**Navigating the Digital Frontier:**
**Understanding U.S. Laws on Electronic Search and Seizure**

Ananda de Almeida, GW Law '24

*September 2025*

## I. Introduction

In an age where our lives are increasingly online, our digital breadcrumbs can become evidence when an arrest unlocks a government probe into your online world. In the United States, the Constitution's Fourth Amendment offers a shield; but how strong is that defense against legal and technological intrusions?

The legal system in the United States offers a nuanced illustration of how due process considerations are addressed within the scope of a key feature of modern criminal legal procedure: government search and seizure of electronic devices and digital evidence. The foundation of this framework is the Fourth Amendment of the U.S. Constitution, which lays the groundwork for the right to privacy and safeguards against unreasonable government searches and seizures. The development of this framework over time illustrates the United States' efforts to reconcile enduring constitutional principles with the rapidly evolving landscape of technological advancements.

U.S. law, with its federalist structure, serves as a broad repository of diverse legal responses addressing the interplay of privacy, state authority, and individual rights amidst evolving technological conditions. Countries looking to update or formulate their own legal standards in the digital age may benefit from examining the U.S. approach to these complex issues, considering its strengths and weaknesses.

This Article will begin by reviewing the U.S. federal legal system and exploring the constitutional safeguards that underpin due process, privacy rights, and the protections against self-incrimination under this framework. It will then turn to studying state-level interpretations and adaptations of these federal norms. The Article will conclude by analyzing how various state approaches relate to the federal baseline, offering insights that might be valuable for countries looking to refine their legal framework in this area.

## II. Overview of U.S. Federal Law

This section will discuss U.S. constitutional protections related to due process, search and seizure procedures, and protections against self-incrimination.

### *A. Due Process and the Fourth Amendment*

The Fourth Amendment of the U.S. Constitution establishes the fundamental criteria for due process protections, which guarantee that individuals have the right to be protected in their bodies, homes, documents, and personal belongings from unreasonable searches and seizures by the government.[1] The amendment also stipulates that search warrants can only be issued if there

[1] U.S. CONST. amend. IV.

is a reasonable basis, confirmed by a sworn statement, and must clearly specify the location to be searched and the individuals or items to be seized.

In essence, the Fourth Amendment protects against *unreasonable* searches and seizures. Central to this protection is the warrant requirement. Law enforcement is required to obtain a warrant before conducting a "search," barring certain exceptions.[2] A search occurs when the government obtains information by encroaching upon a constitutionally protected area, such as entering a home, or when it infringes on a person's reasonable expectation of privacy.[3]

The degree of protection afforded by the Fourth Amendment also hinges on the location of the search or seizure.[4] "Searches and seizures inside a home without a warrant are presumptively unreasonable."[5] For individuals, an officer's reasonable suspicion of criminal activity can justify a temporary stop for further investigation.[6] If there is probable cause, or even a reasonable articulable suspicion, that an object on a person's possession holds evidence of criminality, law enforcement may seize the object.[7] However, officers must obtain a warrant before they can search inside and examine the contents.[8] A vehicle, on the other hand, may be searched without a warrant if there is probable cause to believe it contains evidence of criminality.[9]

To get a warrant, the U.S. Federal Rules of Criminal Procedure (FRCP) provide that law enforcement officers must present a written application to a judge or magistrate, demonstrating "probable cause" that evidence of a crime can be found in a particular location.[10] The application must detail the suspected crimes, describe the intended search area, and identify the evidence sought, meeting the Fourth Amendment's requirement that warrants "particularly describ[e] the place to be searched, and the persons or things to be seized."[11] To establish probable cause, the magistrate must be persuaded that "there is a fair probability that contraband or evidence of a crime will be found in a particular place."[12]

In the absence of a warrant, a search is "only reasonable if an exception to the warrant requirement applies."[13] Exceptions include when consent is given,[14] if there is an urgent need for

---

[2] Dylan Bonfigli, *Get A Warrant: A Bright-Line Rule for Digital Searches Under the Private-Search Doctrine*, 90 S. CAL. L. REV. 307, 312 (2017) (available here).
[3] *Id.* at 311.
[4] *What Does the Fourth Amendment Mean?*, U.S. COURTS (last visited Nov. 27. 2023), https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0.
[5] *Id*. (citing Payton v. New York, 445 U.S. 573 (1980))
[6] *Id*. (citing Terry v. Ohio, 392 U.S. 1 (1968); Minnesota v. Dickerson, 508 U.S. 366 (1993)).
[7] Bonfigli, *supra* note 2.
[8] *Id.*
[9] What Does the Fourth Amendment Mean?, *supra* note 4 (citing Arizona v. Gant, 129 S. Ct. 1710 (2009)).
[10] FED. R. CRIM. PROC. 41.
[11] U.S. CONST. amend. IV.
[12] Bonfigli, *supra* note 2 at 312 (quoting Illinois v. Gates, 462 U.S. 238, 255 (1983)).
[13] Bonfigli, *supra* note 2 at 312.
[14] *See, e.g.*, Schneckloth v. Bustamonte, 412 U.S. 218 (1973) (holding warrantless search and seizure by officer during traffic stop was constitutionally valid because subject voluntarily consented to search).

the search (exigent circumstances),[15] or the items are in plain view.[16] In the context of electronics, the plain view exception only gives legal authority to *seize* the device, however; it does not give authority to *search* it.[17]

When evaluating the reasonableness of an exception, courts must weigh the person's privacy rights against legitimate government interests, such as public safety.[18] The more intrusive the search on individual privacy, the heavier the government's burden to justify the intrusion. Generally, if no exception to the warrant requirement applies, evidence obtained from warrantless searches and seizures must be suppressed under the exclusionary rule.[19]

The Fourth Amendment, created to oversee the search of homes and physical evidence seizure, raises the question today: How do these rights apply to the search and seizure of electronic devices and digital data?

1. Search and Seizure of Electronically Stored Information Through Seizure of Physical Electronic Devices

Over the past few decades, computers and phones have become an increasingly important source of evidence in criminal investigations due to their capacity to document and retain vast amounts of user data.[20] The process of retrieving evidence from an electronic device is known as computer forensics. This process, typically conducted by a trained analyst in a government lab, involves combing through the device's contents after its seizure to find evidence. A range of software programs can be used to aid the lengthy process of data search, which can span from days to weeks, enabling the discovery of specific information that may prove the suspected crime, or sometimes revealing evidence of an unrelated crime. Given the intrusive nature of computer forensics, which involves sifting through immense data to find evidence, it becomes clear why obtaining warrants and ensuring their specificity before searching electronic devices is critical.

As devices like smartphones and laptops store substantial personal information, a warrant must define what and where to search within an electronic device.[21] In this vein, the U.S. Supreme Court, in the landmark case *Riley v. California* (2014), recognized the significant privacy concerns associated with modern cell phones and ruled that warrantless searches of their digital contents at the time of an arrest are unconstitutional.[22]

---

[15] *See*, *e.g.*, Warden v. Hayden, 387 U.S. 294 (1967) (holding the exigencies of a situation may make a warrantless entry and subsequent search imperative and thus permissible under the Fourth Amendment).
[16] *See*, *e.g.*, Arizona v. Hicks, 480 U.S. 321 (1987) (holding the plain view doctrine permits warrantless searches and seizures where the police have probable cause to believe the item at issue is contraband or evidence of a crime).
[17] U.S. Secret Service, Best Practices for Seizing Electronic Evidence: A Pocket Guide for First Responders 9 (2007) [hereinafter Best Practices].
[18] U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 2 (citing Katz v. United States, 389 U.S. 347, 361 (1967)) [hereinafter DOJ].
[19] Bonfigli, *supra* note 2, at 311.
[20] Orin S. Kerr, *Searches and Seizures in A Digital World*, 119 Harv. L. Rev. 531, 537–38 (2005).
[21] *Id*. at 572–73.
[22] *See* Riley v. California, 573 U.S. 373, 401 (2014).

Following his arrest for driving with expired registration, David Riley's cell phone was searched without a warrant, leading to additional charges related to a prior shooting based on the information retrieved.[23] The government's reliance on the search-incident-to-arrest doctrine, which traditionally granted law enforcement considerable discretion to search any containers on a person upon legal arrest, was rejected by the Court, finding that the exception's purposes—officer safety and evidence preservation—do not apply to the digital context of cell phones.[24] First, digital data stored in a cell phone cannot itself be used as a weapon to harm officers, nor can it facilitate an escape; thus, inspecting a phone's digital content does not prevent physical threats.[25] Second, once the cell phone is secured and in police custody, there is no longer a threat that the arrestee will destroy the evidence, negating the second rationale for warrantless searches under the doctrine.[26] Though remote wiping or encryption can block access to the cell phone data, law enforcement can counter these by responding in a targeted manner to urgent threats or by disabling the phone's locking mechanism to secure the evidence.[27]

The Court further recognized that the privacy implications of modern cell phones exceed those related to the search of physical items such as "cigarette pack[s], [] wallet[s], or [] purse[s]."[28] The vast storage capacity of cell phones means they hold a wealth of various types of personal data—"millions of pages of text, thousands of pictures, or hundreds of videos"—all of which can chronicle years of a person's life.[29] This aggregation of information, accessible in one place, can reveal "much more in combination than any isolated record."[30] Because cell phones differ "in both a quantitative and a qualitative sense" from other objects that might be carried on an arrestee's person, a far more substantial set of privacy interests is at play, warranting stricter scrutiny and protections.[31]

The Supreme Court's stance in *Riley* signaled a trend towards favoring privacy interests in digital information and suggests that it will not formalistically apply traditional Fourth Amendment exceptions to digital searches, especially when there is little justification for warrantless searches.[32] But while *Riley* addresses the important constitutionality issue of warrants related to digital data, what does it mean to actually "search" digital data, and when is that data "seized"?

In data search and seizure involving electronic devices, two scenarios typically arise: first, the seizure of a cell phone by law enforcement, necessitating a search warrant before they can look through the phone's content, as was the case in *Riley*.[33] The second scenario involves creating a bitstream copy of the phone's data after seizure (instead of looking through the original device), a process that duplicates and creates an identical image of the contents of the original device. Creating a bitstream copy is not considered a seizure as it does not "meaningfully interfere" with

---

[23] *Id.* at 379.
[24] *Id.* at 403.
[25] *Id.* at 387–88.
[26] *Id.* at 388–91.
[27] *Id*. at 378–90.
[28] *Riley*, 573 U.S. at 393.
[29] *Id.* at 394.
[30] *Id.*
[31] *Id*. at 393.
[32] *Fourth Amendment*, ELEC. PRIV. INFO. CTR. (last visited Dec. 4, 2023), https://epic.org/issues/privacy-laws/fourth-amendment/.
[33] *Riley*, 573 U.S. at 373.

the owner's possessory interests in the data.[34] The act of searching occurs when the copied data is "exposed to human observation," at which point the Fourth Amendment considerations are implicated.[35]

Given the vast volume of data on electronic devices, FRCP Rule 41(e)(2)(B) acknowledges the impracticality of reviewing the extensive data on-site, so it establishes a two-step process where a warrant may authorize officers to first seize or copy the storage medium, and then review it later for relevant information.[36] The term "electronically stored information" encompasses a wide range of data types, including "writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained."[37] The description is "intended to cover all current types of computer-based information and to encompass future changes and developments."[38]

Moreover, federal guidelines for handling digital evidence and electronic devices stress the importance of following specific protocols to preserve the evidence's integrity and the chain of custody.[39] A warrant must include language specific to both the seizure and the search (i.e. the forensic examination) of the device.[40] Only qualified personnel, ideally specialized forensic examiners, should process the device, which needs to be disconnected from any network and powered off to prevent external interference.[41] Additionally, the collection, transfer, and storage of digital evidence must be rigorously documented to maintain a clear chain of custody up to the final destination.[42]

2. Search and Seizure of Electronically Stored Information Through Remote Access

To adapt to new technologies and advancements in the digital age, FRCP Rule 41 was amended in 2016 to allow remote access to electronic storage media for searching and seizing electronically stored information.[43] Specifically, paragraph (b)(6) empowers a magistrate judge to authorize remote searches and seizures where the data has been "concealed through technological means," irrespective of its physical location.[44] This amendment complements the

[34] *See* Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700, 703 (2010) (arguing copying data constitutes a Fourth Amendment seizure "when copying occurs without human observation and interrupts the course of the data's possession or transmission"). Supreme Court precedent has previously found analogous seizures of copies "did not 'meaningfully interfere' with respondent's possessory interest[s]" in the material in question, as in the case of an officer copying down the serial numbers of stolen stereo equipment in the defendant's apartment. *See* Arizona v. Hicks, 480 U.S. 321, 324 (1987).
[35] Bonfigli, *supra* note 2; Kerr, *supra* note 20, at 535.
[36] FED. R. CRIM. PROC. 41(e)(2)(B).
[37] *See*, *e.g.*, FED. R. CIV. PROC. 34(a) (establishing this definition of "electronically stored information" (ESI), which the Advisory Committee on the Federal Rules of Criminal Procedure gives equal effect to in Rule 41 in its Committee Notes on Rules – 2009 Amendment).
[38] CHARLES ALAN WRIGHT & ARTHUR R. MILLER, 3A FED. PRAC. & PROC. § 670 (4th ed.) (citing Fed. R. Crim. P. 41(e)(2)(B) Advisory Committee's notes found in Appendix A., 3A Fed. Prac. & Proc.) (Advisory Committee Notes are explanatory rules that accompany new or amended federal rules. These notes are prepared by the Advisory Committee on the respective rules and provide guidance on the intended application and interpretation of the rule).
[39] BEST PRACTICES, *supra* note 17.
[40] *Id.* at 10.
[41] *Id*.
[42] *Id*.
[43] WRIGHT & MILLER, *supra* note 38.
[44] FED. R. CRIM. P. 41(b)(6).

federal data privacy statutes, Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA), establishing a framework for remote digital investigations.[45]

The ECPA and SCA specify how and under what circumstances service providers, like internet service providers (ISPs) or email services, can legally share user data with the government, with respect to electronic communications and stored communications data, respectively. These laws require the government to present appropriate legal documents such as warrants, subpoenas, or court orders to the service providers before user data can be disclosed.[46] While the ECPA and SCA govern data disclosure from service providers, Rule 41(b)(6) directly addresses the retrieval process of concealed data, streamlining search and seizure operations in the digital realm. Because of this regulation of data, the ECPA and SCA may become relevant in Fourth Amendment cases involving technology.

However, it is important to note that the ECPA and SCA's applicability is limited to service providers sharing user data. For instance, law enforcement may not need a warrant to access messages shared with a third party if the third party consents to share them.[47] The third-party doctrine is a legal principle that suggests that individuals have no reasonable expectation of privacy when it comes to information voluntarily given to third parties.[48] Hence, if an individual shares information with someone else or some entity (like a bank, telephone company, or even social media platforms), the doctrine holds that they have implicitly forfeited their reasonable expectation of privacy over that information, and it can be obtained by law enforcement without a warrant.[49]

In *Carpenter v. United States* (2018), the Supreme Court challenged the longstanding third-party doctrine, establishing that police must still secure a warrant to access extensive cell phone location records.[50] The case centered on Timothy Carpenter, a suspect in a series of robberies.[51] Prosecutors obtained court orders under the SCA, which led to the release of Carpenter's "cell-site location information" (CSLI) from telecom providers, revealing his movements during the time of the crimes and connecting him to the offenses.[52] These records, kept by wireless carriers which detail a user's movements, were traditionally accessible to law enforcement only with a court order, but without a warrant, relying on the third-party doctrine.[53] This was based on the assumption that individuals consented to share this data by choosing to use their cell phone services.[54] However, the Court acknowledged that intimate details such as location data could reveal much about an individual's life over time, and affirmed that people have a reasonable

---

[45] Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (1986); Stored Communications Act (SCA), 18 U.S.C. §§ 2701 et seq.
[46] ECPA, *supra* note 45.
[47] Sara Morrison, *The police want your phone data. Here's what they can get — and what they can't*, Vox (Oct. 21, 2020), https://www.vox.com/recode/2020/2/24/21133600/police-fbi-phone-search-protests-password-rights.
[48] *See generally* Orin Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 (2009); *see also* Bonfigli, *supra* note 2.
[49] *Id*.
[50] *See* Carpenter v. United States, No. 16–402, slip op. at 15 (S. Ct. 2018).
[51] *Id*. at 1–4.
[52] *Id*.
[53] *Id*.
[54] *Id*.

expectation of privacy concerning their long-term movements.[55] Consequently, the Court determined that the acquisition of this type of sensitive data is a Fourth Amendment search and therefore requires a warrant.[56]

Until *Carpenter*, the SCA provided a much lower standard for the government to satisfy to be able to conduct searches and seizures of such data, and the Court reinterpreted the law to find these searches, the acquisition of this data, must be held to the same standard as any Fourth Amendment search. *Carpenter* marks a major strengthening of Fourth Amendment protections of digital data under U.S. federal law.

Another layer of concern exists regarding password protected cell phones. Assuming there is a warrant permitting the search of a smartphone but the government is unable to bypass encryption, does that mean the phone owner has to disclose their password? It depends.

### *B. Self-incrimination and the Fifth Amendment*

The Fifth Amendment provides in part that no person "shall be compelled in any criminal case to be a witness against himself."[57] This provision of the Fifth Amendment ensures that individuals cannot be forced to provide testimony that may incriminate themselves, with "testimony" typically understood as "revealing content of [one's] own mind."[58] Not all personal knowledge or information would fall under this protection; for instance, physical evidence like a key to a lock may be required to be turned over, contrasting with the knowledge of a lock combination, which may be protected.[59] Consequently, this distinction can offer protections to smartphone users, as the Fifth Amendment may shield them from the obligation to disclose their phone's password in legal proceedings.[60]

When it comes to phone passwords, the government may argue for the application of the "foregone conclusion exception."[61] This exception applies when the government can independently confirm the existence of incriminating evidence on a device and establish that the individual owns the phone.[62] If these conditions are met, entering the password is considered non-testimonial because it does not tell the government anything new; it simply demonstrates that the individual knew the password.[63]

Courts across the United States are divided on whether compelling a suspect to unlock their cell phone violates the Fifth Amendment's protection against self-incrimination, and when the

---

[55] *Id*. at 15.
[56] *Id*.
[57] U.S. CONST. amend. V.
[58] Morrison, *supra* note 47.
[59] *Our Fifth Amendment Rights*, MAXEY LAW OFFICES PLLC (Jul. 28, 2021), https://www.maxeylaw.com/blog/2021/july/our-fifth-amendment-rights/#:~:text=Our%20Fifth%20Amendment%20Rights&text=In%20most%20cases%2C%20a%20defendant,role%20in%20finding%20a%20verdict.
[60] Andrew Edmonson, *Password Unprotected: Compelled Disclosure of Cellphone Passwords and the Foregone Conclusion Exception*, 48 RUTGERS COMPUT. & TECH. L.J. 117, 120 (2021).
[61] *Id*.
[62] *Id*.
[63] *Id*; *see also* Urooba Abid, *Police Should Not Be Allowed to Compel Our Cell Phone Passwords*, ACLU (Jun. 22, 2023), https://www.aclu.org/news/privacy-technology/police-should-not-be-allowed-to-compel-our-cell-phone-passwords.

"foregone conclusion exception" can be invoked.[64] The Pennsylvania Supreme Court, in *Commonwealth v. Davis*, ruled that disclosing a passcode is a form of "testimony" and thus protected by the Fifth Amendment.[65] On the other hand, the Illinois Supreme Court, in *People v. Sneed*, ruled that passcodes are not testimonial in nature and thus do not fall under the Fifth Amendment's protections, viewing them as a mere sequence of numbers memorized by the user with minimal independent value.[66] On the federal side, the United State Court of Appeals for the Third Circuit Court ruled that a defendant can be compelled to unlock password-protected devices even if they claim to have forgotten the passwords, whereas the Eleventh Circuit Court of Appeals determined that decrypting and revealing a hard drive's contents is testimonial and thus protected by the Fifth Amendment.[67]

But with a valid search warrant in hand, law enforcement may be able to access the contents of a password-protected cell phone without needing to compel the owner to give up their passcode.[68] Across the United States, law enforcement agencies of all sizes have invested heavily in mobile device forensic tools (MDFTs).[69] These tools have three key features: (1) they enable the extraction of extensive amounts of data from cellphones; (2) they organize extracted data into a digestible format for analysis; and (3) they assist in bypassing security measures in order to copy data.[70]

While *Riley* established the fundamental rule that a warrant is required to search the contents of a cell phone post-arrest, the nuances of this requirement, such as the permissible scope of the search and the exceptions to the rule, have been predominantly shaped by state case law.[71]

## III. State Courts' Application of *Riley*

Post-*Riley* decisions at the state level show varying judicial interpretations regarding the scope of cell phone searches.[72] The diversity of state court interpretations, rooted in the American

---

[64] Abid, *supra* note 63.
[65] Andrew Crocker, *Victory: Pennsylvania Supreme Court Rules Police Can't Force You to Tell Them Your Password*, ELEC. FRONTIER FOUND. (Nov. 20, 2019), https://www.eff.org/deeplinks/2019/11/victory-pennsylvania-supreme-court-rules-police-cant-force-you-tell-them-your (citing Commonwealth v. Davis, 656 Pa. 213, 235 (Pa. 2019)).
[66] *EFF to Supreme Court: Fifth Amendment Protects People from Being Forced to Enter or Hand Over Cell Phone Passcodes to the Police*, ELEC. FRONTIER FOUND. (Nov. 16, 2023), https://www.eff.org/press/releases/eff-supreme-court-fifth-amendment-protects-people-being-forced-enter-or-hand-over#:~:text=%E2%80%9CWhenever%20the%20government%20calls%20on,%E2%80%94the%20Fifth%20Amendment%20applies.%E2%80%9D (citing People v. Sneed, 2023 IL 127968, 82 (Ill. June 15, 2023)).
[67] Morrison, *supra* note 47 (citing United States v. Apple MacPro Computer, 851 F.3d 238, 247 (3d Cir. 2017); In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1341 (11th Cir. 2012)).
[68] *Id*.
[69] Logan Koepke et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*, TEAMUPTURN (Oct. 20, 2020), https://www.upturn.org/work/mass-extraction/.
[70] *Id*.
[71] Jennifer Lynch, *New Federal and State Court Rulings Show Courts are Divided on the Scope of Cell Phone Searches Post-Riley*, ELEC. FRONTIER FOUND. (Oct. 4, 2022), https://www.eff.org/deeplinks/2022/10/new-federal-and-state-court-rulings-show-courts-are-divided-scope-cell-phone.
[72] *Id*.

federalist system, generate a unique legal landscape.[73] This system allows state court judges to establish and apply state-level legal norms reflecting local values, enriching the national body of case law, and sometimes influencing federal standards by offering well-vetted precedents for the Supreme Court to consider.[74]

While the Fourth Amendment's particularity requirement is clear in cases of physical evidence, it becomes more complex when dealing with the elusive nature of electronic data storage.[75] This can pose a challenge for officers to specify what to search beforehand. Consequently, state court rulings differ: some enforce strict search warrant limitations, while others authorize searches permitting police to search the entire phone.[76]

### *A. Regarding Broad Searches*

In the case of *Richardson v. State*, the Court of Appeal of Maryland, the state's highest court (renamed the Supreme Court of Maryland in December 2022), established stringent guidelines for cell phone searches.[77] The case involved Anthony Richardson, who was discovered with a handgun and three cellphones following a school altercation.[78] Police obtained a wide-ranging warrant to search the contents of the cell phone identified as his, which led to evidence of a planned robbery.[79] Richardson, however, challenged the search, arguing the warrant was overly general as it permitted a search for "any and all information" and "any and all data."[80] Upholding the need for specific warrants, the Court ruled that cell phone search warrants must be narrowly defined to search only for data that has a direct connection to the probable cause of the search.[81]

Similarly, in *Oregon v. Mansor*, the Supreme Court of Oregon ruled that while the search warrant was valid and specific enough, it did not permit police to investigate beyond the time frame established by probable cause.[82] When a defendant dialed 9-1-1 due to his toddler's respiratory failure, his subsequent behavior raised suspicions of potential abuse.[83] This suspicion, deemed probable cause, led to a warrant for examining the father's internet searches specifically from the day the incident occurred.[84] Despite this warrant, law enforcement impermissibly extended their search to include months of internet searches, potentially indicating prior child abuse.[85] This overreach led the Supreme Court of Oregon to affirm the defendant's motion to suppress the evidence found outside the warrant's specified timeframe.[86]

---

[73] *See* Comparing Federal & State Courts, U.S. COURTS (last visited Dec. 4, 2023), https://www.uscourts.gov/about-federal-courts/court-role-and-structure/comparing-federal-state-courts.
[74] *Id*.
[75] Kerr, *supra* note 20, at 565; *see* Adam M. Gershowitz, The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches, 69 VAND. L. REV. 585, 590 (2016).
[76] Lynch, *supra* note 71.
[77] *Id*. (citing Richardson v. State, 282 A.3d 98, 104 (Md. 2022)).
[78] *Richardson*, 282 A.3d at 105–06.
[79] *Id.* at 107–08
[80] *Id.* at 108.
[81] *Id.* at 113.
[82] Oregon v. Mansor, 421 P.3d 323, 334 (Or. 2018).
[83] *Mansor*, 421 P.3d at 326–27.
[84] *Id*.
[85] *Id.* at 328.
[86] *Id*. at 333–35.

A New York state trial court, on the other hand, upheld a broad search warrant in *People v. Watkins* that permitted the search of an entire phone, even though the police were looking for a specific video taken at the time of arrest.[87] During Watkins' arrest for carrying a loaded firearm, he was recording the incident on his iPhone.[88] The officers stopped the recording, seized his phone, and subsequently obtained a search warrant, anticipating that the video would provide evidence supporting Watkins' (presumably illegal) possession of the firearm.[89] Despite the obvious location of the footage, a judge granted a search warrant for the phone's entire contents.[90] The county court rejected the defendant's argument that the search should have been limited only to video and audio files, determined that examining the entire phone was justified to identify potential evidence related to the "observed criminality."[91]

In other cases, courts have turned to the good faith exception to admit the evidence, regardless of the validity of the warrant. In *United States v. Morton*, the Court of Appeals for the Fifth Circuit declined to weigh in on a broad search, finding that the "good faith exception" applied.[92] During a traffic stop, state troopers arrested Brian Morton for drug possession and seized three cell phones from his car.[93] Despite only having evidence to support a charge for simple possession, officers applied for a search warrant alleging drug trafficking, a more serious offense, to gain extensive access to Morton's phones.[94] A judge granted the warrant, which led to the discovery of child pornography during the phone search and a subsequent warrant.[95] Morton challenged the original warrant, claiming the search exceeded the evidence for the alleged offense and lacked probable cause.[96]

A panel of judges from the Fifth Circuit initially agreed in part with Morton, determining that while there was probable cause to search his phone's contacts, call logs, and texts as stated in the affidavits, no probable cause existed to search the photos, as the police did not demonstrate their relevance to a simple possession crime under investigation.[97] The panel also ruled that the "good faith exception"—stating that evidence should not be suppressed if law enforcement obtains it in good-faith reliance on a warrant—did not apply, since the officers should have known that searching digital images on the defendant's phone related to drug trafficking lacked probable cause.[98] However, the Fifth Circuit's *en banc* panel, instead of evaluating whether the police had probable cause to search the entirety of the phone's contents, chose to find that the officers reasonably believed their warrant was valid, and applied the "good faith exception" to sanction the search of the photos.[99] The dissenting judges disagreed, highlighting the invasive nature of searching a cell phone compared to a "self-contained search of a pocket, compartment, or

[87] Gershowitz, *supra* note 75, at 602 (citing People v. Watkins, 994 N.Y.S.2d 816, 818 (N.Y. Sup. Ct. 2014)).
[88] *Watkins*, 994 N.Y.S. at 817.
[89] *Id.*
[90] *Id.* at 817–18.
[91] *Id.* at 818.
[92] Lynch, *supra* note 71 (citing United States v. Morton, 46 F.4th 331, 339 (5th Cir. 2022)).
[93] *Morton*, 46 F.4th at 334.
[94] *Id.*
[95] *Id.*
[96] *Morton*, 46 F.4th at 336–38.
[97] *Id*. at 338.
[98] *Id*. at 339.
[99] *Id*.

bag."[100] Citing the warrant's reliance on "sweeping generalizations," they argued that the "good faith exception" should not have been applicable.[101]

### *B. Regarding Warrantless Searches*

Despite the *Riley* decision that the search-incident-to-arrest exception does not apply to cell phones, certain circumstances may still allow warrantless searches.[102] State courts have identified multiple grounds on which police do not need a warrant to search the cell phone data of criminal justice-involved individuals.[103] These exceptions include the abandonment doctrine, probationer search exception, scenarios not considered "searches" for Fourth Amendment purposes, parolee search exception, private citizen search doctrine, exigent circumstances exception, plain view doctrine, and third party doctrine.[104]

Relying on the exigent circumstances exception,[105] the Court of Appeals of Washington in *State v. Samalia* found that "defendant's cell phone data could be searched by police under *Riley* without a warrant because defendant abandoned the cell phone in a stolen vehicle while fleeing the police."[106] The court differentiated this from Riley, noting that the phone—which was subsequently used to locate the escaping suspect—was not seized directly from Samalia but was left in a vehicle he had abandoned, thereby negating his privacy interest in the phone.[107]

The Court of Appeals of Louisiana, in turn, relied on the "private citizen search doctrine" in *State v. Rousset*, finding *Riley* inapplicable "because private citizens conducted the initial warrantless search of the cell phone."[108] In this case, the defendant left his phone unattended and after several private citizens found images associated with child pornography on his phone, the phone was handed to law enforcement, leading to Rousset's arrest.[109] The court reasoned that *Riley* "did not apply to the exchange or sharing by the citizens of the phone and these images with law enforcement."[110]

Moreover, "in *State v. Hill*, the Court of Appeals of Georgia found that *Riley* was inapplicable because police did not search defendant's cell phone under the Fourth Amendment."[111] "Rather, police in *Hill* merely placed a call from the phone in order to discover identifying information about the phone's owner who had left the phone in a taxi before departing without paying."[112] The court concluded that because Hill had no reasonable expectation of privacy in the

---

[100] *Id.* at 342.
[101] *Id*.
[102] Christopher D. Totten, *Do Officers Really Need A Warrant to Search Cell Phone Digital Data?: A Content Analysis Study of Significant State Court Interpretive Cases for* Riley v. California, 58 No. 6 Crim. Law Bulletin ART 4 (2022).
[103] *Id*.
[104] *Id*.
[105] An exception for emergency circumstances, such as when a suspect may flee. *See* Totten, *supra* note 102.
[106] *See* State v. Samalia, 344 P.3d 722 (Wash. Ct. App. 2015).
[107] Totten, *supra* note 102 (citing State v. Samalia, 344 P.3d at 726).
[108] *Id.* (citing State v. Rousset, 2020-0202 (La. App. 4 Cir. 6/3/20)).
[109] *Id.* (citing State v. Rousset, 2020-0202 (La. App. 4 Cir. 6/3/20)).
[110] *Id.* (citing State v. Rousset, 2020-0202 (La. App. 4 Cir. 6/3/20)).
[111] Totten, *supra* note 102.
[112] *Id.*

information at issue—his own name, date of birth, and phone number—there was no search under the Fourth Amendment.[113]

## IV. Concluding Observations

The foregoing examination of U.S. federal law and state court rulings reveals a wide spectrum of views on the required specificity in search warrants and the extent to which courts tolerate broad searches of electronic devices. Countries updating their search and seizure laws in this respect might consider certain protective aspects of the U.S. legal framework, which generally emphasizes warrants for digital searches, specific warrant criteria for privacy protection, and defined exceptions for warrantless searches, aiming to balance individual privacy and the needs of law enforcement in the digital age.

Although Supreme Court decisions set binding constitutional interpretations nationwide, they still leave some questions on technology in this realm unanswered, leaving room for state-level discretion and interpretation. Although a unanimous Supreme Court said in *Riley* that the approach to cell phone privacy was "simple–get a warrant," the actual process is far from simple, as the Court did not articulate the standards limiting the scope of such searches after the warrant is issued.[114] Consequently, states must comply with the warrant requirement but often circumvent it by issuing broad search warrants, potentially overlooking the "heightened privacy concerns" contemplated by *Riley*.[115]

For example, some state courts have issued warrants that improperly authorize the police to comb through "any and all data" on a phone.[116] A good illustration is *People v. Watkins*, where a New York court upheld a search warrant for "all data" on the phone, even though police were looking for a specific piece of evidence located in the phone's library.[117] While in some cases, broad language can be justifiable— particularly if there's a chance the suspect concealed or mislabeled evidence—this language may not make sense when the evidence's precise location is already known.[118] But even if the particularity problem posed by broad warrants is recognized, some courts have upheld defective warrants, where the execution of the broad warrant was likely found to be in good faith.[119] In *United States v. Morton*, the Fifth Circuit *en banc* panel, instead of evaluating whether there was probable cause to search the entirety of the phone's contents, chose to consider whether the officers reasonably believed their warrant was valid.[120]

While some courts are lenient with broad search scopes, others have enforced strict limits on warrants, in line with *Riley's* emphasis on privacy rights concerning cell phones.[121] In *Richardson*, Maryland recognized that "the privacy concerns implicated by cell phone storage

---

[113] *Id*. (citing State v. Hill, 789 S.E.2d 317, 320 (Ga. Ct. App. 2016)).
[114] *Riley*, 573 U.S. at 403.
[115] *Id*. at 393 ("A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.").
[116] Gershowitz, *supra* note 75, at 602 (citing Moore v. State, 160 So. 3d 728, 731 (Miss. Ct. App. 2015)).
[117] *Watkins*, 994 N.Y.S. at 818.
[118] Gershowitz, *supra* note 75, at 608.
[119] Lynch, *supra* note 71.
[120] *Morton*, 46 F.4th at 339.
[121] Lynch, *supra* note 71.

capacity and the pervasiveness of cell phones in daily life do not fade away when police obtain warrants to search cell phones."[122] The court acknowledged the lack of a universal approach to cell phone warrants, but emphasized the need for officers and judges to limit search discretion to reasonably protect the phone owner's privacy.[123] Effective measures include setting time limits, specifying searchable apps, or defining clear search protocols. The Court of Appeals emphasized that warrants must be sufficiently detailed, allowing officers to only search for items directly related to the probable cause of the search.[124] In *Mansor*, Oregon also implemented stringent protections, recognizing that a warrant "must be sufficiently specific in describing the items to be seized and examined that the officers can, 'with reasonable effort ascertain' those items to a 'reasonable degree of certainty.'"[125] Moreover, even if the warrant is specific, it must not authorize a search that is "broader than the supporting affidavit supplies probable cause to justify."[126]

In sum, the patchwork of judicial interpretations across jurisdictions reflects the complexity of applying the Supreme Court's guidance from *Riley* to protect cell phone privacy. While some courts have issued overbroad warrants, which deviate from the intent of *Riley*, others have aligned more closely with its principles, imposing stringent requirements for the specificity of warrants to safeguard privacy rights. Notably, jurisdictions like Maryland and Oregon have adopted measures that mirror *Riley*'s concern for heightened privacy in digital contexts, by demanding detailed warrant parameters and limiting search scope. These practices affirm the imperative of applying the Fourth Amendment's particularity requirement to digital searches with the same vigor as traditional searches.[127] The evolution towards a more consistent legal standard hinges on further clarification from higher courts, which would ensure that *Riley*'s protective measures for cell phone privacy are uniformly respected.

[122] *Richardson*, 282 A.3d at 104.
[123] *Id.* at 123.
[124] *Id.* at 104.
[125] *Mansor*, 421 P.3d at 339.
[126] *Id.* at 339–40.
[127] For an alternative approach to digital privacy rights under the Fourth Amenmdnet, *see* ORIN KERR, THE DIGITAL FOURTH AMENDMENT: PRIVACY AND POLICING IN OUR ONLINE WORLD (2025) (advocating for broad search warrants but strict prohibitions on the use of non-responsive data).