PHYSICAL FRUITS VS. DIGITAL FRUITS: WHY *PATANE* SHOULD NOT APPLY TO THE CONTENTS OF DIGITAL DEVICES

Abbey Flynn†

Abstract

A police officer asks a person in custody to unlock their cellphone and hand it over so the officer can look at its contents. This simple interaction—which happens more and more often as cellphones dominate modern life—implicates three different constitutional doctrines. Riley v. California *dictates that the officer must get a warrant or consent to search the cellphone. And* Miranda v. Arizona *requires that the officer inform the person of their right to remain silent before questioning them. But many might not realize that this scenario also implicates* United States v. Patane, *the case allowing admission of physical evidence found in violation of* Miranda. *And as currently interpreted,* Patane *means that even if an officer purposely violates* Miranda, *the contents of the device will likely be admissible in court.*

The Court decided Patane *before Americans became dependent on cellphones and computers for nearly every aspect of their personal and professional lives. As courts begin to apply* Patane *to the contents of digital devices that law enforcement officers unlock due to a* Miranda *violation, police have an even greater incentive to flout* Miranda, *just as the dissenting justices in* Patane *feared. And in the quick interactions police officers use to gain access to cellphones, the Fifth Amendment question implicated by* Miranda *and* Patane *is intertwined with the Fourth Amendment question from* Riley*—meaning weak Fifth Amendment protections for contents on cellphones due to Patane can help police evade the warrant requirement imposed by* Riley.

This article argues that Patane *should not apply to the contents of digital devices due to the vast difference between the traditional physical evidence examined in* Patane *and evidence found on cellphones and computers. This article also provides arguments advocates can use when arguing that* Patane *should not apply to the contents of digital devices.*

---

† J.D., University of California, Berkeley, School of Law, 2020; B.A., Haverford College, 2014. Many thanks to Professor Orin Kerr of Berkeley Law for his guidance, encouragement, and feedback as I developed this article. Thanks also go to Karun Tilak for his review of multiple drafts of this article. Finally, thank you to the editors and peer reviewers at the Illinois Journal of Law, Technology & Policy for all of their feedback and edits.

TABLE OF CONTENTS

I. INTRODUCTION

Every day across the country, law enforcement officers ask people to unlock their digital devices, hoping to access digital evidence in investigations ranging from low-level misdemeanors to complicated conspiracies. The Fourth Amendment provides some clear limitations on law enforcement—like the presumption that searching a cellphone's contents requires a warrant.[1] But the Supreme Court has yet to weigh in on Fifth Amendment protections for digital devices.[2] Two main Fifth Amendment questions exist. First, how does *Miranda v. Arizona* apply when police ask someone to unlock a digital device?[3] And second, if a *Miranda* violation exists, can prosecutors nonetheless admit the digital contents of the device under the physical fruits exception to *Miranda*'s

1. *See* Riley v. California, 573 U.S. 373, 403 (2014) (holding that a search of cellphone contents does not fall within the "search incident to arrest" exception to the warrant requirement).

2. This article uses the terms "Fifth Amendment" and "Self-Incrimination Clause" interchangeably. References to the Fifth Amendment only refer to the portion of the amendment addressing self-incrimination, which states that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. CONST., amend. V.

3. Miranda v. Arizona, 384 U.S. 436 (1966); *see infra* notes 23–24.

exclusionary rule, as established in *United States v. Patane*?[4] This article will address the latter question.

Whether *Patane* applies to the contents of digital devices has serious ramifications for police conduct, the outcome of criminal cases, and civil liberties. As currently read, *Patane* allows police officers to intentionally ignore *Miranda* when seeking physical evidence.[5] While concerning in cases involving purely physical evidence like guns or drugs, the *Patane* plurality becomes especially alarming in the context of digital devices. After all, digital devices contain a "cache of sensitive personal information" pertaining to every aspect of a person's life, revealing much more than a single physical object.[6] But a person in custody and questioned by police likely does not understand that the Fifth Amendment may protect the act of unlocking a cellphone or a statement communicating the passcode, and can feel pressured to give police access to a phone. And the request to unlock a device often also comes with a request to search the device. Consenting to that search allows officers to evade the warrant requirement from *Riley*.[7] And the dissent in *Patane* characterized the plurality opinion as an "unjustifiable invitation to law enforcement officers to flout *Miranda* when there may be physical evidence to be gained."[8] In the context of digital devices, police can gain more than physical evidence: they can gain access to a digital log of a person's life.

The consequences extend beyond the Fifth Amendment implications. Police can use this consent-based search of a phone to access materials well beyond what a warrant would allow them to see.[9] The result is unfiltered access to every aspect of a person's life, and given this amount of information, police have every incentive to purposefully violate *Miranda*. Despite those serious consequences, courts have largely ignored the differences between digital evidence and purely physical objects when assessing whether *Patane* applies to the contents of digital devices.[10] Currently, if a court equates the contents of digital devices with physical objects, it does not even need to rigorously analyze

4. United States v. Patane, 542 U.S. 630, 645 (2004). Orin Kerr initially raised this question in a 2016 Washington Post opinion piece. Orin Kerr, *When 'Miranda' Violations Lead to Passwords*, WASH. POST (Dec. 16, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/12/12/when-miranda-violations-lead-to-passwords. Kerr provides commentary on United States v. Ashmore, No. 2:16-CR-20016, 2016 U.S. Dist. LEXIS 185939 (W.D. Ark. Dec. 7, 2016). In *Ashmore*, police obtained passwords in violation of *Miranda*. *Id.* at *16. The court excluded the passwords themselves but admitted the contents of the devices under the independent source doctrine. *Id.* at *16–17. Kerr argued that the court reached the right result in admitting the contents but that the court should have reached that result under *Patane* instead of the independent source doctrine. *See also* Orin S. Kerr, *Two New Cases on Decrypting Locked Devices*, REASON (Apr. 9, 2018, 12:51 AM), https://reason.com/volokh/2018/04/09/two-new-cases-on-accessing-encrypted-dev/ (discussing a magistrate judge's analysis of *Patane* in a case involving cellphone contents).

5. *Patane*, 542 U.S. at 647 (Souter, J., dissenting).

6. Riley v. California, 573 U.S. 373, 395 (2014).

7. *See* Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) ("It is . . . well settled that one of the specifically established exceptions to the requirements of both a warrant and probable cause is a search that is conducted pursuant to consent.").

8. *Patane*, 542 U.S. at 647 (Souter, J., dissenting).

9. *See* Marron v. United States, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another.").

10. *See infra* Part III.

whether *Miranda* applies, as a court could state that *Patane* allows admission regardless of whether there is a *Miranda* violation.[11] But a closer examination of the fractured plurality in *Patane* shows that, while *Patane* applies to objects like guns or drugs, the decision should not bar exclusion of highly personal records, like digital data.[12] Further, the Supreme Court should explicitly address developments in technology in its Fifth Amendment and *Miranda* doctrine, like it has done for the Fourth Amendment.[13] Until courts enforce protections in digital device cases—either through the existing *Patane* doctrine or through adapting Fifth Amendment doctrine to address technology—law enforcement will flout *Miranda* in cases involving digital devices.

This article will begin in Part II by explaining the entanglement between the Fourth and Fifth Amendment in cases involving digital devices. This part will explain how the Court has historically entangled the Fourth and Fifth Amendments, and how the entanglement in cases involving digital devices allows police to easily access devices. Part III will provide context on *Patane* and how lower courts have applied *Patane* in the few cases addressing contents of digital devices accessed in violation of *Miranda*.

Part IV will explain options litigators have for arguing that *Patane* should not apply in the new digital landscape. This section explains how rules of criminal procedure have shifted in the face of advances in technology and why *Patane* should follow suit. This section also explains how principles in Fifth Amendment law and the text of *Patane* itself support exclusion of digital evidence gained in violation of *Miranda*. *Marks v. United States*[14] requires a narrower reading of *Patane* that allows for the exclusion of some physical fruits, and the contents of digital devices fit within a long-held notion that intensely private writings and documents require special treatment under the Fifth Amendment.

II. THE ENTANGLEMENT OF THE FOURTH AND FIFTH AMENDMENT IN INVESTIGATIONS INVOLVING DIGITAL DEVICES

Take this scenario: a law enforcement officer detains a person, placing them in custody, but perhaps not in handcuffs yet. That detention means that if the police wish to question the person, the officer must first recite their *Miranda* rights. The average person may not know they have any rights at this point. Even someone familiar with *Miranda* may not recognize that "in custody" can consist of less than being handcuffed and booked into jail.[15] The police officer

11. *See* United States v. Oloyede, 933 F.3d 302, 309 (4th Cir. 2019). In *Oloyede*, the Fourth Circuit cited *Patane* to explain that "even were we to accept [the defendant]'s argument that she made a testimonial communication when she unlocked her phone, it would provide no meaningful help to her defense because the fruit of that voluntary communication, even though made without a *Miranda* warning, would nonetheless be admissible into evidence." *Id*.

12. *See infra* Part IV.

13. *Id*.

14. Marks v. United States, 430 U.S. 188 (1977).

15. Further, even if someone understands when *Miranda* rights are required, they likely will not know what those rights entail. A 2013 study found that the vast majority of Americans cannot freely recall all *Miranda*

asks the person to unlock their cellphone, perhaps even providing an explanation that such a request is standard procedure. The person obliges, not knowing any better, and hands the phone to the officer. With the phone already in hand, the officer asks if he can look at some things on the phone. Not thinking this question has any significance (after all, the officer already has the unlocked phone in his hand), the person says "OK." And with that quick chain of events, the police officer has bypassed both Fourth and Fifth Amendment protections for the contents of the person's device.

That short interaction presents three separate constitutional questions. The first question is a threshold Fifth Amendment question: does an officer's command to unlock a phone violate *Miranda*, which requires an officer to provide warnings when interrogating someone in custody? Even if the officer violates *Miranda*, a second Fifth Amendment issue means that the answer to the first question may not matter. The second question is whether *United States v. Patane*, which allows admission of physical evidence gained in violation of *Miranda*, applies to the contents of the device.[16] And the third question concerns the officer's request to search the phone, a Fourth Amendment question. Although the Supreme Court in *Riley v. California* established that police need a warrant to search the contents of a cellphone, consent negates the need for a warrant.[17]

The first and third constitutional questions—the threshold *Miranda* question and the Fourth Amendment question—have received wide legal discussion in recent years.[18] The first question, concerning how *Miranda* applies when police ask someone to unlock a digital device, has resulted in significant scholarly debate.[19] *Miranda* established the broad proposition that custodial interrogations create a coercive environment, and that the Fifth Amendment requires the exclusion of statements made without warnings designed to correct that coercive environment.[20] The *Miranda* Court also emphasized that Fifth Amendment protections reached beyond the courthouse doors, framing the interrogation as the start of the adversarial process.[21]

---

rights, indicating a need for warnings. Richard Rogers et al., *General Knowledge and Misknowledge of* Miranda *Rights: Are Effective* Miranda *Advisements Still Necessary?*, 19 PSYCHOL. PUB. POL. & L. 432, 439 (2013).

16. Kerr, *supra* note 4.

17. Riley v. California, 573 U.S. 373, 395 (2014); Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

18. *See infra* notes 23–24 for discussion of Fifth Amendment protections for unlocking cellphones.

19. *Id.*

20. Miranda v. Arizona, 384 U.S. 436, 444 (1966). The Court defined "custodial interrogation" as "questioning initiated by law enforcement officers after a person has been taken into custody or otherwise deprived of his freedom of action in any significant way." *Id.* As for the content of the warning, the Court required that "[p]rior to any questioning, the person must be warned that he has a right to remain silent, that any statement he does make may be used as evidence against him, and that he has a right to the presence of an attorney, either retained or appointed." *Id.* The Court wrote that "such a warning is an absolute prerequisite in overcoming the inherent pressures of the interrogation atmosphere." *Id.* at 468. Further, a person can only waive those rights if "the waiver is made voluntarily, knowingly and intelligently." *Id.* at 444.

21. *Id.* at 467–469. The Court wrote that "there can be no doubt that the Fifth Amendment privilege is available outside of criminal court proceedings and serves to protect persons in all settings in which their freedom of action is curtailed in any significant way from being compelled to incriminate themselves." *Id.* at 467. The Court described the pressures of in-custody interrogations and described its holding as necessary "to permit a full opportunity to exercise the privilege against self-incrimination." *Id.* The Court also explained that warnings

Miranda may only apply to certain methods police use to unlock a phone. Police use three main methods to get a person to unlock a phone: (1) asking the person to state the passcode; (2) asking the person to enter the passcode; and (3) using an individual's biometrics to unlock a device.[22] Although there is consensus that asking someone to state a passcode—and in effect provide testimonial information—violates *Miranda*, courts and scholars reach different results about whether asking someone to enter a passcode or using a person's biometrics to unlock a device can violate *Miranda*.[23] Given a split amongst state supreme courts about when unlocking a device—or providing information that will be used to unlock a device—violates *Miranda*, the Supreme Court will need to start providing guidance on how the Fifth Amendment applies in cases involving modern technology.[24]

The Supreme Court addressed the third question of Fourth Amendment protections for the contents of digital devices in *Riley v. California*.[25] The 2014 case established that the search incident to arrest exception does not apply to the contents of cellphones. Chief Justice Roberts, writing for the majority, explained that the rapidly changed role of smartphones in daily life compared to just "a decade ago" required the Court to issue additional protections.[26] He distinguished data on phones from physical records, stating that only now do people "carry a cache of sensitive personal information" as they go about their day, as cellphones contain a digital record of "nearly every aspect" of someone's life.[27]

"may serve to make the individual more acutely aware that he is faced with a phase of the adversary system—that he is not in the presence of persons acting solely in his interest." *Id.* at 469.

22. Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989, 1001–03 (2018).

23. So far, both scholars and courts have reached different outcomes on which methods result in a testimonial act that could be protected by *Miranda* and/or the Fifth Amendment. *See* Bryan H. Choi, *The Privilege Against Cellphone Incrimination*, 97 TEX. L. REV. ONLINE 73, 76–77 (2019) (explaining that different methods of protecting the contents of a digital device lead to different legal protections); *see also* Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203, 225–230 (2018). Generally speaking, courts have found that using an individual's biometrics to unlock a device (such as using FaceID or a fingerprint scanner) do not violate *Miranda*. Stating or writing a passcode is largely seen as violating *Miranda*, since it requires a person to make a statement. Courts have split over the question of whether asking a person to enter their passcode and hand over an unlocked digital device violates the Fifth Amendment. *See infra* note 24. Two state supreme courts have recently reached opposite conclusions on this issue in the compelled decryption context, raising the question of whether the Supreme Court will weigh in on this debate. *Id.*

24. *Compare* Seo v. State, 148 N.E.3d 952 (Ind. 2020) (finding that compelling someone to enter their passcode violates the Fifth Amendment) *with* Commonwealth v. Jones, 481 Mass. 540 (Mass. 2019) (finding that compelling someone to unlock a phone does not violate the Fifth Amendment). As exhibited by *Seo* and *Jone*s, Fifth Amendment issues in law enforcement efforts to access digital devices arise even outside the applicability of *Miranda*. For a discussion of the Fifth Amendment in the compelled decryption context (where a court orders someone to unlock a digital device), *see generally* Orin Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767 (2019). *See also* Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone? A Response to Professor Kerr*, 97 TEX. L. REV. ONLINE 63 (2019).

25. Riley v. California, 573 U.S. 373, 395 (2014).

26. *Id*. The Court decided *Patane* ten years prior to *Riley*.

27. *Riley*, 573 U.S. at 395. The Court has extended Fourth Amendment privacy interests related to cellphones beyond just searches of the devices. In *Carpenter v. United States*, the Court recognized a privacy interest in location information from cell service towers, due to the intimate and expansive nature of the gathered data, which can reveal "familial, political, professional, religious, and sexual associations." Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

But the second constitutional question in the hurdle—whether *Patane* applies to the contents of digital devices—has not received the same attention, even though the answer to the question is intertwined with the other two constitutional questions. In *Patane*, the Court limited *Miranda* by creating a rule that physical evidence gained in violation of *Miranda* is admissible, even if the statement that led to the evidence is not.[28] In the cellphone context, that means the act of unlocking a device or stating a passcode could be suppressed if the police violated *Miranda*, but the contents of the digital device would have no Fifth Amendment protections.[29]

Although the hypothetical presents three distinct legal issues, these three legal issues are intertwined, and the rules for one legal protection affect police action in ways that influence the other legal question. The reality of investigations involving digital devices means that Fourth and Fifth Amendment questions come up together—sometimes in the very same moment. A police officer's request to "please unlock your phone and hand it to me so I can review your text messages" invokes the Fourth and Fifth Amendment issues in one short sentence. But as this article will explain, the Supreme Court has realigned Fourth Amendment protections with changes in technology, without addressing how the Fifth Amendment fits in. As a result, a lack of Fifth Amendment protections can, in everyday police interactions with the public, be used to circumvent Fourth Amendment protections, too.

While Fifth Amendment doctrine has regressed to provide less protection over recent years, Fourth Amendment doctrine has responded to changes in technology and society by expanding protections for digital devices.[30] But the two amendments address similar issues: the limitations on how the government can collect information used for a prosecution. As explained by one scholar, "the Fourth and Fifth Amendments . . . articulate two very different sorts of restraints upon two distinct means of information gathering by the government in the criminal process."[31]

Subsection A will explain the historical entanglement of the Fourth and Fifth Amendments. Subsection B will explain how the Fourth and Fifth Amendments are entangled in present day cases involving the contents of digital devices.

A. The Historical Entanglement (and Attempted Disentanglement) of the Fourth and Fifth Amendments

The Fourth and Fifth Amendment have a long entanglement. Over the history of the Court, this entanglement has, as one scholar put it, "engendered a

28. *Patane*, 542 U.S. at 636.

29. *See, e.g.*, United States v. Hernandez, No. 18-CR-1888-L, 2018 WL 3862017, at *1 (S.D. Cal. Aug. 13, 2018) (concluding that the "[d]efendant's demonstration of her passcode after requesting an attorney is subject to suppression for violation of *Miranda*, but the contents of the phone which were accessed by virtue of the passcode demonstration are not subject to suppression").

30. *See infra* Part IV-A.

31. Richard A. Nagareda, *Compulsion to Be a Witness and the Resurrection of Boyd*, 74 N.Y.U. L. REV. 1575, 1587 (1999).

history wrought with doctrinal confusion and theoretical disarray, which current doctrine has only exacerbated."[32] Prior Supreme Court doctrine explicitly intermingled analysis of the Fourth and Fifth Amendments; now, the Court steers clear of importing rationales or logic used in the analysis of one amendment to the other.[33] But neither of these approaches really gets the issue right. The Fourth and Fifth Amendments are inextricably linked because they are both methods of limiting state power in investigations and prosecutions, but they address two different issues that arise during the course of those investigations and prosecutions.[34] But to imagine that the two do not regularly interact or influence each other is to ignore how the amendments come up in real life.

In the 19th century, the Court linked the Fourth and Fifth Amendments together in *Boyd v. United States*.[35] The Court used the case to espouse on broad principles underlying the Fourth and Fifth Amendments and the interplay between the amendments. The Court explained that the two amendments have an "intimate relationship" and that "they throw great light on each other."[36] Modern-day analysis of the opinion concludes that "[a]mendments overlapped to create an inviolable zone of privacy within which the government could not gather information."[37]

The *Boyd* Court also took an expansive view of what the Fifth Amendment meant, in contrast to the current Court.[38] Specifically, the *Boyd* Court took the Fifth Amendment's language that no one shall be "compelled in any criminal case to be a witness against himself"[39] to mean more than just statements made

32. Michael S. Pardo, *Disentangling the Fourth Amendment and the Self-Incrimination Clause*, 90 IOWA L. REV. 1857, 1858 (2005).

33. *See id.* at 1859 (describing that "[s]ubsequent doctrine has. . . 'sounded the death knell'" for the "fusion of Fourth and Fifth Amendment analysis") (quoting United States v. Doe, 465 U.S. 605, 618 (1984) (O'Connor, J., concurring)).

34. Nagareda, *supra* note 31, at 1587; *see also* Pardo, *supra* note 32, at 1860. Pardo writes that "the self-incrimination privilege applies to a subset of events *within* the universe of potential Fourth Amendment events." *Id*. Here, it is important to clarify what Pardo means when referring to "events." Justice Thomas and other members of the *Patane* plurality might disagree with Pardo's analysis. After all, the *Patane* plurality advances the idea that a violation of the Self-Incrimination Clause occurs when the prosecution introduces evidence at trial; not at the phase of collecting that information. United States v. Patane, 542 U.S. 630, 638 (2004). But speaking in terms of "events" refocuses the conversations to the actual interactions between the police and the public that result in police taking statements and conducting searches. A single interaction between a police officer and a person can result in a police officer collecting an immense amount of evidence, both in the form of statements and physical evidence.

35. Boyd v. United States, 116 U.S. 616, 633 (1886). The *Boyd* Court presented its opinion as far reaching, writing that "[t]he principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life." *Id*. at 630. These principles extended beyond the facts in *Boyd*, which involved the seizure of imported glass due to possible violation of customs laws.

36. *See id.* at 633. The Court elaborated that "the 'unreasonable searches and seizures' condemned in the [F]ourth [A]mendment are almost always made for the purpose of compelling a man to give evidence against himself, which in criminal cases is condemned in the [F]ifth [A]mendment; and compelling a man 'in a criminal case to be a witness against himself," which is condemned in the [F]ifth [A]mendment, throws light on the question as to what is an 'unreasonable search and seizure' within the meaning of the [F]ourth [A]mendment." *Id*.

37. Pardo, *supra* note 32, at 1858.

38. *Boyd*, 116 U.S. at 630.

39. U.S. CONST., amend. V.

at trial. The Court explained that "we have been unable to perceive that the seizure of a man's private books and papers to be used in evidence against him is substantially different from compelling him to be a witness against himself,"[40] emphasizing the importance of privacy in assessing the need for Fifth Amendment protections. This interpretation understandably confused future lawyers and scholars.[41]

The Court later walked back this expansive view—as seen in Justice Thomas's opinion in *Patane*—but for the greater part of the 20th century, the Court still embraced a wider view of the Fifth Amendment than the Court has in the 21st century. In *Miranda* itself, the Court wrote that, "there can be no doubt that the Fifth Amendment privilege is available outside of criminal court proceedings."[42] In *Schmerber v. California*, a Fifth Amendment case from the same year as *Miranda*, Justice Brennan wrote about evidence that would "otherwise provide the State with evidence of a testimonial or communicative nature," indicating that the Fifth Amendment can protect communicative evidence beyond statements in an interrogation.[43] Only in the past few decades has the Court narrowed *Miranda* by describing it as a mere prophylactic, while also limiting the meaning of the Self-Incrimination Clause itself by rejecting *Boyd*'s expansive view of the Fifth Amendment.[44] *Patane* was perhaps the culmination of those efforts.[45]

---

40. *Boyd*, 116 U.S. at 633.

41. *See* Nagareda, *supra* note 31, at 1626–27. Nagareda has suggested that a better approach to disentangling the Fourth and Fifth Amendment is to assess how the evidence is acquired, with the Fourth Amendment protecting evidence that the government can take on its own, and the Fifth Amendment protecting evidence that is produced by a person under investigation. *Id.* For Nagareda, this approach is a more helpful way to distinguish whether the Fourth or Fifth Amendment is at play. *Id*. at 1621. Nagareda compared the police taking a blood sample from someone properly in custody to how the "police might use their own ingenuity to gain access to a safe or a computer hard drive duly seized from [a home]." *Id*. at 1627. For Nagareda, "there is no giving of evidence in any meaningful sense; there is just a taking of evidence by the government-the extracting of the blood sample, the cracking of the safe, or the accessing of the hard drive." *Id*. This same argument applies in the document production context. Nagareda writes that "incriminatory documents do not appear magically in the government's hands; instead, they appear as the result of some act, either by the government unilaterally (a seizure) or by some person (either the individual incriminated by the documents or, conceivably, a third party)." *Id*. at 1626. Anything seized would implicate Fourth Amendment protections, while anything handed over would implicate Fifth Amendment protections. *Id*. Although this theory produces different results for different methods of accessing a digital devices (for example, asking for a passcode as compared to using a person's biometrics to unlock the device), generally speaking, courts have found that different methods of accessing a device implicate different Fifth Amendment protections.

42. *See* Miranda v. Arizona, 384 U.S. 436, 467 (1966) (explaining that the Fifth Amendment "serves to protect persons in all settings in which their freedom of action is curtailed in any significant way from being compelled to incriminate themselves").

43. Schmerber v. California, 384 U.S. 757, 764 (1966).

44. *See* Charles D. Weisselberg, *Saving Miranda*, 84 CORNELL L. REV. 109, 111 (1998) (arguing that the language of *Miranda* as a prophylactic grew only out of the dissenting judges in *Miranda*, while the majority tied *Miranda* directly to the Fifth Amendment). *See also* Donald A. Dripps, *Miranda for the Next Fifty Years: Why the Fifth Amendment Should Go Fourth*, 97 BOST. UNIV. L. REV. 893, 901–02 (2017) (arguing that the *Miranda* exclusionary rule resembles the bright-line rules in the Fourth Amendment context, where justices and scholars are comfortable with simultaneously under- and over-protective rules in order to give police officers clear guidance).

45. *See* Sandra Guerra Thompson, *Evading Miranda: How Seibert and Patane Failed to "Save" Miranda*, 40 VAL. U. L. REV. 645, 650 (2006) (explaining that *Patane* and Missouri v. Seibert, 542 U.S. 600 (2004), "presented the perfect opportunities for the Court to put a stop to deliberate violations of *Miranda*, but the decisions do exactly the opposite").

Though courts try to keep the rationales for—and analyses of—the two amendments separate to avoid a resurrection of *Boyd*, courts still jumble together concepts from the Fourth and Fifth Amendment, showing the difficulty in completely disentangling the two doctrines. For example, in *United States v. Djibo*, an Eastern District of New York case involving a cellphone accessed thanks to a *Miranda* violation, the court cited *Riley*—a Fourth Amendment case—when discussing why *Patane* should not apply.[46] *Djibo* is perhaps emblematic of a problem Michael S. Pardo hypothesized, occurring when courts view the Fourth and Fifth Amendment as totally separate doctrines. Pardo wrote that "treat[ing] the two strands of doctrine as separate, independent problems… causes an analytic tangling of the rationales, concerns, and concepts proper to each amendment's analysis. Fourth Amendment rationales, concerns, and concepts get mistakenly imported into Fifth Amendment analysis, and vice versa."[47] But since both amendments "regulate government attempts to gather information," meaning that "potential Fifth Amendment events may also be potential Fourth Amendment events," courts mix up the rationales.[48]

Because the amendments are inherently interconnected, courts should instead acknowledge the situations that implicate both amendments. Not every situation will involve entanglement—after all, some Fifth Amendment events do not implicate the Fourth Amendment, and vice versa.[49] While viewing each amendment in a silo may feel doctrinally pure, it can just lead to more confusion, especially when the Fourth and Fifth Amendments arise at the same time.[50] And as the next section will explain, in many situations where the police seek to access digital devices, the two amendments often go hand in hand.

B. The Inevitable Entanglement of the Fourth and Fifth Amendments in Investigations and Arrests Involving Digital Devices

With cellphones, police have more to gain than with traditional physical evidence—indeed, unlocking a phone can easily lead to the discovery of incriminating information beyond the scope of the initial investigation.[51] Text messages with clients could show that the person has been engaging in sex work. Photos could show evidence of alcohol or drug use—which even if not a crime in and of itself, could be a violation of someone's terms of probation or parole. Records of calls made or emails sent could show that someone violated a no-contact order. Venmo or Paypal transactions could provide evidence of illegal

46. United States v. Djibo, 151 F. Supp. 3d 297 (E.D.N.Y. 2015).

47. Pardo, *supra* note 32, at 1860 (arguing the "*Boyd* Court was partially correct in seeing the two Amendments as overlapping and that the complete rejection of this view in current doctrine and theory has led to its own type of entanglement-an entanglement that arises from a failure to see a connection between the two constitutional provisions").

48. *Id.*

49. *See* Nagareda, *supra* note 31, at 1626–27; Pardo, *supra* note 32, at 1880 n.136.

50. Pardo, *supra* note 32, at 1860.

51. Adam M. Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 VAND. L. REV. 585, 588 (2016) (explaining that police may seek—and receive—warrants that "authorize an expansive search of the entire cell phone-and the millions of pages of attendant data-with little or no guidance or limitation on what police can search").

transactions. The cellphone gives the officer a look into a person's entire life, and the ability for law enforcement to comb through the device to find as much incriminating information as possible, for both the offense they sought to investigate, and anything else. And the increasing amount of incriminating information can lead to additional charges—and additional pressure to take a plea deal as the charges pile up.

But in many cases, police can only do this fishing-expedition style search of a digital device when they gain consent to search the device. When police apply for a warrant under *Riley*, the Fourth Amendment may require them to describe with particularity the information sought.[52] Thus, their search of the device would be limited to certain apps, time periods, and other methods of restricting the search.[53] But a consent search legally opens up the entire device to police—allowing them to look for both evidence related to the present investigation, and any other information that might interest them. And once the Sixth Amendment right to counsel attaches, police have more restrictions on speaking to someone without their lawyer present.[54] Thus, for police, the "golden window" to gain access to all of a device's contents comes before the commencement of formal criminal proceedings like an indictment (when the right to counsel attaches), and via a consent search. And because of how courts currently interpret *Patane*, the police are free to ignore *Miranda* in their pursuit of accessing all contents on the device.

Police frequently use deceptive techniques to gain access to all the contents of a device during this "golden window" devoid of meaningful legal checks on the police. Both judicial orders and motions to suppress provide examples of how police already use deceptive tactics to gain access to digital devices. For example, in *United States v. Ansah*, a Northern District of Georgia case, the police lied to the defendant about what would happen if he gave the police his passcode, leading to a finding that his admissions were involuntary.[55] Officers explained they were seizing the phone, and Mr. Ansah could get it back sooner if he told them the passcode.[56] Mr. Ansah expressed hesitation, but the officers then claimed that they were "not going into your e-mails or anything like that."[57] The court explained that once the officers obtained the passcode, "it appears that the agents used his password as the first step in doing exactly what they assured they would not do, i.e., look for e-mails and many other things 'like that,' throughout the electronic memory of his phone."[58]

52. *But see id.* at 618 (noting that many magistrate judges have failed to enforce the particularity requirement for cell phone search warrants). For a discussion of the entanglement of the Fourth and Fifth Amendment in cases where the police have obtained a warrant, *see* Sacharoff, *supra* note 23, at 250 (exploring how "encrypted devices seized by law enforcement with a search warrant present a hybrid case that brings into play both the Fourth and Fifth Amendments").

53. Gershowitz, *supra* note 51, at 601.

54. Massiah v. United States, 377 U.S. 201, 206 (1964); Brewer v. Williams, 430 U.S. 387, 400 (1977).

55. United States v. Ansah, 1:17-CR-00381-1-WSD-JSA, 2018 WL 4495523 at *5 (N.D. Ga. June 12, 2018).

56. *Id.* at *2. But at the time of the court's evidentiary hearing in the motion to suppress eight months later, officers still had not yet returned the phone, even though defendant had unlocked it as requested.

57. *Id.*

58. *Id.* at *5.

The deliberateness of the police conduct in *Djibo*, the case where the district court imparted Fourth Amendment logic onto the *Patane* analysis, was also one of the reasons why the court suppressed the contents of the digital device.[59] In *Djibo*, an officer took an initial "peek" at the contents of the phone before seeking a warrant.[60] That initial "peek" amounted to 921 pages of material, including "text messages, WhatsApp messages, call logs and contacts."[61] After deciding that material was "insufficient to support the narcotics investigation" that was the original object of the investigation, the officer then applied for a search warrant, 30 days after Mr. Djibo unlocked the phone.[62] While these facts appear to get at the Fourth Amendment inquiry more so than the Fifth Amendment question, the *Djibo* court cited these facts in its *Patane* discussion—showcasing the intertwined nature of the two amendments.[63]

A look at allegations in motions to suppress in cases involving the contents of digital devices also shows how law enforcement can exploit stressful and confusing situations during this legal "golden window" to gain access to a device. For example, in *United States v. Okeke*, defense attorneys alleged in their briefing that law enforcement took advantage of their client's naiveté when seeking to unlock and search his devices, as he was a foreign national unfamiliar with *Miranda*.[64] Mr. Okeke gave consent to search his devices before ever receiving *Miranda* warnings.[65] In the briefing for *United States v. Oloyede*, the only Court of Appeals case to address the applicability of *Patane* to digital devices, attorneys for Ms. Mojisola Popoola described how law enforcement officers entered the home at 6:30am, placed Popoola under arrest while she was in pajamas, then searched the home and located a phone they requested she unlock—without ever Mirandizing her.[66]

These cases show that for digital devices, Fourth and Fifth Amendment protections often go hand in hand. A request of someone in custody to open their phone may be quickly followed by a request to "take a look" at the contents of the phone. The average person is unlikely to understand that unlocking a phone and providing consent to search the phone are two different actions, with different legal consequences. And since police will naturally request to unlock a phone before asking to search it, this sequence will lead to more "yes" responses to the consent-to-search question.

Social science research confirms that people are inclined to succumb to police pressure to unlock phones. A 2019 study by Roseanna Sommers and Vanessa K. Bohns investigated how often individuals unlock a phone and allow someone to search it upon request, as well as public perceptions of what a

59. United States v. Djibo, 151 F. Supp. 3d 297, 307 (E.D.N.Y. 2015).
60. *Id*. at 302.
61. *Id*. at 309.
62. *Id.*
63. *See id*. at 310.
64. Def.'s Mot. & Mem. of Law to Suppress Statements and Evid., United States v. Okeke, No. 4:19-CR-00084-RBS-RJK, 2019 WL 8013476.
65. *Id*.
66. Br. of Appellants, at *92–93, United States v. Oloyede, 2018 WL 395404.

"reasonable" person would do in that situation.[67] In the study, participants were brought into a lab and asked to unlock their phone and hand it to a lab worker to search through.[68] They found that 97% of respondents in a study unlocked and handed their phone to a study administrator when requested.[69] The study also asked other participants—who were never requested to give up their phone—whether they would unlock and allow their phone to be searched, and whether a "reasonable" person would do so.[70] Only 27% of respondents said they would allow their phone to be searched, and only 14% said a reasonable person would do so.[71] While most people believe other reasonable people would never unlock and allow their phones to be searched, the overwhelming majority of people do comply.[72]

Judges also will likely have an unrealistic understanding of the pressure people feel to give up a passcode, unlock a phone, or consent to a search. The judiciary—and especially the federal judiciary—skews more white and more affluent than people who come into contact with police on a daily basis.[73] The largely white judiciary does not have an accurate perception of the pressure that people of color—and Black people in particular—may feel in remaining compliant when interacting with law enforcement,[74] given the prevalence of police violence against Black people, even in low-level investigations.[75]

---

67. Roseanna Sommers & Vanessa K. Bohns, *The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance*, 128 YALE L. J. 1962 (2019). The researchers also sought to validate their results by comparing their lab results to data on how often people consent to police searches in real life. *Id.* at 1988. An analysis of Los Angeles Police Department data showed that the vast majority of individuals stopped in Los Angeles consented to vehicle searches, while people surveyed guessed that far fewer people would have consented to a search of their vehicle. *Id.*

68. *Id.* at 1983–84. The framing of the question in this study, if done by law enforcement while someone was in custody, would implicate both the Fourth and Fifth Amendment—showing how for cellphones, Fourth and Fifth Amendment issues go hand in hand.

69. *Id.* at 1985.

70. *Id*.

71. *Id.* The study also evaluated whether informing the study participants that they did not have to unlock and provide their phone would change the rate that respondents relinquished their phone, or respondents' beliefs on whether they or a reasonable person would do so. The study found only small decreases, and that the "social demands of police-citizen interactions persist even when people are informed of their rights." *Id.* at 1962. These findings suggest that a more expansive understanding of what an involuntary relinquishment of a passcode looks like—for example, like in United States v. Ansah, 1:17-CR-00381-1-WSD-JSA, 2018 WL 4495523 (N.D. Ga. June 12, 2018)—may be necessary to truly address the pressures individuals feel to comply with police requests to unlock phones.

72. *See* Sommers & Bohns, *supra* note 67, at 1985.

73. *See Examining the Demographic Composition of U.S. Circuit and District Courts*, CTR. FOR AM. PROGRESS (Feb. 13, 2020), https://www.americanprogress.org/issues/courts/reports/2020/02/13/480112/examining-demographic-compositions-u-s-circuit-district-courts (reporting that people of color make up only a small percentage of the federal judiciary).

74. *See* Sommers & Bohns, *supra* note 67, at 1975 (citing *In re J.M.*, 619 A.2d 497, 513 (D.C. 1992) (Mack, J., dissenting)). D.C. Court of Appeals judge Julia Cooper Mack—the first Black woman to serve on the D.C. Court of Appeals—explained that in a police bus sweep "no innocent black male (with any knowledge of American history) would feel free to ignore or walk away." *In re J.M.*, 619 A.2d at 513. Sommers and Bohns also cite to Justice Alan C. Page, a Black member of the Minnesota Supreme Court, writing that he "was taught by his parents, that for personal safety . . . it is best to comply carefully and without question to the officer's request." State v. Harris, 590 N.W.2d 90, 106 n.4 (Minn. 1999) (Page, J., dissenting)).

75. George Floyd, killed by Minneapolis police in 2020, was accused of using a fake $20 bill to buy groceries. Eric Garner, killed by New York City police in 2014, was accused of selling loose cigarettes. *See* Jemima McEvoy, *New Transcripts Reveal How Suspicion Over Counterfeit Money Escalated Into The Death Of George Floyd*, FORBES (July 8, 2020 7:33 PM), https://www.forbes.com/sites/jemimamcevoy/2020/07/08/new-

The failure to appreciate the pressure that people feel to comply with the police has both Fourth and Fifth Amendment implications. Since Justice Thomas's *Patane* plurality opinion only allows exclusion for involuntary statements, judges will likely ignore the pressures people feel to unlock phones. In the voluntariness question for searches under the Fourth Amendment, "judges rarely give weight to individualized factors about the accused when deciding voluntariness" and instead focus on things like whether officers drew weapons or an officer's tone of voice.[76] How many judges would find that a police request to unlock a phone, phrased as "will you unlock your phone so we can look at it briefly?" will create enough pressure to render the response involuntary? But the research shows that for many people, they will feel high pressure to give in to police.[77]

The current law ignores the pressures at play for people to comply with the police, give up passcodes, and allow searches of their digital devices. And these pressures simultaneously implicate the Fourth and Fifth Amendments. A move by the courts or lawmakers to protect an individuals' rights under one amendment may not be effective unless the other right is also protected. Practically speaking, the amendments are often implicated in the very same interaction with police officers, with neither officers nor individuals distinguishing between the two. Here, the invitation from *Patane* to flout *Miranda* in cases involving digital devices can also increase the chances that police can bypass *Riley* protections by getting consent to search, too. Accordingly, in the context of police seeking access to individuals' digital devices, the Fourth and Fifth Amendments are intertwined, even as courts seek to imagine the amendments as carrying completely separate rights.

Of course, restricting *Patane* is not the only way to address the pressure people feel to give up devices. For example, as suggested by Sommers and Bohn, an informed consent requirement—that requires officers to inform people that they do not have to give up their device—could lessen the pressure.[78] But Sommers and Bohn explain that this modification—a sort of "*Miranda* for search"—may not actually lessen the pressure.[79] And scholars, lawyers, and

transcripts-reveal-how-suspicion-over-counterfeit-money-escalated-into-the-death-of-george-floyd/#3c41074746ba; *see also* Katie Benner, *Eric Garner's Death Will Not Lead to Federal Charges for N.Y.P.D. Officer*, N.Y. TIMES (July 16, 2019), https://www.nytimes.com/2019/07/16/nyregion/eric-garner-case-death-daniel-pantaleo.html.

76. Sommers & Bohns, *supra* note 67, at 1970 (summarizing research on factors courts use to assess voluntariness under the Fourth Amendment); *see also* Marcy Strauss, *Reconstructing Consent*, 92 J. CRIM. L. & CRIMINOLOGY 211, 213 (2001) (arguing that "the subjective views of the [people accused of crimes] are almost always invariably ignored by the courts").

77. The Sommers & Bohns study concluded by finding that "the social demands of police-citizen interactions persist even when people are informed of their rights." Sommers & Bohns, *supra* note 67 at 1962. Thus, the solution to this problem may not just be assuring that police inform people of their *Miranda* rights, but rather empirically testing specialized warnings, or banning certain types of consent searches (or passcodes entries) altogether. *See id.* at 2017 ("We suggest that advocates should require empirical evidence showing that warnings are effective before embracing these reforms."). Supreme Court justices have also acknowledged the immense pressure people feel to comply with the police. For example, in his dissent in *Ohio v. Robinette*, Justice Stevens wrote that people often do things not for their self-interest, but because they believe they may have a legal duty they must comply. Ohio v. Robinette, 519 U.S. 33, 48 (1996).

78. Sommers & Bohn, *supra* note 67, at 1995 n.114.

79. *Id*.

courts already pay a great deal of attention to *Riley* and the threshold question of which methods of unlocking a device can violate the Fifth Amendment. But scholars, courts, and advocates have paid less attention to how *Patane* fits into this problem. This article seeks to explain the *Patane* decision and how that decision has led to police accessing devices with impunity and provide a framework for differentiating the digital evidence implicated in cases involving cellphones and computers from the traditional physical evidence that was at play in *Patane*.

III. *PATANE*, THE PHYSICAL FRUITS DOCTRINE, AND ITS LIMITED APPLICATION TO CASES INVOLVING DIGITAL DEVICES

Although *Miranda* stated that "no evidence obtained as a result of interrogation can be used against" a defendant who never received *Miranda* warnings, the Court did not explicitly address physical fruits found thanks to unwarned statements.[80] In 2004, following years of limiting the reach of the Fifth Amendment generally, and *Miranda* in particular, the Supreme Court decided *Patane*.[81] The Supreme Court had long ago abandoned the expansive view of the Fifth Amendment found in *Boyd*, and in the 20th century, nearly every word in the short Self-Incrimination Clause became subject to debate.[82] *Patane* represented the coalescence of two ways the Court had begun limiting the Fifth Amendment: by limiting the definition of "testimonial" evidence,[83] and by carving out more and more exceptions to the *Miranda* exclusionary rule.[84] The fractured Court produced a variety of rationales for why physical fruits of statements obtained in violation of *Miranda* should—or should not—be admissible at trial. This section will explain the *Patane* decision and how courts have applied *Patane* so far in the few cases involving digital devices.

80. Miranda v. Arizona, 384 U.S. 436, 479 (1966).

81. United States v. Patane, 542 U.S. 630 (2004).

82. *See* Akhil Amar & Renée Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L. REV. 857, 861 (1995) ("[V]irtually every word and phrase - person, compelled, in any criminal case, and witness - sits atop considerable confusion or perversion because courts do not yet understand how the words fit together, or what big idea(s) might underlie the clause.").

83. In *Fisher v. United States*, the Court decided that the act of producing business documents is not testimonial. Fisher v. United States, 425 U.S. 391 (1976). In *Schmerber v. California*, the Court found a blood or breath sample in the context of a DUI investigation is not testimonial. Schmerber v. California, 384 U.S. 757 (1966).

84. The Court also created specific situations that allowed for an exception to *Miranda*'s exclusionary rule, continuously poking holes in *Miranda*. For example, in *New York v. Quarles*, the Court created a public safety exception to the *Miranda* exclusionary rule, allowing officers to question people about safety concerns—like the location of a gun in a public place—before administering a *Miranda* warning. New York v. Quarles, 467 U.S. 649, 657 (1984). In *Oregon v. Elstad*, the Court allowed the admission of a confession made following *Miranda* warnings, when the suspect had already given a confession during a non-Mirandized confession. Oregon v. Elstad, 470 U.S. 298 (1985). And in *Harris v. New York*, the Court allowed the introduction of unwarned statements for impeachment evidence in order to protect the integrity of court proceedings. Harris v. New York, 401 U.S. 222 (1971). The Court gradually eroded *Miranda*'s broad reach as it picked out specific situations where the exclusionary rule would not apply.

A. The Patane *Decision*

The police encounter and interrogation that led to *Patane* concerned a rather mundane investigation, in which the defendant, Samuel Patane, was indicted for a felon-in-possession of a firearm charge following police officers' retrieval of a gun from his bedroom.[85] The officers had come to Mr. Patane's home to arrest him for violating a restraining order and to investigate whether he possessed a gun.[86] However, they only located the gun after arresting and questioning Mr. Patane, without completing the *Miranda* advisement.[87] Mr. Patane "was initially reluctant" to talk about whether he had a gun in the home, but an officer "persisted," and Mr. Patane then told the officer where to find the gun and gave him permission to retrieve it.[88] Indeed, this scenario resembles the hypothetical presented in Part II: a *Miranda* violation leads to the discovery of physical evidence that police access thanks to a consent search.

Writing for a plurality joined by Justice Scalia and Chief Justice Rehnquist, Justice Thomas stated that courts can always admit physical fruits of a voluntary statement obtained in violation of *Miranda*. Justice Thomas emphasized the differences he believed to separate *Miranda* and the Self-Incrimination Clause.[89] He characterized *Miranda* as a prophylactic that only seeks to prevent violations of the Self-Incrimination Clause itself.[90] And while he acknowledged that "the *Miranda* rule creates a presumption of coercion" in interrogations, prophylactic rules like *Miranda* "sweep beyond the actual protections of the Self-Incrimination Clause."[91] In his view, a rule designed to deter "mere failures to warn" does not actually protect the core Fifth Amendment right.[92] Thus, according to Justice Thomas, any further application of the *Miranda* exclusionary rule needs to be evaluated to determine whether it actually protects the right against self-incrimination.

For Justice Thomas, the physical fruit cannot violate the Self-Incrimination Clause because the Self-Incrimination Clause—in his view—only protects against statements. Justice Thomas interpreted the Self-Incrimination Clause as a trial right by emphasizing its "explicit textual protection" barring the compulsion of people to serve as witnesses against themselves.[93] That interpretation meant that since only actual statements can violate the Self-Incrimination Clause, the "physical evidence resulting from voluntary statements" does not implicate the Self-Incrimination Clause.[94] But at the same time, Justice Thomas left a hole in his logic. He briefly noted that "the Court

85. Patane, 542 U.S. at 635 (Thomas, J., plurality).
86. *Id.* at 634–35.
87. *Id.* at 635.
88. *Id*.
89. *Id.* at 636.
90. *Id.* at 643.
91. *Id.* at 639.
92. *Id.* at 642.
93. *Id.* at 640 (further contrasting the Fifth Amendment's "self-executing" clause with the Fourth Amendment, which does not explicitly provide a remedy for violations).
94. *Id.* at 634.

requires the exclusion of the physical fruit of actually coerced statements."[95] However, he never reconciled this assertion with his earlier logic that only statements—and not physical objects—implicate the Fifth Amendment.[96]

Justice Kennedy, joined by Justice O'Connor, wrote a brief—and less than clear—concurrence, focusing on the "important probative value of reliable physical evidence."[97] Justice Kennedy agreed with Justice Thomas that admitting "nontestimonial physical fruits (like the Glock in this case)" does not risk admitting a person's "coerced incriminating statements" against himself.[98] However, Justice Kennedy declined to address points raised by Justice Thomas, such as whether deterring police violations of *Miranda* could ever merit excluding a physical fruit. Instead, Justice Kennedy simply stated that it was "doubtful that exclusion can be justified by a deterrence rationale" that considered both law enforcement needs and individual rights.[99]

In contrast, Justice Souter wrote a dissent, joined by Justice Stevens and Justice Ginsburg, that refuted the plurality's characterization that physical fruits cannot implicate the Self-Incrimination Clause and focused on the practical consequences of the plurality opinion.[100] The dissent repeatedly criticized the plurality for "closing their eyes" to the evidentiary gains law enforcement officers achieve through violations of *Miranda*, and thus creating an "inducement for interrogators" to ignore *Miranda*.[101]

Finally, Justice Breyer separately dissented, briefly stating that courts should exclude physical evidence resulting from *Miranda* violations for the

95. *Id.* at 637.

96. *See* Yale Kamisar, *Postscript: Another Look at Patane and Seibert, the 2004 Miranda 'Poisoned Fruit' Cases*, 2 OHIO ST. J. CRIM. L. 97 (2004). Kamisar critiqued Justice Thomas's brief—and unsupported—assertion that physical fruits of involuntary statements must be treated differently. Kamisar wrote: "It is not at all clear (and Justice Thomas does nothing to make it clear) why the specific language in the text of the Fifth Amendment constitutes an impenetrable barrier to the exclusion of physical evidence obtained from someone in Mr. Patane's circumstances but is inoperative when the issue presented is the admissibility of the same kind of evidence derived from statements obtained in violation of 'the core protection' afforded by the Fifth Amendment." *Id.* at 102.

97. *Patane*, 542 U.S. at 645 (Kennedy, J., concurring).

98. *Id.*

99. *Id*.

100. *Id.* (Souter, J., dissenting).

101. *Id.* Justice Souter also sought to differentiate physical fruits from other existing exceptions to the exclusionary rule, explaining that the introduction of Mr. Patane's gun did not raise concerns present in other cases, like the need to allow unwarned statements for impeachment evidence out of "respect for integrity of the judicial process." *Id.* at 646–47 (*citing* Harris v. New York, 401 U.S. 222 (1971)). Justice Souter also discussed the inapplicability of *New York v. Quarles* and *Oregon v. Elstad*. New York v. Quarles, 467 U.S. 649 (1984) (creating a public safety exception to the *Miranda* exclusionary rule); *Oregon v. Elstad*, 470 U.S. 298 (allowing admission of a properly Mirandized statement following a non-Mirandized statement). Justice Souter also noted that *Patan*e seemed at odds with the other *Miranda* case decided the same day, Missouri v. Seibert, 542 U.S. 600 (2004) (finding that gaining a *Miranda* waiver mid-interrogation and having the suspect repeat a confession made prior to the waiver must be excluded). In *Seibert*, the Court emphasized that the specific interrogation technique was used to flout *Miranda*. *Id.* at 613 (explaining that the questioning technique's "manifest purpose… is to get a confession the suspect would not make if he understood his rights at the outset"). *See also id.* at 618 (Kennedy, J., concurring) (stating that "the interrogation technique used in this case is designed to circumvent *Miranda v. Arizona* . . . .").

reasons articulated by Justice Souter, unless the violation occurred in good faith.[102]

B. Application of Patane *in Cases Involving Digital Devices*

Post-*Patane* caselaw shows that courts have failed to address how digital fruits may differ from physical fruits. Most post-*Patane* cases in federal courts have addressed purely physical objects, like guns or drugs. Only a handful of federal courts have addressed the application of *Patane* to digital devices.[103] The lone federal appellate court case involving digital data accessed following a *Miranda* violation applied the plurality without question. And the one federal district court order that found *Patane* inapplicable in a case involving the contents of a cellphone—and thus suppressing those digital contents—focused largely on Fourth Amendment principles, failing to adequately explain why *Patane* should not apply in this scenario.

In *United States v. Oloyede*, the Fourth Circuit quickly disposed of the *Patane* issue after briefly concluding that unlocking a device did not represent a testimonial act for the purposes of the Fifth Amendment.[104] In *Oloyede*, a FBI agent executing a search warrant asked Mojisola Popoola, one of four co-defendants in the appeal, "Could you please unlock your iPhone?" while executing a search warrant in her home.[105] Ms. Popoola, at this point in custody but without a *Miranda* warning, unlocked the phone and handed it back to the agent. The court held that even if the act of entering in her password was testimonial, it "would provide no meaningful help for her defense" as the contents of the phone would be admissible under *Patane*.[106] The Fourth Circuit panel then relied on Justice Thomas's plurality to explain that the phone data

102. *Patane*, 542 U.S. at 647–48 (Breyer, J., dissenting). Justice Breyer also referenced his concurrence in *Seibert*. In *Seibert*, Justice Breyer advocated for a rule that would exclude Mirandized statements made during the same interrogation as an earlier non-Mirandized admission, unless there was no bad faith by the officers. *Seibert*, 542 U.S. at 617 (Breyer, J., concurring).

103. A Sixth Circuit case presents a related issue that will not be explored in this article: where police violate *Miranda* to find a digital device and seek to admit that device's contents, but the digital device was unlocked. In *United States v. Hilton*, the court admitted the contents of a Blackberry under the inevitable discovery doctrine after briefly mentioning the *Patane* issue. United States v. Hilton, 625 Fed. Appx. 754 (6th Cir. 2015). In *Hilton*, the court did not mention whether the Blackberry was protected by a password or encrypted. After police took Mr. Hilton into custody in his home—but before advising him of *Miranda*—Mr. Hilton told officers that he had child pornography on a Blackberry, which the officers then retrieved in a kitchen drawer. *Id.* at 756–57. Without specifying how officers unlocked the device (and thus whether they violated *Miranda* to access the phone's contents) and briefly mentioning *Patane*, the court admitted the contents by applying the inevitable discovery doctrine. The court explained that the police already knew that the defendant used that model of cellphone to access a child pornography website, and would have sought to search the phone. *Id*. at 759. If the phone was not password-protected or encrypted, then this case presents a separate, but related, question to the issue in this article—if police find an unlocked digital device in violation of *Miranda*, can they still admit the contents of the device? I will not address this related question in this article. However, if the phone in *Hilton* was indeed locked, the use of the inevitable discovery doctrine to justify the Sixth Circuit's decision is questionable. *See, e.g.* United States v. Djibo, 151 F. Supp. 3d 297, 310–11 (foreclosing the application of the inevitable discovery doctrine for the contents of a cellphone obtained after a Fifth Amendment violation, when there was testimony indicating law enforcement did not have a reliable method of gaining access to a phone without knowing the passcode).

104. United States v. Oloyede, 933 F.3d 302, 308–10 (4th Cir. 2019).

105. *Id.* at 308.

106. *Id.* at 309.

was a physical object that does not implicate the Self-Incrimination Clause as it "present[ed] no risk that . . . *coerced statements* (however defined) [would] be used against [her] at a criminal trial."[107]

Very few district courts have addressed the application of *Patane* to the contents of digital devices. Most simply applied *Patane* like in *Oloyede*,[108] but two cases begin to discuss why the contents of digital devices may raise different concerns than the gun in *Patane*. In *United States v. Stark*, the Eastern District of Michigan admitted photographs found on a password-protected computer, emphasizing the photographs—which depicted other people—were "non-testimonial."[109] The *Stark* court described that *Patane* allowed the admission of "non-testimonial, i.e., physical, evidence obtained as a result of incriminating statements made in violation of *Miranda*," but did not elaborate on the division between non-testimonial and physical evidence, or if a different kind of photograph or digital evidence could merit exclusion.[110]

In *United States v. Djibo*, a judge in the Eastern District of New York excluded the contents of a phone after declining to apply *Patane*, emphasizing the differences between traditional physical evidence and digital devices.[111] In *Djibo*, a Customs and Border Protection officer asked a traveler for his passcode while detaining him at an airport, but before administering *Miranda* warnings.[112] The judge provided three reasons for not applying *Patane*.[113] First, the court noted that once the defendant, Adamou Djibo, received the *Miranda* warnings, he asked for an attorney, leading the court to believe he would have refused to enter the passcode had he been informed of his rights.[114] Second, the court emphasized the need to deter law enforcement from flouting *Miranda*, focusing on the specific conduct of the investigating officer.[115] The court noted that the officer lacked credibility after his "evasiveness during the Court's direct questioning" and concluded that the officer "sought to sidestep . . . constitutional guarantees."[116] Third, the court emphasized the difference between a cellphone and the gun in *Patane*, writing about the vast amount of

107. *Id.* at 309–10 (quoting United States v. Patane, 542 U.S. 630, 643 (2004)) (alterations in original).

108. For examples of district court opinions where courts applied *Patane* to the contents of digital devices without further analysis, *see* United States v. Woodland, 285 F. Supp. 3d 864, 874 (D. Md. 2018); United States v. Hernandez, No. 18-CR-1888-L, 2018 WL 3862017, at *4 (S.D. Cal. Aug. 13, 2018); United States v. Orozco Ramirez, No. 17-CR-185-LMM-AJB-011, 2019 WL 2165920, at *8 (N.D. Ga. Apr. 22, 2019); United States v. Mendez-Bernal, No. 3:19-CR-00010-TCB-RGV, 2020 WL 6495109, at *18 (N.D. Ga. July 22, 2020); United States v. Mendez-Bernal, 3:19-cr-00010-TCB-RGV, 2020 WL 6495109, at *18 n.25 (N.D. Ga. July 22, 2020). State courts have also applied *Patane* to the contents of digital devices without distinguishing between digital evidence and traditional physical evidence. State v. Sayles, 202 Conn. App. 736, 751 (2021).

109. United States v. Stark, No. 09-cr-20317, 2009 WL 3672103 at *3 (E.D. Mich. Nov. 2, 2009).

110. *Id.*

111. United States v. Djibo, 151 F. Supp. 3d 297, 307 (E.D.N.Y. 2015).

112. *Id.*

113. *Id.* at 309–10.

114. *Id.* at 309. In contrast, Mr. Patane told the investigating officer that he knew his rights, thus interrupting and ending the officer's recitation of rights. United States v. Patane, 542 U.S. 630, 635 (2004).

115. *Djibo*, 151 F. Supp. 3d at 309.

116. *Id.* When the court asked the officer why he sought the passcode, the officer responded only with "to get the passcode." The court concluded that the officer's "intention was to expand the definition of "border search" in a way this Court cannot abide and in a way that invokes *Wong Sun v. United States*, 371 U.S. 471, (1963)." *Id.*

personal information contained on a cellphone, and that "in today's modern world, a cell phone passcode is the proverbial 'key to a man's kingdom.'"[117]

But the court's reasoning in *Djibo* focused on the intensely private nature of the information, without grappling with why *Patane* should lead to a different result when dealing with the contents of digital devices. Privacy, after all, has been more of a factor in assessing Fourth Amendment protections than Fifth Amendment protections.[118] This analysis mirrors the approach many defense attorneys have taken in motions to suppress.[119]

In the meantime, the *Patane* dissenting justices' fears have been realized, as law enforcement officers flout *Miranda* to gain more evidence.[120] *Patane* has encouraged police to disregard *Miranda* when the physical evidence at stake is worth more than a defendant's statements.[121] Officers use a variety of tactics to trick people into giving up their passcodes. For example, in *Djibo*, the officers initially characterized the request for the defendant's passcode as part of a routine border search, without informing the defendant of *Miranda*.[122] And in *United States v. Hernandez*, although Homeland Security Investigations officers administered the *Miranda* warning to a woman under arrest, they continued questioning her and asked her to demonstrate how to unlock her phone after she had twice requested to speak to an attorney.[123] The *Hernandez* court excluded the physical demonstration of the phone but admitted its contents, even though "the contents would not have been discovered but for Defendant's demonstration of the passcode after her invocation."[124] And officers have also started using the answers to questions they seek to categorize as routine booking questions—like someone's birthday or cellphone numbers—to guess cellphone passcodes, hoping to allow statements in under that exception.[125]

---

117. *Id.* at 310.

118. *See supra* Part II.

119. *See, e.g.*, Brief of Appellants at *19, United States v. Oloyede, 2018 WL 2244758 (4th Cir. Jan. 8, 2018) (citing *Djibo* and stating that *Patane* allows the admission of "physical evidence, but not testimonial evidence," without explaining why the contents of the cellphone would count as testimonial evidence); Br. of Defendants, United States v. Okeke, 2019 WL 8013476 (E.D. Va. Dec. 15, 2019) (failing to cite to *Patane* when discussing why information obtained from the phone should be suppressed under the Fifth Amendment, and citing to Justice Breyer's dissent in *Patane* while arguing that the contents of the phone should be suppressed under the Fourth Amendment).

120. Officers also flout *Miranda* in cases involving traditional physical evidence. *See, e.g.*, United States v. Rakotojoelinandrasana, 450 Fed. Appx. 549 (8th Cir. 2011) (admitting traditional physical evidence—a stash of money and a BB gun—despite a blatant *Miranda* violation, where the defendant repeatedly asked to end the interrogation).

121. Some district courts have suppressed the contents of digital devices as being the fruit of a coerced or involuntary statement when officers obtained a password after an individual had already requested to speak to an attorney. *See United States v. Ansah*, 2018 WL 4495523, at *6 (N.D. Ga. June 12, 2018); *United States v. Eiland*, No. 4:18-CR-3154, 2019 WL 2724077, at *5 (D. Neb. July 1, 2019). *But see* United States v. Lopez, No. 13CR2092 WQH, 2016 WL 7370030 (S.D. Cal. December 20, 2016) (admitting evidence despite defendant's post-*Miranda* invocation of rights). The varied use of an involuntariness finding to exclude physical fruits suggests that some courts may be seeking to get around the harsh *Patane* rule without adopting the type of analysis used in *Djibo*.

122. United States v. Djibo, 151 F. Supp. 3d 297, 299–300 (E.D.N.Y. 2015).

123. United States v. Hernandez, No. 18-CR-1888-L, 2018 WL 3862017, at *1 (S.D. Cal. Aug. 13, 2018).

124. *Id.* at *4.

125. *See, e.g*. United States v. Lopez, No. 13CR2092 WQH, 2016 WL 7370030 at *1. (S.D. Cal. Dec. 20, 2016). In *Lopez*, the agent began asking the suspect for identifying information like her date of birth. The agent

Patane and its progeny provide an unsatisfactory framework for dealing with digital devices with both physical and communicative aspects. Courts should not blindly apply *Patane* without grappling with how digital evidence fits in with the doctrine. Part IV provides possible strategies for litigating *Patane* issues.

IV. STRATEGIES FOR LITIGATING *PATANE* ISSUES IN CASES INVOLVING THE CONTENTS OF DIGITAL DEVICES

In the absence of direction from the Court that will reorient thinking on the Fifth Amendment in cases involving technology—and the Fifth Amendment's relationship with the Fourth Amendment in these cases—defense attorneys still need to advocate that *Patane* should not apply to digital devices. And in crafting litigation strategies, attorneys can take one of two main approaches: argue that the Fifth Amendment should respond to changes in technology like the Fourth Amendment has or explain how existing Fifth Amendment principles and *Patane* itself support the exclusion of digital evidence gained in violation of *Miranda*.

Although arguing for a wholesale change to how the Fifth Amendment treats digital evidence may seem like a hard ask for a court, courts have been most willing to change doctrinal rules in criminal procedure with the advent of new technologies.[126] Indeed, the Fourth Amendment has undergone significant changes in recent years.[127] An argument that *Patane* just does not make sense in the digital age has gained viability following *Riley* and *Carpenter*.

In the alternative, courts and advocates could rely on existing principles in Fifth Amendment doctrine to carve out a "digital fruits" exception to *Patane*. A closer read of *Patane* and other Fifth Amendment caselaw suggests that courts should treat digital fruits—a physical fruit with communicative aspects and serious personal privacy implications—differently than the gun in *Patane*. Two key arguments explain why *Patane* can still allow the exclusion of the contents of a digital device gained in violation of *Miranda*.

First, the possible "diary exception" in Fifth Amendment caselaw, which protects intensely private thoughts, should extend to the contents of digital devices. Fifth Amendment doctrine has long suggested that diaries, a record of one's personal thoughts and reflections, may merit protection under the Fifth Amendment.[128] Like diaries, the contents of phones and digital devices offer a detailed view into the most intimate details and reflections in a person's life.[129]

Mirandized the suspect after this initial set of questions. After the interview, another agent unlocked the suspect's cellphone by guessing the passcode—her date of birth.

126. *See generally* Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 557 (2017) (discussing "how digitization is challenging formal distinctions in Fourth Amendment doctrine that previously have played a role in protecting the right to privacy").

127. Riley v. California, 573 U.S. 373 (2014); Carpenter v. United States, 138 S. Ct. 2206 (2018).

128. *See infra* Part IV-B.

129. Some people even use their phones as digital alternatives to physical diaries. *See* Farhad Manjoo, *Why A Digital Diary Will Change Your Life*, N.Y. TIMES: OPINION (June 12, 2019), https://www.nytimes.com/2019/06/12/opinion/digital-diary.html (discussing a mobile application that allows users to record their thoughts on their phone, as opposed to a traditional diary or journal).

Attorneys can use the principles underlying the diary exception to differentiate traditional physical evidence from more personal evidence, and argue that *Patane* should recognize this difference.

Second, while courts have largely applied Justice Thomas's plurality as the governing law, the narrower concurrence from Justice Kennedy leaves room for courts to balance the interests of law enforcement and a possible need for deterrence.[130] Applying the principle from *United States v. Marks*[131] that a case's holding comes from the narrowest grounds necessary to achieve the result, Justice Kennedy's concurrence should control the lower courts—not Justice Thomas's plurality. And Justice Kennedy's concurrence hints at a balancing test that should lead to a different result for the contents of digital devices.

A. The Fifth Amendment Should Follow the Fourth Amendment and Adapt to Changes in Technology by Declining to Apply Patane *to the Contents of Digital Devices*

Scholars have long advocated that changes in technology require wholesale changes to rules of criminal procedure. When an investigation concerns issues like computer hacking, DNA sequencing to identify a suspect, or communications over the internet, scholars have explained that traditional rules of criminal procedure—that were designed for purely physical evidence—do not effectively translate to new technologies.[132] New technologies require new rules, and the Court has started to recognize this view in *Riley* and *Carpenter*.[133] One approach to litigating *Patane* issues in the context of digital devices is to simply argue that digital devices require a new rule: that *Patane* does not apply to digital evidence.

In the Fourth Amendment context, the Court has recognized the need for new rules. For example, in *Riley*, the Court noted that the government's argument "that a search of all data stored on a cell phone is 'materially indistinguishable' from searches of . . . physical items . . . is like saying a ride on horseback is materially indistinguishable from a flight to the moon."[134] The Court explained that both the amount and type of information contained on cellphones implicated privacy interests different than traditional physical objects.[135] Similarly, the Court in *Carpenter* recognized that when the government "ask[ed] for a straightforward application of the third-party doctrine," the immense amount of information at stake really meant the

130. *See* United States v. Patane, 542 U.S. 630, 644–45 (2004).

131. United States v. Marks, 430 U.S. 188 (1977).

132. Orin Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279 (2005). Elizabeth E. Joh, *Reclaiming Abandoned DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857 (2006); Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010).

133. Riley v. California, 573 U.S. 373, 393 (2014); Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

134. *Riley*, 573 U.S. at 393.

135. *Id.*

government was asking for "a significant extension of [the doctrine] to a distinct category of information."[136]

Applying *Patane* to digital devices would not be a "straightforward application," but rather the kind of "significant extension" that the Court rejected in *Carpenter*.[137] Unlocking a device in violation of *Miranda* and gaining consent to search the device gives police access to digital content well beyond what they would view if they received a warrant. If an officer applied for a warrant, that officer may need to provide parameters to limit the search: which apps the relevant data might appear on, the general time frame of data sought, and other limiting factors.[138] But a warrantless look into a phone lets the officer peruse any and all information on the phone. That warrantless look lets the officer go on a fishing expedition, checking not only for information relevant to an investigation, but also evidence of any other sort of activity. And as the Court noted in *Riley*, the kind of information found on a phone is immensely different than traditional physical evidence.[139]

As exhibited most recently by *Carpenter* and *Riley*, the Court seeks to adapt Fourth Amendment doctrine to changes in technology.[140] Orin Kerr's equilibrium adjustment theory of the Fourth Amendment describes how search and seizure doctrine responds to changes in technology to ensure a balance of advantages and protections between individuals and law enforcement.[141] When a new technology develops, individuals may use that technology to evade detection by law enforcement, or law enforcement may use it to more closely surveil the public.[142] Under Kerr's theory, the Court creates rules to restore the relative balance of investigative advantages and privacy protections back to an earlier equilibrium, so neither side keeps an advantage over the other thanks to new technology.[143] But the Court should not limit "equilibrium adjustment" to the Fourth Amendment. This approach offers guidance on how the Fifth Amendment can respond to the way digital devices have changed how both individuals and law enforcement act.

The balance of power shifted long ago in the Fifth Amendment context as people increasingly began to rely on digital devices. Digital devices have given law enforcement multiple advantages in the Fifth Amendment context. First, as prosecutors rely more and more on digital evidence—like photos, text messages, and internet history—to prove cases, the contents of digital devices often matter more than real, in-person witnesses. The sheer amount of digital data can obviate the need for some actual witnesses, and in turn create a strong temptation for law enforcement to ignore *Miranda*.

---

136. *Carpenter*, 138 S. Ct. at 2219.
137. *See id.*
138. *See* Gershowitz, *supra* note 51 at 601.
139. *Riley*, 573 U.S. at 393.
140. *Id.* at 397; Carpenter, 138 S. Ct. at 2219.
141. *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).
142. *Id.* at 489.
143. *Id.* at 482.

Second, even though privacy is typically tied to the Fourth Amendment, the private nature of the data matters for the Fifth Amendment, too. If someone can unlock a device, it is likely the device will contain some personal information that connects that individual to the phone (regardless of whether that person is a sole user of the phone). Accordingly, police will not care about the act of unlocking the phone in order to tie someone to a device (a statement or action that may be testimonial—and thus excluded if done in violation of *Miranda*), removing their incentive to obey *Miranda*. Introducing statements, thoughts, and locations, and then painting them all as the defendant's—with no real way for the defense to refute without having a defendant testify—seems like a tempting proposition for police. A clear rule that would disincentivize police from violating *Miranda* is necessary to protect against police misconduct, as digital devices present even greater incentive issues than traditional physical fruits.

While many associate bright-line rules with Fourth Amendment context, and not the Fifth Amendment, there is both a history of and a need for bright line rules in the Fifth Amendment context. Donald Dripps writes that, when applying *Miranda* and the Fifth Amendment, courts should adopt bright-line rules responsive to new contexts and changes in the "legal ecology," like they have done in the Fourth Amendment context.[144] These bright-line rules give law enforcement clear guidance on how to act, as opposed to vague standards.[145] Dripps argues that the bright line rules in the Fourth Amendment context have "no formal difference" from the prophylactic rules of the Fifth Amendment context.[146] In the Fourth Amendment context, courts and scholars are comfortable with how bright line rules are both under- and over-inclusive.[147] Instead of being perfect, they create structures that limit law enforcement actions. Dripps argues that the Court should adopt similar rules for the Fifth Amendment: rules that a clear to understand so that they actually limit law enforcement actions.

But what should that rule be? A decision that *Patane* does not apply to the contents of digital devices would increase law enforcement's incentive to Mirandize people before requesting they unlock their phones, to ensure the contents are not excluded. But as demonstrated by the Sommers and Bohns study, providing a warning does not drastically reduce the rate that people hand over their phones, even if very few people believe that a reasonable person would unlock and hand over their phone.[148] Accordingly, not applying *Patane* to digital fruits, and thus excluding the contents of digital devices when officers violate *Miranda*, may not change individual behavior. But it may change the behavior of police, who may no longer rush to get an individual to unlock their phone so they can access it contents. A clear rule—like Dripps suggests—offering additional protection for the contents of digital devices by categorically

144. Dripps, *supra* note 44, at 894.
145. *Id.*
146. *Id.* at 895.
147. *Id.*
148. Sommers & Bohns, *supra* note 67, at 1994.

excluding non-Mirandized unlocking of a device would likely make police more cautious, and increase the likelihood they will Mirandize a person.

The Court's Fifth Amendment doctrine needs to recognize the ways technology has changed how people communicate, express their thoughts, and process private information, just as the Court has done with the Fourth Amendment. *Patane* has already created the "unjustifiable invitation to law enforcement officers to flout *Miranda* when there may be physical evidence to be gained" that the dissenting justices feared.[149] Law enforcement have even more incentive to flout *Miranda* in cases with digital devices, as they seek to access a trove of data, instead of a single object. And knowing that *Miranda* poses no bar in turn weakens Fourth Amendment protections, since police have an added incentive to quickly gain access to a digital device.

Commentators may argue that an about-face by the Court on *Miranda*, or a reconciliation of the relationship between the Fourth and Fifth Amendments, is unlikely. But given that Justice Thomas is the only judge from the *Patane* plurality or concurrence still on the bench, the current Court should not be assumed to hold the same views. Indeed, Chief Justice Roberts wrote the majority opinion in both *Riley* and *Carpenter*.[150] And many jurists seem to disagree with the conclusion in *Patane*; some state supreme courts have explicitly interpreted their own state constitutions to provide greater protections against self-incrimination by declining to create *Patane*-like rules, even when the state constitution's language mirrors the Fifth Amendment.[151] Practically speaking, for digital devices, Fourth and Fifth Amendment issues often go hand in hand. Now is the time for the Court to turn back towards recognizing the interplay between these two amendments by recognizing that the Fifth Amendment offers protections for the contents of digital devices.

B. Fifth Amendment Doctrine Already Recognizes the Difference Between Intensely Personal Information and Purely Physical Objects

Advocates can also tie their arguments to underlying principles in Fifth Amendment doctrine. Some Supreme Court justices have long suggested that highly personal, prerecorded information—like a diary—is testimonial, and should be treated differently than other prerecorded statements or objects. The era of protecting all personal, private papers, as established in *Boyd v. United States* back in 1886, is long gone.[152] But the Court has repeatedly expressed that the most private of papers—like a diary—may remain protected by the Fifth Amendment, even when documents like business records are not.[153] The

149. United States v. Patane, 542 U.S. 630, 647 (2004) (Souter, J., dissenting).

150. Riley v. California, 573 U.S. 373 (2014); Carpenter v. United States, 138 S. Ct. 2206 (2018).

151. *See* State v. Farris, 849 N.E.2d 985, 995 (Oh. 2006) (concluding that although the U.S. Constitution and Ohio Constitution are "essentially identical," the Ohio Constitution provides greater protections than the Fifth Amendment for physical evidence obtained in violation of *Miranda*); State v. Peterson, 923 A.2d 585 (Vt. 2007); Commonwealth v. Martin, 444 Mass. 213 (Mass. 2005); State v. Knapp, 285 Wis. 2d 86 (Wis. 2005).

152. *See* Boyd v. United States, 116 U.S. 616 (1886).

153. *See, e.g.*, United States v. Doe, 465 U.S. 605, 610 n.7 (1984) (affirming Fisher v. United States, 425 U.S. 391 (1976) and noting that the documents at issue in *Doe* were even less personal than the business records

question of how to handle physical objects that also communicate highly personal information is not a new problem for the Court. And this thread in Fifth Amendment doctrine should inform how courts apply *Patane* in cases involving objects with communicative value.

A "diary exception" provides protection for some highly personal, but pre-recorded, information, in contrast to recent restrictions to the Fifth Amendment that limit the meaning of "testimonial" evidence. Proponents of a limited understanding of the Fifth Amendment argue that prior cases about the meaning of "testimonial" exclude the possibility of testimonial physical evidence. In *Schmerber v. California*, the Court found that blood and breath tests were not testimonial, even though they communicate highly personal information about a person's body.[154] And in *Fisher v. United States*, the Court held that producing physical objects like business records does not constitute a testimonial act, focusing on how those records—and any statements therein—were not compelled, because they were created before law enforcement sought them.[155]

But some earlier Fifth Amendment cases have distinguished general physical objects from private, personal writings. The Court in *Fisher* only addressed business records, and explicitly set aside the question of private papers.[156] This exception—often referred to as the diary exception—received additional support following *Fisher*. In *United States v. Doe*, another business records case, the Court repeated this limitation of the *Fisher* holding, with Justice Marshall emphasizing the importance of the diary exception in his concurrence.[157] And before he joined the Court, Justice Samuel Alito wrote a law review article that touched on the diary exception.[158] Justice Alito wrote that "certain intimate personal documents—a diary is the best example—are like an extension of the individual's mind . . . . Forcing an individual to give up possession of these intimate writings may be psychologically comparable to prying words from his lips."[159]

Justices and scholars have also written that invasive physical information—like breath or blood tests—differ from private documents like diaries. In Justice Brennan's *Schmerber* opinion, he emphasized that blood does not compel someone to testify against themselves "or otherwise provide the

---

at issue *Fisher*); *see also id.* at 619 (Marshall, J., concurring) (explaining that business records "implicate a lesser degree of concern for privacy interests" than diaries).

154. Schmerber v. California, 384 U.S. 757, 765 (1966).

155. *Fisher*, 425 U.S. at 398–99.

156. *Id*. at 414. The Court cited to *Boyd* when stating "[w]hether the Fifth Amendment would shield the taxpayer from producing his own tax records in his possession is a question not involved here; for the papers demanded here are not his 'private papers.'"

157. *Doe*, 465 U.S. at 610 n.7; *see also id.* at 619 (Marshall, J., concurring). In his concurrence, Justice Marshall also cited one of his earlier dissents on this issue that laid out his views on Fifth Amendment protections for documents. *See id*. at n.2. In *Couch v. United States*, Justice Marshall wrote that "diaries and personal letters that record only their author's personal thoughts lie at the heart of our sense of privacy. In contrast, I see no bar in the . . . Fifth Amendment to the seizure of a letter from one conspirator to another directing the recipient to take steps that further the conspiracy. Business records . . . lie between those cases." Couch v. United States, 409 U.S. 322, 350 (1972) (Marshall, J., dissenting).

158. Samuel A. Alito, *Documents and the Privilege Against Self-Incrimination*, 48 U. PITT. L. REV. 27 (1986).

159. *Id*. at 39.

State with evidence of a testimonial or communicative nature"—highlighting that evidence need not be traditional "testimony" in order to have a communicative value.[160] Similarly, Akhil Amar and Renée Lettow argued, "Unlike bodies, diaries are clearly communicative and testimony-like."[161] Diaries express statements like opinions, fears, or reflections, showing a communicative dimension not found in other physical objects.

In *Patane*, language used by Justice Thomas and Justice Kennedy in the plurality and concurrence seems to classify physical objects as objects alone, without any communicative value. Both Justice Thomas and Justice Kennedy emphasized the physical aspect of the gun in *Patane*, using language like the "nontestimonial physical fruits" of interrogation.[162] The emphasis on the nontestimonial nature of the Glock is telling. A purely physical object communicates its existence. But while a gun may not communicate more than its make, model, and individual characteristics, the contents of digital devices communicate much more. And the past understanding of a diary as an object that has both physical and testimonial value shows that the distinction between physical and testimonial is not as clear cut as Justice Thomas claims it to be.

Digital devices are simultaneously physical objects and containers of vast troves of data. For example, in a prosecution for a stolen laptop, the laptop itself would serve as nontestimonial physical evidence, like the gun in *Patane*. A laptop as an object invokes the same concerns as the gun in *Patane*. But a case focused on a laptop's contents invokes different concerns. If law enforcement violated *Miranda* to unlock the device, that creates a presumption that they accessed the device's contents through compulsion or coercion, meaning the person provided a vast trove of information to law enforcement as a result of that coercion. And the contents of that digital device can contain a vast array of information—like photos, audio recordings, notes, location tracking data, and more—that implicate much more than a single physical object.[163] Accordingly, the contents of a digital device raise different issues than a purely physical object like a gun.

A diary raises the same type of concerns. The existence of a diary itself is not troubling in the same way that its contents are troubling.[164] After all, when looking at the exterior of a diary, the contents remain unknown. The diary could

160. Schmerber v. California, 384 U.S. 757, 764 (1966).

161. Amar & Lettow, *supra* note 82, at 921. Amar and Lettow elaborated that "reading a person's diary (even if lawfully obtained) in open court, civil or criminal, can be seen as an additional invasion of privacy—an incremental 'search' of a man's soul, an additional 'seizure' of a woman's most intimate secrets—that once again calls for a careful judicial inquiry into the reasonableness of this public reading." *Id.*

162. United States v. Patane, 542 U.S. 630, 645 (2004) (Kennedy, J., concurring); *see also id.* at 643 (Thomas, J., plurality) ("Introduction of the nontestimonial fruit of a voluntary statement . . . does not implicate the Self-Incrimination Clause.").

163. *See United States v. Djibo*, 151 F.Supp.3d 297, 310 (E.D.N.Y. 2015). The *Djibo* court built off of *Riley* to explain the difference between the gun in *Patane* and the contents of a phone, explaining that "…as the *Riley* court held, a cell phone is not just a physical object containing information. It is more personal than a purse or a wallet, and certainly more so than the firearm that was used in evidence against Respondent Patane. It is the combined footprint of what has been occurring socially, economically, personally, psychologically, spiritually and sometimes even sexually, in the owner's life, and it pinpoints the whereabouts of the owner over time with greater precision than any tool heretofore used by law enforcement without aid of a warrant." *Id.*

164. *See* Amar & Lettow, *supra* note 82, at 921.

be empty, or it could contain highly personal details and recollections. The diary on its own is not testimonial. But its contents might be. And thus, insinuating that any physical object cannot contain any testimonial elements ignores the multifaceted nature of certain physical objects, like diaries, laptops, and cellphones.

Contents of digital devices look much closer to a diary than the business records in *Fisher* or the blood sample in *Schmerber*. Beyond just what one may write in a notes app, data on a phone can reveal personal information that a person may hesitate to even write down. For example, search records can show what information a person seeks to know—or things they might fear. Location tracking data can follow someone's movements. Health information can show a raised heart rate at a specific moment or the existence of a specific medical condition. Together, all these data points provide even more personal, private information than a diary would.

Going back to earlier understandings of criminal procedure rules to understand how digital evidence should be treated is not a new concept. Donald Dripps has argued that original understandings of the Fourth Amendment offered more protection to "papers" than "effects," and that searches of digital devices should be viewed similarly to the invasive searches of personal papers that the Founding Fathers feared.[165] In those invasive searches, a "pooling of small quantities of criminal evidence with large quantities of innocent and intimate information" resulted in searches that were more invasive than they were informative.[166] For this reason, Dripps argued that digital devices should be considered more like "papers" than "effects."[167]

Although the "diary" exception has received little discussion in recent years in Fifth Amendment jurisprudence, analogizing modern scenarios—like how the Fifth Amendment treats digital devices—to past problems helps communicate what is at stake when dealing with new technologies. This comparison helps show that the concerns created with Fifth Amendment protections for digital devices are not necessarily new concerns: instead, they are new manifestations of earlier debates on the scope of the Fifth Amendment. And connecting modern-day problems to earlier debates may help judges understand what is at stake when considering motions to suppress contents of digital devices that police access in violation of *Miranda.*

C. United States v. Marks *Dictates that Justice Kennedy's Concurrence Controls*

Patane is a fractured decision, and confusion on the common ground between the plurality and concurrence has led defense attorneys and courts to ignore a possible exception to the rule that physical fruits do not implicate the Fifth Amendment. In *Marks v. United States*, the Court explained how to

165. Donald A. Dripps, *Dearest Property: Digital Evidence and the History of Private Papers as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 52 (2013).

166. *Id.* at 51.

167. *Id.*

interpret the holding in a case when no opinion garners a majority of the justices.[168] The Court explained its rule, focusing on the narrowest grounds that unite a majority of the justices:

> When a fragmented Court decides a case and no single rationale explaining the result enjoys the assent of five Justices, "the holding of the Court may be viewed as that position taken by those Members who concurred in the judgments on the narrowest grounds . . . ."[169]

In *Patane*, that narrowest opinion belongs to Justice Kennedy.[170] Justice Kennedy seemed to signal that his opinion controlled by explicitly noting issues from Justice Thomas's opinion that he declined to address.[171] At the same time, he agreed with Justice Thomas's general conclusion, writing that "admission of nontestimonial physical fruits (the Glock in this case) . . . does not run the risk of admitting into trial an accused's coerced incriminating statements against himself."[172]

So, what's the difference between Justice Thomas's and Justice Kennedy's opinions, if Justice Kennedy agrees with the general conclusion? Justice Kennedy seems to back off from Justice Thomas's assertion that deterrence cannot matter in this context. Justice Kennedy instead wrote that "in light of the important probative value of reliable physical evidence, it is doubtful that exclusion can be justified by a deterrence rationale sensitive to both law enforcement interests and a suspect's rights during an in-custody interrogation."[173] When *Patane* was decided in 2004, Justice Kennedy doubted that a physical object could necessitate exclusion in order to deter law enforcement. But unlike Justice Thomas, he did not categorically state that deterrence was irrelevant to the inquiry.[174]

The narrower sections of Justice Kennedy's opinion have significance for how a court should decide a "digital fruits" case over fifteen years after *Patane*. While the Glock did not merit exclusion, Justice Kennedy leaves open the possibility that another object could, after weighing the need for deterrence compared to the item's probative value and reliability. Digital fruits may be that very situation where Justice Kennedy might have found that deterrence outweighs law enforcement need for access.

However, few courts have applied *Marks* to *Patane* or acknowledged the differences between Justice Thomas and Justice Kennedy's opinions.[175] Only two circuit court decisions have engaged *Marks* with the plurality and

---

168. United States v. Marks, 430 U.S. 188 (1977).

169. *Id.* at 193 (quoting Gregg v. Georgia, 428 U.S. 153, 169 n.15 (1976)).

170. *See* United States v. Patane, 542 U.S. 630, 645 (2004) (Kennedy, J., concurring).

171. *Id.* Justice Kennedy did not reach a conclusion about whether a *Miranda* violation actually occurred, or "whether there is 'anything to deter' so long as the unwarned statements are not later introduced at trial." *Id.*

172. *Id.*

173. *Id.*

174. *See id.* at 643 (Thomas, J., plurality) ("[A]n exclusionary rule cannot be justified by reference to a deterrence effect on law enforcement.").

175. *Compare* United States v. Phillips, 468 F.3d 1264 (10th Cir. 2006) (citing the plurality for the facts of the case and the concurrence for the holding) *with* the two cases dealing with digital devices: United States v. Oloyede, 933 F.3d 302, 309 (citing only to the plurality) *and* United States v. Hilton, 625 Fed. Appx. 754, 759 (citing only to the plurality).

concurrence in *Patane*. Writing for a unanimous Eleventh Circuit panel in *United States v. Jackson*, Judge William Pryor walked through how *Marks* applies to *Patane* and noted that Justice Kennedy did not agree with everything in Justice Thomas's plurality concurrence.[176] The Eleventh Circuit concluded that "the *Patane* plurality and concurrence agreed, at least, that *Miranda* does not require the exclusion of physical evidence that is discovered on the basis of a voluntary, although unwarned, statement," and admitted the physical evidence.[177] This result was unsurprising: *Jackson* involved a gun, just like in *Patane*.[178]

In *Tekoh v. County of Los Angeles*,[179] the Ninth Circuit recently applied *United States v. Davis*[180]—its en banc decision interpreting *Marks*—to *Patane*. The Ninth Circuit explained that Justice Kennedy's concurrence was narrower than the plurality, and that it "did not echo the plurality's broader discussion of *Miranda*, and it thus controls."[181] The Ninth Circuit also noted that Justice Kennedy's concurrence was "narrowly focused on the distinction between physical evidence and un-*Mirandized* statements," but did not delve any further into the differences between the concurrence and the plurality.[182]

Another court failed to walk through the application of *Marks*, but acknowledged the balancing factors in Justice Kennedy's concurrence.[183] In *United States v. Brathwaite*, a unanimous Fifth Circuit panel may have acknowledged that Justice Kennedy's concurrence could allow for some possible physical fruit to merit exclusion.[184] The Fifth Circuit cited Justice Kennedy's language that "it is doubtful that exclusion can be justified by a deterrence rationale sensitive to both law enforcement interests and a suspect's rights during an in-custody interrogation."[185] The court further wrote that in the present case—a felon in possession case where police located a gun after violating *Miranda*, just like in *Patane*—the "objectives" of the criminal justice system "do not require suppression."[186]

Just because courts have not applied *Marks* to *Patane* does not mean they should continue ignoring *Marks*. Richard Re has noted that "*Patane* has occasioned little *Marks* attention" even though "*Missouri v. Seibert*—another fractured *Miranda* decision that was issued the same day but without rule agreement—has become one of the most *Marks*'d cases ever."[187] Re hypothesizes that *Patane* has received relatively little application of *Marks* due

176. United States v. Jackson, 506 F.3d 1358, 1360–61 (11th Cir. 2007).
177. *Id.* at 1361.
178. *See id.* at 1360 ("There the officers found a shotgun, two shotgun shells, and Jackson's driver's license.").
179. Tekoh v. Cnty. of Los Angeles, 985 F.3d 713, 721 (9th Cir. 2021).
180. United States v. Davis, 825 F.3d 1014, 1024 (9th Cir. 2016) (en banc).
181. *Tekoh*, 985 F.3d at 721.
182. *Id.*
183. *See* United States v. Brathwaite, 458 F.3d 376, 382 n. 7 (5th Cir. 2006) (citing Kennedy's concurrence in *Patane*).
184. *Id.*
185. *Id.*
186. *Id.*
187. Richard Re, *Beyond the* Marks *Rule*, 132 HARV. L. REV. 1943, 2004 (2019).

to "rule agreement," where the Justice Thomas plurality and Justice Kennedy concurrence each "separately endorse a single legal rule."[188] But while Justice Kennedy largely endorses Justice Thomas's proposed legal rule, Justice Kennedy leaves room for a case that will prove him wrong and show that a deterrence rationale can support the exclusion of a physical object. The vast majority of cases applying *Patane* may never need to address this nuance, but digital devices require a deeper analysis of the factors Justice Kennedy considered when assessing whether exclusion based on a deterrence rationale could ever be warranted.

Justice Kennedy's opinion provides the basis for an interests-balancing approach that addresses both deterrence and the probative value of the evidence. Justice Kennedy stated that he was "doubtful" exclusion could ever be justified due to the "important probative value of reliable physical evidence," as exclusion would need a rationale "sensitive to both law enforcement interests and a suspect's rights . . . ."[189] This language highlights three main areas for concern for Justice Kennedy: the reliability of the physical evidence, law enforcement need for the evidence, and individual rights. Justice Kennedy doubted these interests could ever point to excluding a form of physical evidence.[190] But the Justices in *Patane*, decided in 2004 when only 65% of Americans owned a basic cellphone and smartphones did not exist, likely could not anticipate the future role of digital devices in daily life.[191] If anything can meet the balancing test in Justice Kennedy's concurrence, it will be the contents of digital devices.

Justice Kennedy's first concern, about the reliability of physical evidence, may cut towards excluding digital evidence. While it is tempting to say that digital evidence is highly reliable (after all, people rely on phones and computers every day to carefully log information), the reality is more nuanced. Returning to the diary example, Amar and Lettow argued that the diary exception in Fifth Amendment doctrine resulted partially from a diary's unreliability, as "[w]riters of diaries often fantasized or write in a personal short-hand easily misinterpreted."[192] Like a diary, contents of digital devices also have reliability issues. While digital fruits present a huge trove of information, that information often needs interpretation. For example, internet searches for how to do something—like how to buy drugs on the dark web while minimizing one's trace—can hint at someone seeking more information on something they've done, something they are considering doing, or an action by somebody else.

---

188. *Id.*

189. See United States v. Patane, 542 U.S. 630, 645 (2004) (Kennedy, J., concurring). It is possible that the district court in *Djibo* picked up on this language. One of the court's rationales for excluding the contents of the cellphone, and declining to apply *Patane*, was that "the incentive of deterring police misconduct is present in this case." United States v. Djibo, 151 F. Supp. 3d 297, 309 (E.D.N.Y. 2015). However, the *Djibo* court never specifically referenced Justice Kennedy's language about the possibility of deterrence outweighing law enforcement needs, nor did it conclude that Justice Kennedy's concurrence controlled.

190. *Patane*, 542 U.S. at 645 (Kennedy, J., concurring).

191. *See* Monica Anderson, *Technology Device Ownership: 2015*, PEW RSCH. CTR. (2015), https://www.pewresearch.org/wp-content/uploads/sites/9/2015/10/PI_2015-10-29_device-ownership_FINAL.pdf.

192. Amar & Lettow, *supra* note 82, at 921.

Further, a person's ability to unlock a phone does not mean they have always had exclusive control over a device. Just because law enforcement can attribute one piece of data to a phone does not mean that the phone's owner produced or knew of all the data. The Justices, in their personal experience, may believe that someone normally acquires a phone by heading out to the Apple Store and picking up a new iPhone. But many Americans acquire phones through means other than directly buying a brand new phone from a store. Many people in lower-income communities may share phones or computers out of necessity, or pass along devices with pre-existing data to friends or family members in need of a device.[193] People leaving jail or prison—who are at heightened risk of increased surveillance by the police due to their probation or parole status, not to mention racial profiling—often receive used phones from loved ones to help them through their first few days back in society.[194] Some may argue that people coordinating crimes would know better than to share their device with others. But police seek to review contents of digital devices in cases beyond high-level conspiracies, including in low-level cases often more related to poverty, like drug dealing or sex work.

Second, the police need for this evidence is relatively low. In the device-unlocking context, the need is not simply about the need for the contents, but rather the need to access the contents via asking an individual to unlock the device before administering *Miranda*. Police have other options. Orin Kerr and Bruce Schneier have outlined six different encryption workarounds—ranging from getting a court order requiring someone to decrypt the device to using software to guess a passcode.[195] Indeed, requiring police to delay unlocking a device by seeking a court order to compel decryption looks similar to the warrant requirement of the Fourth Amendment, and thus imposes relatively little burden, especially since under *Riley* officers will need to obtain a warrant to search contents of the digital device.[196]

Third, there is a strong need to protect individual rights. The *Patane* dissent's fear that officers will flout *Miranda* when physical evidence is key is heightened in the context of digital evidence. The *Patane* dissent, while focusing on a case where the physical evidence was crucial to a conviction for a felon-in-possession charge, only considered objects with a purely physical nature.[197] Accessing a cellphone leads to a huge trove of data that creates even more

193. Further, a 2012 study found that while people consider the contents of their phones to be private, 84% of people would either "definitely allow" or "probably allow" a spouse or another close family member to borrow their phone for a few hours. Jennifer M. Urban et al., *Mobile Phones and Privacy*, *in* BCLT RESEARCH PAPER SERIES (2012), https://ssrn.com/abstract=2103405.

194. *See generally* JOCELYN FONTAINE ET AL, FAMILES AND REENTRY: UNPACKING HOW SOCIAL SUPPORT MATTERS (Urban Institute 2012), https://www.urban.org/sites/default/files/publication/24921/1001630-Families-and-Reentry-Unpacking-How-Social-Support-Matters.PDF (describing the role of families in providing financial support upon reentry); *see also* Reuben Jonathan Miller, *How Thousands of American Laws Keep People 'Imprisoned' Long After They're Released*, POLITICO (Dec. 30, 2020, 4:30 AM), https://www.politico.com/news/magazine/2020/12/30/post-prison-laws-reentry-451445 (describing reliance on family and friends after release).

195. *See* Kerr & Schneier, *supra* note 22, at 989.

196. Riley v. California, 573 U.S. 373, 393 (2014).

197. *See* United States v. Patane, 542 U.S. 630, 645 (Souter, J., dissenting).

incentive to ignore *Miranda*. As described in *Djibo*, a cell phone passcode is the proverbial "key to a man's kingdom."[198]

Justice Kennedy left open the possibility of a situation where the kind of physical evidence at issue could warrant a deterrence need. He laid out factors he would consider in assessing whether deterrence is needed. Digital evidence requires deterrence in a way not required by a purely physical object like a gun.

V. CONCLUSION

In the wake of *Patane*, federal courts have interpreted the case as imposing a hardline rule that can never allow exclusion of a physical fruit. But as written, *Patane* can still protect the contents of digital devices following *Miranda* violations. Courts should interpret the Fifth Amendment to meaningfully adapt to the changing role of technology by declining to apply *Patane* to the contents of digital devices. Otherwise, a rule admitting the contents of devices regardless of whether an officer adhered to *Miranda* will encourage law enforcement to flout constitutional protections, rendering *Miranda* irrelevant when police rely upon the contents of digital devices to secure convictions and weakening Fourth Amendment protections at the same time.

198. United States v. Djibo, 151 F. Supp. 3d 297, 310 (E.D.N.Y. 2015).