the Search of Apple iPhone, IMEI 013888003738427*, 31 F. Supp. 3d 159, 166 (D.D.C. 2014); *Matter of Search of ODYS LOOX Plus Tablet Serial No. 4707213703415 in Custody of United States Postal Inspection Serv., 1400 New York Ave NW, Washington, DC*, 28 F. Supp. 3d 40, 45 (D.D.C. 2014).[14]

In the alternative, this Court should follow the Oregon Supreme Court in imposing a restriction on law enforcement's ability to use any evidence that exceeds its authorization to search. *State v. Mansor*, 421 P.3d 323, 342–43 (Or. 2018). A use restriction would limit the government, except in exigent circumstances and other narrow exceptions, to using only data that is actually responsive to—that is, described by—the

[14] The Fourth Amendment does not require Burch to make a formal request for the return of his data because the government has no legal basis to retain information it has no authorization to hold. *See Ganias*, 824 F.3d at 236 (Chin, J., dissenting) (noting that government, not defendant, bears burden of proving reasonableness under Fourth Amendment). The availability of statutory procedures that provide for the return of property has no bearing on the constitutional requirements.

warrant (or within the scope of consent in this case). As one influential commentator has explained, "[t]his approach best reconciles the government's compelling need to obtain the evidence sought in the warrant with the Fourth Amendment's prohibition on general warrants." Orin S. Kerr, *Executing Warrants for Digit. Evid.: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech. L. Rev. 1, 10 (2015). While a purge rule is more privacy protective and protects against the problem of "parallel construction" whereby the government builds an independent evidentiary basis to conceal the original source of unlawfully obtained evidence, under either approach, the Court must ensure that "future searches of electronic records" do not turn "all warrants for digital data into general warrants." *CDT*, 621 F.3d at 1178 (Kozinski, J., concurring); *see also United States v. Sedaghaty*, 728 F.3d 885, 914 (9th Cir. 2013) (invalidating computer search where agents sought to retain and use "information beyond the scope of the warrant" and insisting that agents "should have sought a further warrant").

IV. THE BROWN COUNTY SHERIFF OFFICE'S SUBSEQUENT SEARCH OF BURCH'S DATA VIOLATED THE FOURTH AMENDMENT.

Because the retention of Burch's phone was unlawful, this Court need not reach the issue of the Brown County Sherriff's Office (BCSO) subsequent search of the cell phone data. Nonetheless, the BCSO's search of Burch's data pursuant to its investigation of a wholly unrelated crime constituted an independent violation of the Fourth Amendment. Not only was this search executed on data the government no longer had authority to retain, it was conducted without a warrant. *See, e.g.*, *Ganias*, 824 F.3d at 199 (finding good faith reliance on second search warrant immunized government's retention and search of defendant's data in later, unrelated investigation); *see also United States v. Wey*, 256 F. Supp. 3d 355, 407 (S.D.N.Y. 2017) (Fourth Amendment violated when law enforcement mined overseized information for evidence of new crimes); *United States v. Hulscher*, No. 4:16-CR-40070-01-KES, 2017 WL 657436, at *3 (D.S.D. Feb. 17, 2017) (finding second search warrant necessary to investigate wholly separate set of crimes and noting that to find otherwise "would allow for mass retention of unresponsive cell phone data [and] is simply inconsistent with the protections of the Fourth Amendment").

As even the State acknowledges, the police's authority to "subsequently examine an item lawfully in their possession" extends only "to the same extent they could originally search the item." State Br. at 26. That is also consistent with the lead opinion in *Randall*, 2019 WI 80, ¶ 35 (consent to search lawfully obtained blood sample for alcohol content does not provide authorization to search for "genetic information"). Because searching for evidence of an unrelated crime far exceeds the scope of Burch's authorization, even if GBPD lawfully could have retained a copy of Burch's data, the BCSO was obligated to obtain a second warrant to search it.

CONCLUSION

This Court should reverse the decision below and remand for a new trial.

Dated this 4th of March, 2021.

Respectfully submitted,

Laurence J. Dupuis (WBN 1029261)
Legal Director
American Civil Liberties Union of
Wisconsin Foundation
207 E. Buffalo Street, Suite 325
Milwaukee, WI 53202
Telephone: (414) 272-4032, ext. 212
Email: ldupuis@aclu-wi.org

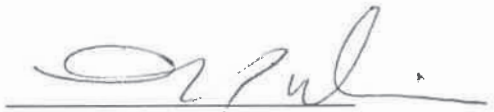
Jennifer Granick, admitted *pro hac vice*
American Civil Liberties
Union Foundation
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 343-0758
Email: jgranick@aclu.org

Jennifer Lynch, admitted *pro hac vice*
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Email: jlynch@eff.org

CERTIFICATION AS TO FORM AND LENGTH

I hereby certify that this brief conforms to the rules contained in Wis. Stat. § 809.19(8)(b) and (c) for a brief produced with a proportional serif font. The length of this brief is 7,500 words, permitted per order of this Court issued on February 18, 2021.

Dated this 4th of March, 2021



Laurence J. Dupuis (WBN 1029261)
Legal Director
American Civil Liberties Union of
Wisconsin Foundation
207 E. Buffalo Street, Suite 325
Milwaukee, WI 53202
Telephone: (414) 272-4032, ext. 212
Email: ldupuis@aclu-wi.org

CERTIFICATE OF COMPLIANCE WITH WIS. STAT. § 809.19(12)

I hereby certify that:

I have submitted an electronic copy of this brief, excluding the appendix, if any, which complies with the requirements of Wis. Stat. § 809.19(12).

I further certify that:

This electronic brief is identical in content and format to the printed form of the brief filed as of this date.

A copy of this certificate has been served with the paper copies of this brief filed with the Court and served on all parties.

Dated this 4th of March, 2021

Laurence J. Dupuis (WBN 1029261)
Legal Director
American Civil Liberties Union of
Wisconsin Foundation
207 E. Buffalo Street, Suite 325
Milwaukee, WI 53202
Telephone: (414) 272-4032, ext. 212
Email: ldupuis@aclu-wi.org