Penalty Default Rules for Digital Searches: Why Courts Should Spur Legislative Action via Second-Order Regulation

Meghan Holloway†

We live in a data-rich age. But Fourth Amendment doctrines have failed to adapt to our current reality. Legal principles that evolved to cabin the scope of physical searches seldom constrain searches of digital devices. As a result, a warrant to search a digital device gives police officers unfettered access to all of our information. While many scholars have argued that courts should address this problem by adopting rules that directly limit the scope of digital searches, this Comment argues that some courts have already eschewed this approach in favor of rules that encourage legislatures to regulate digital searches. Legislative regulation of digital searches is preferable because the legislative branch is better equipped to deal with a rapidly evolving technological landscape. Unfortunately, however, courts have not gone about incentivizing legislative action effectively. This Article posits that if courts want to encourage legislatures to act, they should adopt a penalty default rule that disadvantages the police. Specifically, courts should temporarily ban the plain view doctrine during searches of digital devices until legislatures limit the scope of digital searches.

† AB 2016, Brown University; JD Candidate 2021, The University of Chicago Law School. Thanks to *The University of Chicago Law Review* editors and Professor Lior Strahilevitz for their helpful advice on this Comment.

INTRODUCTION

Paul is the subject of an investigation into tax fraud. Law enforcement officials believe that he participated in a scheme that defrauded the government of a significant amount of money. As part of the investigation, officers obtain a warrant to search Paul's home for evidence of this scheme. The warrant gives the officers the ability to search all of Paul's electronic documents and files for evidence of the crime. When the officers arrive to execute the warrant, they copy all of the data from Paul's laptops, external hard drives, phones, and tablets. The copied devices contain all of Paul's emails, phones, documents, text messages, and browsing history. The data show officers where Paul was on any given day, how long he spent looking at a given website, and what files he deleted. All of this information is taken to a police station

where forensic experts spend weeks looking through data from Paul's devices. While the warrant only authorizes officers to look for evidence of tax fraud, the experts look at every file, photo, text, or website on that computer—even though evidence of tax fraud would likely be in a Word document or PDF. The officers find evidence of Paul's tax evasion, but they also find evidence that he illegally purchased marijuana and viewed pirated *Game of Thrones* episodes. This additional evidence results in new criminal charges.[1]

Instinctually, the officers' expansive search of Paul's devices feels intrusive and unnecessarily invasive. Most Americans probably think that the Fourth Amendment should prevent officers from seizing all of a suspect's data and rummaging through it for evidence of a crime.

But while we may think that these police practices should be unconstitutional, that is not necessarily true. The Fourth Amendment, as it has traditionally been applied to physical searches, does little to limit the scope of a search of a digital device.[2] Constitutional doctrines that limit the scope of physical searches have not effectively adapted to the rapid pace of technological change. Fourth Amendment jurisprudence evolved to regulate searches of physical spaces, which can store only so much information. Digital devices, however, are able to contain amounts of data that would be impossible to casually store in an analog form. For example, one terabyte of data is analogous to all the books in a twelve-story library.[3] This storage capacity was inconceivable a generation ago.[4] Now, it is commonplace. Fourth Amendment doctrines that evolved to constrain the scope of a search of a house have not adapted to similarly constrain a search of digital libraries.

Faced with this emerging problem, courts could take one of two regulatory approaches: (1) regulate police behavior by giving officers a set of rules to follow, or (2) issue decisions that

---

[1] While Paul is fictional, this example is based on the facts of *United States v Burgess*, 576 F3d 1078, 1082–84 (10th Cir 2009) (upholding a conviction for child pornography charges based on a search pursuant to a warrant for images of drug trafficking).

[2] For a discussion of why the Fourth Amendment fails to effectively limit the scope of digital searches, see Part I.B.

[3] See Paul Ohm, Response, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va L Rev Brief 1, 6 (2011).

[4] See Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U Pa L Rev 373, 391 (2014).

encourage the executive or legislative branches to address the problem.[5] These two approaches are called first- and second-order regulations, respectively.[6] Most of the scholarship on digital searches has focused on how courts should reduce the scope of digital searches through first-order regulation. For example, commentators have argued that magistrate judges should prescribe digital search procedures in a warrant,[7] impose use restrictions on data,[8] and alter how warrant exceptions apply to digital searches.[9] This Comment takes a different approach by focusing on the second type of judicial regulation: how courts can incentivize legislatures to regulate digital searches.

First, this Comment shows that many federal courts have already eschewed first-order regulation in favor of encouraging legislative action. However, I argue that courts are attempting to spur legislative action the wrong way. Specifically, judges have undercut their pleas for legislative intervention by crafting rules that reflect existing police practices.[10] Regulators are not incentivized to propose alternatives when the existing rules do little to change police behavior. But without some policymaking intervention, the privacy-invasive status quo will persist: suspects like Paul will continue to experience intrusive digital searches that would be unconstitutional in other contexts.

If courts really want to motivate legislative change, they will have to take more drastic steps by adopting penalty default rules. Penalty default rules are rules that disadvantage certain parties to encourage those parties or other third parties (in this case,

---

5 See John Rappaport, *Second-Order Regulation of Law Enforcement*, 103 Cal L Rev 205, 213–14 (2015).

6 Id.

7 See Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates' Revolt*, 68 Emory L J 49, 82–93 (2018); Ohm, Response, 97 Va L Rev Brief at 11–12 (cited in note 3). But see generally Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va L Rev 1241 (2010) (arguing that imposition of such procedures by magistrate judges is unconstitutional and unwise).

8 See generally Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex Tech L Rev 1 (2015).

9 See Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv L Rev 531, 582–84 (2005); Andrew Vahid Moshirnia, Note, *Separating Hard Fact from Hard Drive: A Solution for Plain View Doctrine in the Digital Domain*, 23 Harv J L & Tech 609, 626–33 (2010). But see David J.S. Ziff, Note, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 Colum L Rev 841, 853–61 (2005).

10 See Part IV.B.

legislators) to act.[11] Historically, default rules that penalize the police have been effective at causing legislatures to enact laws that regulate criminal procedure.[12] This Comment argues that courts should learn from these successes and temporarily prohibit officers from invoking the plain view doctrine when searching a digital device until policymakers promulgate regulations that limit the scope of digital searches.

Part I explains why the Fourth Amendment, as it has traditionally been applied to physical searches, does little to limit the scope of digital searches. As a result, courts have had to fashion new rules to limit the scope of digital searches. Part II explains that courts can pursue two different regulatory strategies: (1) regulating police conduct directly, or (2) trying to incentivize legislatures to craft those regulations. Part III applies this framework to digital searches and argues that courts are trying to spur legislative regulation. But, as Part IV explains, courts are not going about this in the most effective way; instead, courts should adopt a penalty default rule that better incentivizes policymakers to limit the scope of digital searches.

I. THE FOURTH AMENDMENT PERMITS OVERLY BROAD DIGITAL SEARCHES

Today, digital devices are ubiquitous in everyday life. Be it a cell phone, a laptop, a smartwatch, or some other form of technology, many Americans have a digital device on them at all times.[13] We use our devices almost constantly, and each time we do, we leave a small trail of data behind.[14] As Justice Sonia Sotomayor cautioned, our data "reflect[ ] a wealth of detail about [our] familial, political, professional, religious, and sexual associations."[15] If stitched together, the information on our devices can paint a very

---

[11] See Tara Mikkilineni, Note, *Constitutional Default Rules and Interbranch Cooperation*, 82 NYU L Rev 1403, 1409–10 (2007). *Hadley v Baxendale*, 156 Eng Rep 145 (Ex 1854), exemplifies the idea: the court imposed a rule that makes a party in breach of a contract liable for foreseeable damages only in order to incentivize the party harmed by the breach to disclose potential damages in contract negotiations.

[12] See Part IV.A.

[13] Consumers in the United States, for example, look at their smartphones an average of fifty-two times per day. See *Global Mobile Consumer Survey, US Edition* *2 (Deloitte, 2018), archived at https://perma.cc/CYS5-9XRU.

[14] Consider Jacqueline Howard, *Americans Devote More than Ten Hours a Day to Screen Time, and Growing* (CNN, July 29, 2016), archived at https://perma.cc/X9E2-3LU3.

[15] *United States v Jones*, 565 US 400, 415 (2012) (Sotomayor concurring).

intimate picture of our lives—and digital devices are capable of storing vast amounts of information.

Searching a suspect's computer or phone has become a routine part of many modern criminal investigations.[16] But once an officer has a warrant to search a digital device, there are few safeguards that prevent officers from sifting through all of a suspect's data to find something incriminating. This Part explains why Fourth Amendment doctrine, as it has been applied to physical searches, fails to appropriately limit the scope of digital searches.

A. The Fourth Amendment Limits the Scope of Physical Searches

The Fourth Amendment guarantees individuals the right to be free from "unreasonable searches and seizures."[17] When the Framers drafted this phrase, the type of search they aimed to prohibit was a search pursuant to a "general warrant." This type of document, widely reviled, "allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[18] To ensure that such general, probing searches would not be possible in the new republic, the Framers adopted the Fourth Amendment. Consistent with the Framers' aim, courts have interpreted the Fourth Amendment to place limits on an officer's ability to conduct a generalized search of a physical space.

One way that the Fourth Amendment limits the scope of a physical search is by requiring an officer to obtain a warrant before beginning a search. A search is presumptively unreasonable if it is conducted without a warrant.[19] In order for a warrant to be valid, it must satisfy three constitutional criteria: (1) it must be supported by "probable cause"; (2) it must contain an officer's "[o]ath or affirmation"; and (3) it must "particularly describ[e] the

---

16 Consider H. Marshall Jarrett, et al, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* *ix (Department of Justice, 2009), archived at https://perma.cc/MLW8-8FH4.

17 US Const Amend IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

18 *Carpenter v United States*, 138 S Ct 2206, 2213 (2018), quoting *Riley v California*, 573 US 373, 403 (2014).

19 *Kentucky v King*, 563 US 452, 459 (2011), citing *Brigham City v Stuart*, 547 US 398, 403 (2006). There are numerous exceptions to this rule, such as the exigency exception and the automobile exception. See *Missouri v McNeely*, 569 US 141, 148–49 (2013) (discussing the scope of the exigency exception); *California v Acevedo*, 500 US 565, 579–80 (1991) (discussing the scope of the automobile exception). In these situations, a warrant is not required. However, this Comment focuses exclusively on the legal limitations on digital searches conducted pursuant to a warrant.

place to be searched, and the persons or things to be seized."[20] The last requirement—contained in the Particularity Clause—invalidates warrants that either fail to specify the items that will be seized or provide such a general description that the warrant sweeps in innocuous items.[21]

The Particularity Clause limits the scope of an officer's search because an officer can only search for the items listed in the warrant. If an officer looks for items not listed in the warrant, the officer is conducting a warrantless search, which is presumed to be unconstitutional. That means that an officer can only look in places where the items listed in a warrant could reasonably be found.[22] For example, an officer with a warrant to search a home for a stolen flat-screen television could only search in the places where that television would likely be found. A television cannot fit in a shoebox or a dresser drawer, so the officer could not open either container under the terms of the warrant.[23] As a result, the description in the warrant prevents officers from using warrants to engage in extensive searches for incriminating evidence.

Of course, during an otherwise lawful search, an officer may find incriminating evidence that is not listed in the warrant. When this happens, the officer is not required to turn a blind eye but instead can seize the evidence pursuant to the plain view doctrine.[24] Under the plain view doctrine, an officer can only seize evidence if he or she: (1) sees the evidence from a place where the officer is legally allowed to be; (2) is able to access the evidence legally; and (3) immediately realizes that the evidence is incriminating.[25] In other words, the plain view doctrine is "not [ ] an independent 'exception' to the Warrant Clause, but simply [ ] an extension of whatever the prior justification for an officer's 'access to an object' may be."[26] Therefore, for physical searches at least, the plain view doctrine only applies in the limited set of

---

20 US Const Amend IV.

21 See *United States v Ninety-Two Thousand Four Hundred Twenty-Two Dollars and Fifty-Seven Cents*, 307 F3d 137, 149 (3d Cir 2002).

22 See *United States v Ross*, 456 US 798, 824 (1982).

23 See id ("[P]robable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom.").

24 See *Horton v California*, 496 US 128, 133 (1990).

25 Id at 136–37.

26 *Texas v Brown*, 460 US 730, 738–39 (1983) (Rehnquist) (plurality).

circumstances when an officer discovers new evidence while searching for the items that were specified in the warrant.[27]

In sum, the Fourth Amendment has evolved over time to significantly limit the scope of a physical search. Its Particularity Clause restricts what an officer can look for when conducting a search pursuant to a warrant, and the plain view exception was crafted to be a narrow exception to this rule.

B. Fourth Amendment Doctrines Fail to Limit the Scope of Digital Searches

Although Fourth Amendment doctrines limit the scope of physical searches, the Particularity Clause and plain view exception have failed to have the same restrictive effect for digital searches. An officer with a warrant to search a digital device may look through all the data on a computer irrespective of what the warrant includes and seize anything that is incriminating. This Section discusses three problems with the current state of the doctrine.

1. The Particularity Clause does not limit the scope of warrants to search digital devices.

When the Particularity Clause is applied to digital searches, it does little to limit where an officer can search. As discussed previously, the Particularity Clause limits the scope of an officer's search because the officer can only search in the places where the evidence listed in the warrant is likely to be. But when an officer applies for a warrant to search a digital device, the description of what will be searched and seized is often general. Typically, warrants merely state the type of devices an officer plans to search, the format the digital evidence might be in (for example, a photo

---

[27] The plain view doctrine was intended to be a narrow exception to the warrant requirement. Its creation was driven by practical necessity. Without the plain view doctrine, an officer who finds incriminating evidence that is not listed in a warrant would have to stop searching and leave the scene to get a second warrant. The resulting delay jeopardizes both the officer's safety and the integrity of the evidence.

But at the same time, the Fourth Amendment's warrant requirement prohibits generalized searches for incriminating evidence. An overly broad plain view exception would swallow the need for a warrant. Therefore, in crafting the plain view exception, the Supreme Court aimed to strike a balance between a pragmatic concern about policing and a desire to protect the privacy of those being searched. See *Coolidge v New Hampshire*, 403 US 443, 467–78 (1971) (Stewart) (plurality).

or text file), and what crime the evidence will help prove.[28] For example, in *United States v Mann*,[29] officers obtained a warrant that allowed them to search a home for "video tapes, CD's or other digital media, computers, and the contents of said computers, tapes, or other electronic media, to search for images of women in locker rooms or other private areas."[30]

Courts allow for this level of generality because they recognize that more specificity is often impossible—it is just too difficult for an officer to know in advance what the incriminating files will be named or where those files will be on the hard drive.[31] Even seemingly reasonable limitations (such as restricting a warrant in a child pornography case to only include visual media) are impractical. For example, if a warrant only permitted an officer to search for image files, a suspect could easily evade a search pursuant to that warrant by saving images in documents.[32] Due to these challenges, courts consistently grant warrants to search an entire digital device. While courts recognize that a probing examination of every piece of data on a computer is in tension with the Particularity Clause, they acknowledge the practical necessity of permitting such a search.[33] Because digital devices are

---

[28] See, for example, *United States v Perez*, 2015 WL 3498734, *1 (ED Pa) ("A warrant authorizing the search for and seizure of, *inter alia*, all 'visual depictions' of child pornography 'on whatever medium,' and documents, emails, records, notes, and other materials related to child pornography, was subsequently issued.").

[29] 592 F3d 779 (7th Cir 2010).

[30] Id at 780–81.

[31] See, for example, id at 782 ("The problem with . . . computer searches lies in the fact that such images could be nearly anywhere on the computers. . . . [C]omputer files may be manipulated to hide their true contents."); *United States v Hill*, 459 F3d 966, 978 (9th Cir 2006) ("Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.").

[32] See also *United States v Williams*, 592 F3d 511, 522 (4th Cir 2010) ("To be effective, [a digital] search could not be limited to reviewing only the files' designation or labeling, because the designation or labeling of files on a computer can easily be manipulated to hide their substance.").

[33] See, for example, *United States v Upham*, 168 F3d 532, 535 (1st Cir 1999) (finding that, "[a]s a practical matter, the seizure and subsequent off-premises search of [a] computer . . . [i]s about the narrowest definable search and seizure reasonably likely to obtain the [evidence]"); *United States v Perez*, 712 F Appx 136, 139–40 (3d Cir 2017) (noting that courts have struggled to apply the particularity requirement to digital searches, but nonetheless upholding a search of all computer equipment found at a particular address); *United States v Stabile*, 633 F3d 219, 237 (3d Cir 2011) (discussing how broad searches of hard drives may be necessary to combat attempts to conceal criminal activity, but noting that "granting the Government a *carte blanche* to search *every* file on the hard drive impermissibly transforms a limited search into a general one") (quotation marks omitted);

such rich sources of evidence, courts are unwilling to conclude that warrants to search entire digital devices violate the Particularity Clause.[34] As a result, a warrant to search a digital device often gives an officer complete access to search everything on that device.

2. Police procedures have evolved to give officers the time and tools to look through all the data on a digital device.

In theory, this broad access would not pose a threat to privacy if police departments were searching digital devices the same way that they search physical spaces. But the way officers search physical spaces doesn't work for digital devices. As a result, officers have adopted a different set of search protocols for digital searches that give officers the ability to search through all the data they seize.

When officers search physical spaces, they go to the location listed in the warrant and search that site for evidence. For example, the police might go to an office and stay at that office until they search through all the documents for evidence of tax fraud.[35] An officer cannot follow the same procedure when searching a computer. Computers can store billions of pages of information.[36] Reading through all that information would take weeks.[37]

United States v Richards, 659 F3d 527, 538–40 (6th Cir 2011) (explaining that "federal courts have rejected most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers"). But see *United States v Galpin*, 720 F3d 436, 447–48 (2d Cir 2013) (finding that a warrant to search a digital device was overbroad because it allowed for the seizure of materials unrelated to the criminal offense specified in the warrant).

[34] See, for example, *Upham*, 168 F3d at 535 (upholding a warrant that authorized the search of "any and all computer software and hardware" found at a particular location); *Williams*, 592 F3d at 522 (stating that a computer search "must, by implication, authorize at least a cursory review of each file on the computer"); *Mann*, 592 F3d at 782–83 (upholding a search warrant for an entire computer because the materials sought in the warrant "could be essentially anywhere on the computer"); *Hill*, 459 F3d at 973 (same); *United States v Burgess*, 576 F3d 1078, 1092–93 (10th Cir 2009) (recognizing Fourth Amendment concerns implicated by computer searches, but explaining that "a computer search may be as extensive as reasonably required to locate the items described in the warrant").

[35] See, for example, *United States v Hillyard*, 677 F2d 1336, 1338–39 (9th Cir 1982) (describing a warrant issued in an investigation for stolen vehicles that authorized police to "search all motor vehicles and heavy equipment found on [defendant's] premises").

[36] Ohm, Response, 97 Va L Rev Brief at 6 (cited in note 3).

[37] See FRCrP 41(e)(2), Advisory Committee's Notes to the 2009 Amendment ("Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location.").

As a result, police officers use a different process to search through digital devices. Instead of conducting the search on location, officers make a copy of all the digital devices listed in the warrant and then search through the copies at the station.[38] This process is called a two-stage search and is unique to searches of digital devices.[39] At the station, officers will use different forensic search tools to find evidence that is responsive to the warrant.[40] For example, an officer may run all the files through an algorithm that sees if any of them match a database of innocuous and incriminating files.[41] An officer may then use keyword searches to find text files that relate to the subject of the warrant.[42] Or the officer might restore the suspect's internet history during the relevant investigatory period.[43] The Fourth Amendment does not significantly limit how long an officer can search through a copy of a digital device at the police station.[44] As a result, two-stage searches give officers a prolonged period of time to find incriminating needles in haystacks of data.

3. The plain view doctrine, when applied to digital searches, is no longer a narrow exception to the warrant requirement.

The plain view doctrine further expands the scope of digital searches by allowing officers to seize whatever they find on a computer. As discussed previously, to invoke the plain view doctrine, officers must satisfy three conditions. They must: (1) see the evidence from a place where they are legally allowed to be; (2) be able to access the evidence legally; and (3) immediately realize that the evidence is incriminating.[45] Unfortunately, in the digital

---

[38] See Jarrett, et al, *Searching and Seizing Computers* at *86 (cited in note 16); Kerr, 48 Tex Tech L Rev at 6–7 (cited in note 8).

[39] See FRCrP 41(e)(2)(B).

[40] See Jarrett, et al, *Searching and Seizing Computers* at *86 (cited in note 16); Kerr, 48 Tex Tech L Rev at 6–7 (cited in note 8).

[41] See Kerr, 119 Harv L Rev at 546 (cited in note 9).

[42] Id at 545–46.

[43] Id at 542.

[44] Because computers can store immense amounts of information, courts have been reluctant to limit how long an officer can spend searching for incriminating evidence on a digital device. See, for example, *United States v Mutschelknaus*, 564 F Supp 2d 1072, 1077 (D ND 2008) ("[T]he Federal Rules of Criminal Procedure do not require that the forensic analysis of computers and other electronic equipment take place within a specific time limit."); *United States v Burns*, 2008 WL 4542990, *8 (ND Ill) ("A delay must be reasonable, but there is no constitutional upper limit on reasonableness.").

[45] See *Horton*, 496 US at 136–37.

search context, these three conditions fail to meaningfully restrict the circumstances in which an officer can invoke the doctrine.

Generally speaking, an officer is allowed to search for and seize only what is described in a warrant.[46] But in digital searches, an officer with a warrant can legally open every single file and examine every piece of data on a computer.[47] This means that the officer always satisfies the first two prongs of the plain view doctrine: the officer is always in a place where he or she is legally allowed to be and is able to access the evidence legally. The result is that if an officer sees information that is clearly incriminating, he or she also satisfies the third prong and the plain view doctrine applies—regardless of how unrelated the information may be to the original investigation.

For example, if an officer with a warrant to search a computer for evidence of tax fraud searches for and finds child pornography, the officer is legally allowed to seize that evidence under the plain view doctrine. It does not matter that the child pornography is completely unrelated to tax fraud, or that evidence of tax fraud is likely to be found in documents whereas the evidence the officer found was photographic.[48] Because the officer had a warrant to search the computer and because digital evidence can be easily hidden, the officer was able to look at every file on the computer to find the evidence described in the warrant.[49]

C. Analyzing the Constitutionality of Digital Searches

For physical searches, the Fourth Amendment's Particularity Clause typically limits the scope of a search.[50] But with respect to digital searches, these doctrines place few restrictions on an officer's ability to look through everything on a computer. Moreover, because police search procedures have evolved, officers have the time to take advantage of this broad access. Police can spend weeks looking at a digital device for something incriminating.

---

46 See *Marron v United States*, 275 US 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.").

47 See Part I.B.1.

48 See *Horton*, 496 US at 135–36.

49 See notes 33–34 and accompanying text.

50 See *Ross*, 456 US at 824 (explaining that the permissible scope of a search is defined by the "object of the search and the places in which there is probable cause to believe that [the object] may be found").

And, if the officer finds this evidence, he or she can seize it under the plain view doctrine.

This type of generalized search creates a dilemma for courts. The Fourth Amendment was adopted because the Framers believed that general warrants posed a serious threat to our liberty.[51] Officers are not supposed to engage in "a general exploratory search from one object to another until something incriminating at last emerges."[52] Such a search violates the rights to privacy and property protected by the Constitution.[53] But in the digital context, the Particularity Clause and the plain view doctrine appear to allow officers to do just that—officers can search through everything on a digital device until they find something incriminating. As the Second Circuit cautioned:

> Once the government has obtained [a warrant] to search [a] hard drive, the government may claim that the contents of every file it chose to open were in plain view and, therefore, admissible even if they implicate the defendant in a crime not contemplated by the warrant. There is, thus, a serious risk that every warrant for electronic information will become, in effect, a general warrant.[54]

Because existing legal doctrines that have limited the scope of physical searches have to do the same for digital searches, courts have had to return to first principles to analyze the constitutionality of digital searches. Under the Fourth Amendment, all searches are required to be reasonable.[55] As discussed previously, a search is unreasonable if it consists of exploratory rummaging. In other words, a search must be narrowly tailored to find only the evidence specified in the warrant.[56] Courts have applied this principle to digital searches and have found that it requires that "the forensic steps of the [officer's] search process [be] reasonably directed at uncovering the evidence specified in the search warrant."[57] In other words, a digital search violates the Fourth

---

51 See *Carpenter*, 138 S Ct at 2213.

52 *Horton*, 496 US at 136, quoting *Coolidge*, 403 US at 466 (Stewart) (plurality).

53 See *Carpenter*, 138 S Ct at 2213.

54 *Galpin*, 720 F3d at 447 (quotation marks omitted).

55 US Const Amend IV. See also *King*, 563 US at 459 ("[T]he ultimate touchstone of the Fourth Amendment is reasonableness.") (quotation marks omitted).

56 See *Coolidge*, 403 US at 467 (Stewart) (plurality) (stating that the Fourth Amendment requires searches to be as "limited as possible" and not include "general, exploratory rummaging").

57 *United States v Loera*, 923 F3d 907, 917 (10th Cir 2019).

Amendment when it is not conducted in a way that tries to minimize the amount of nonresponsive information viewed by officers.[58] That said, this constitutional principle is relatively vague. It does not clearly tell an officer what he or she can and cannot do when conducting a digital search. Courts have attempted to fashion new rules that limit the scope of digital searches, but as the next Part will show, direct judicial regulation of digital searches can only go so far.

II. TWO WAYS COURTS CAN APPROACH DIGITAL SEARCHES: FIRST- AND SECOND-ORDER REGULATIONS

To prevent officers from engaging in unconstitutional behavior, courts typically craft rules that directly dictate how officers should behave. This process is called first-order regulation. But courts sometimes issue decisions that try to spur the enactment of new laws that govern officer behavior.[59] This second approach has been called second-order regulation. While first-order regulation is by far the most common type of rule in Fourth Amendment contexts, the Supreme Court has sometimes engaged in second-order regulation of searches.[60] This Part explains the differences between these two regulatory approaches. Part II.A provides examples of when courts have adopted the two different approaches to influence law enforcement behavior. Part II.B then further explores second-order regulation by discussing the types of rules courts can adopt to incentivize parties to act.

A. First- and Second-Order Regulations

In most Fourth Amendment cases, judges issue decisions that directly regulate law enforcement officials.[61] Courts create rules

---

58 See *Galpin*, 720 F3d at 451 (stating that a court assessing the reasonableness of a digital search should consider "the degree, if any, to which digital search protocols target information outside the scope of the valid portion of the warrant"); *United States v Townsend*, 649 F Appx 189, 191 (3d Cir 2016) (interpreting the Fourth Amendment as requiring the use of a search protocol that was "reasonably calculated to uncover suspect files while minimizing the likelihood of opening personal files unrelated to the investigation"); *Loera*, 923 F3d at 917 (stating that "[o]ur electronic search precedents demonstrate a shift . . . toward considering whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant"). See also *United States v Rarick*, 636 F Appx 911, 916 (6th Cir 2016); *Mann*, 592 F3d at 786; *United States v Johnston*, 789 F3d 934, 942 (9th Cir 2015).

59 See Rappaport, 103 Cal L Rev at 209–10 (cited in note 5).

60 See id.

61 See id at 215.

that officers must follow when searching or seizing property. If officers do not comply with judge-made rules for searching and seizing property, a court may later conclude that evidence the officers collect is inadmissible.[62] The body of judge-made rules that directly govern officer conduct is complex and detailed. For example, consider the litany of restrictions that the Supreme Court has placed on an officer's ability to stop and search a car. To illustrate: After stopping a car, an officer can search through the car if the officer has probable cause to believe evidence of a crime is inside.[63] The scope of the search will depend on whether the officer has probable cause to believe that just the trunk or the entire car contains evidence of a crime.[64] Alternatively, if the officer arrests the driver, the officer can search the passenger compartment if it is "reasonable to believe" it contains evidence of the crime of arrest.[65] Some of the rules governing automobile stops are clearer than others, but all the rules tell officers what to do when they face certain sets of facts. In other words, the defining characteristic of a first-order regulation is that it speaks directly to officers in the field.[66]

In lieu of directly speaking to police officers, courts will occasionally issue decisions that aim to stimulate nonjudicial policymaking.[67] Scholars like Professor John Rappaport have called this mechanism "second-order regulation."[68] Courts employing second-order regulation do not want to determine the rules that govern officer behavior; instead, these courts want to encourage the legislative or executive branches to adopt rules that are consistent with constitutional principles.[69]

Generally, courts choose to engage in second-order regulation instead of first-order regulation when judges believe that it is best to leave the regulatory decisions to the legislature. This often occurs when courts are considering a problem that is rapidly

---

62 This doctrine is known as the "exclusionary rule." See *Utah v Strieff*, 136 S Ct 2056, 2061 (2016) (defining the rule as "often requir[ing] trial courts to exclude unlawfully seized evidence in a criminal trial").

63 See *California v Acevedo*, 500 US 565, 579–80 (1991).

64 See id.

65 See *Arizona v Gant*, 556 US 332, 351 (2009).

66 See Rappaport, 103 Cal L Rev at 215 (cited in note 5).

67 See id at 218. See also Mikkilineni, Note, 82 NYU L Rev at 1404–05 (cited in note 11) (analyzing the extent to which the Court is able to incentivize legislative regulation).

68 Rappaport, 103 Cal L Rev at 214–15 (cited in note 5).

69 See id.

evolving or is already the subject of pending legislation.[70] It can also occur when judges think they lack the expertise necessary to effectively craft rules on a subject.[71]

A good illustration of second-order regulation is the Supreme Court's treatment of inventory searches.[72] An inventory search is a search that occurs after an officer has impounded a car.[73] During such a search, the officer will catalog everything in the vehicle, making note of anything valuable, illegal, or dangerous that is discovered. In *South Dakota v Opperman*,[74] the Supreme Court held that inventory searches are constitutional if they are conducted "pursuant to standard police procedures."[75] But the Court did not dictate what those procedures must be. Instead, the Court required police departments to have *some* standard procedure that was not based on individualized suspicion.[76] Until police departments formulated such a policy, they could not constitutionally conduct inventory searches. By banning inventory searches until police departments adopted their own standard policies, the Court encouraged law enforcement departments to self-regulate.[77]

B. Default Rules as a Type of Second-Order Regulation

When courts engage in second-order regulation, they often create default rules that regulate officer behavior until nonjudicial policymakers adopt an alternative policy. These default rules can take two forms. First, they can be placeholder default rules that are feasible in the interim but which courts hope will be supplanted by a legislatively enacted alternative.[78] Or, second, courts can enact a rule that makes a party worse off by default so that the party is motivated to act.[79] This second type is called a penalty default rule. When courts adopt either type of default rule—

---

70 See id at 263–64.

71 See id at 263.

72 See Rappaport, 103 Cal L Rev at 221 (cited in note 5).

73 See *Colorado v Bertine*, 479 US 367, 368–69 (1987).

74 428 US 364 (1976).

75 Id at 372.

76 See id at 375–76.

77 See *Bertine*, 479 US at 374 ("[R]easonable police regulations relating to inventory procedures administered in good faith satisfy the Fourth Amendment, even though courts might as a matter of hindsight be able to devise equally reasonable rules requiring a different procedure.").

78 See Rappaport, 103 Cal L Rev at 218–19 (cited in note 5); Mikkilineni, Note, 82 NYU L Rev at 1407–08 (cited in note 11); John Ferejohn and Barry Friedman, *Toward a Political Theory of Constitutional Default Rules*, 33 Fla St U L Rev 825, 850–52 (2006).

79 See Mikkilineni, Note, 82 NYU L Rev at 1409–10 (cited in note 11).

placeholder or penalty—they do so to enable legislatures to replace the default rules with alternative policies.

1. Placeholder default rules.

A placeholder default rule is a rule that police departments have to follow until nonjudicial policymakers adopt a constitutional alternative.[80] An example of this approach is the Supreme Court's treatment of post-indictment lineups. In a post-indictment lineup, police ask a witness to identify the perpetrator of a crime from a group of people. In *United States v Wade*,[81] the Supreme Court held that postindictment lineups were unconstitutional if the suspect did not have a lawyer present to ensure the lineup was conducted fairly.[82] While this holding created a rule for officers to follow, the Court stated that the rule was replaceable: "[O]ther regulations, such as those of local police departments, which eliminate the risks of abuse and unintentional suggestion at lineup proceedings and the impediments to meaningful confrontation at trial may [ ] remove the basis" for requiring counsel to be present.[83] In other words, the attorney requirement was an interim rule that police departments could replace with another rule that minimizes bias in lineups. To make its point crystal clear, the Court included several alternative policies suggested by commentators or followed by other nations that police departments could adopt in the footnotes of its opinion.[84] By leaving the door open to other rules, the Court gave police departments the option to replace its articulated rule with alternatives.[85] This facilitation of divergence is what distinguishes default rules from direct regulation: police are encouraged to replace default rules, while they are supposed to perpetually follow direct regulations.

2. Penalty default rules.

Penalty default rules make a party worse off by default to motivate the party to act.[86] Originally conceptualized by Professors Ian Ayres and Robert Gertner, penalty default rules were

---

80 See Ferejohn and Friedman, 33 Fla St U L Rev at 850–52 (cited in note 78).
81 388 US 218 (1967).
82 See id at 237.
83 Id at 239.
84 See id at 236–37 nn 26, 29, 30.
85 See Ferejohn and Friedman, 33 Fla St U L Rev at 851 (cited in note 78).
86 See Mikkilineni, Note, 82 NYU L Rev at 1409 (cited in note 11).

first described in contracts.[87] But in recent years, commentators have argued that penalty default rules can be found in constitutional law as well.[88] For example, in *Barker v Wingo*,[89] the Supreme Court held that if a defendant is not given a speedy trial, the Sixth Amendment is violated.[90] But rather than remedy the constitutional violation through direct regulation, the Court adopted a default rule that was particularly undesirable for the government: the indictment must be dismissed if a defendant is not given a speedy trial.[91] Concerned that defendants who would otherwise be convicted would go free under *Barker*, Congress acted by passing the federal Speedy Trial Act.[92] In other words, the Court motivated the legislature to regulate criminal procedure by adopting a penalty default rule.[93]

In summary, second-order regulations are judicial decisions that incentivize nonjudicial policymakers to regulate police conduct. They might prohibit a police tactic entirely as a penalty default or provide for a placeholder rule. But whatever tactic a court employs, the underlying purpose of a second-order regulation is to encourage the other branches to regulate officer behavior. The remainder of this Comment will show not only that courts are already using second-order regulation, but also that second-order regulation is a more promising tool to combat intrusive digital searches than first-order regulation.

III. THE JUDICIAL EMBRACE OF SECOND-ORDER REGULATION

As discussed in Part I, digital searches pose unique Fourth Amendment challenges: police search procedures have evolved to enable officers to sift through vast amounts of data, while traditional legal doctrines do little to narrow the expanding scope of digital searches. This Part shows that courts have already embraced second-order regulations to address this problem.

---

87 See Ian Ayres and Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 Yale L J 87, 91 (1989). But see generally Eric A. Posner, *There Are No Penalty Default Rules in Contract Law*, 33 Fla St U L Rev 563 (2005).

88 See, for example Ferejohn and Friedman, 33 Fla St U L Rev at 846–47 (cited in note 78); William J. Stuntz, *Of Seatbelts and Sentences, Supreme Court Justices and Spending Patterns—Understanding the Unraveling of American Criminal Justice,* 119 Harv L Rev F 148, 155 (2006).

89 407 US 514 (1972).

90 See id at 522.

91 See id.

92 Pub L No 93-619, 88 Stat 2076 (1975), codified at 18 USC §§ 3152–56, 3161–74.

93 See also Mikkilineni, Note, 82 NYU L Rev at 1411–12 (cited in note 11).

Part III.A describes how courts have conveyed that they are ill equipped to dictate how police officers should conduct searches in a rapidly evolving technological environment. As a result, courts have not been willing to directly regulate digital searches. Instead, courts have increasingly asked the legislative or executive branches to step in and craft rules for officers to follow when searching digital devices. To that end, Part III.B argues that courts have opted for second-order regulation and adopted a set of default rules. These rules aim to regulate digital searches while still giving legislators the ability to supplant the rules with alternatives.

A. Courts Want Legislatures to Regulate Digital Searches

To ensure that police conduct complies with constitutional principles, courts often directly regulate officer behavior.[94] But when opportunities arise to directly regulate the way officers conduct digital searches, courts have explicitly refused to do so. For example, federal courts have consistently rejected arguments that warrants to search digital devices must include search protocols.[95] Instead, some circuits have asked legislatures to step in and restrict the scope of digital searches.

Search protocols are procedures that officers must follow when conducting a search.[96] A search protocol may limit how long data can be stored or dictate the steps an officer must follow when conducting a search.[97] In theory, search protocols limit the scope

---

94 See Rappaport, 103 Cal L Rev at 215 (cited in note 5).

95 See, for example, *United States v Richards*, 659 F3d 527, 539 (6th Cir 2011) ("[G]iven the unique problem encountered in computer searches, and the practical difficulties inherent in implementing [ ] search methodologies, the majority of federal courts have eschewed the use of a specific search protocol."). See also, for example, *United States v Cartier*, 543 F3d 442, 447–48 (8th Cir 2008) (finding that a warrant to search a computer did not violate the Fourth Amendment's warrant clause despite lacking a "specific search strategy"); *United States v Stabile*, 633 F3d 219, 240 (3d Cir 2011) (same); *Mann*, 592 F3d at 785 (same); *United States v Russian*, 848 F3d 1239, 1245 n 1 (10th Cir 2017) (same); *United States v Khanani*, 502 F3d 1281, 1290–91 (11th Cir 2007) (same); *Richards*, 659 F3d at 538 n 9 (collecting cases). While state courts also apply Fourth Amendment principles to police conduct, this Comment focuses on the approach taken by federal courts.

96 See Kerr, 96 Va L Rev at 1248–49 (cited in note 7). See also *In re the Search of Premises Known as: Three Hotmail Email Accounts*, 2016 WL 1239916, *2 (D Kan) (defining a search protocol as "a document submitted by the government explaining to the Court how it will conduct its search"); *In re the Search of Apple iPhone, IMEI 013888003738427*, 31 F Supp 3d 159, 166 (DDC 2014) (stating that a search protocol is "an explanation of the [ ] methodology the government will use to separate what is permitted to be seized from what is not").

97 See Kerr, 96 Va L Rev at 1249 (cited in note 7).

of a search in the same way that the Particularity Clause does—by making officers declare ex ante what they are looking for and how they will find it.[98] For a brief period, commentators thought that including search protocols in warrants would become the norm. In *United States v Comprehensive Drug Testing, Inc*,[99] the Ninth Circuit briefly mandated that every warrant application to search a digital device contain search protocols.[100] However, few circuits elected to follow its approach.[101] Even the Ninth Circuit ultimately backtracked: the circuit reversed its stance within a year, revising the opinion and relegating the controversial approach to nonbinding guidance.[102]

Many courts refused to require search protocols because they were concerned that direct regulation would be ineffective.[103] Courts were concerned that they would get the protocols wrong and thereby unduly hamper the effectiveness of law enforcement.[104] To be effective, a search protocol must be narrowly tailored so that it limits the scope of a search. But if the protocol is too restrictive, it can prevent an officer from finding relevant evidence hidden on a device.[105] Striking the right balance is difficult in part because, as discussed previously, digital evidence can be easily disguised.[106] To make matters worse, many magistrate

---

98 See, for example, Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv J L & Tech 75, 85–89 (1994). The legal hook for this argument is that warrants to search digital devices are overbroad because they allow officers to search through lots of innocuous materials. See id at 86. One way to limit the scope of a search is by including search protocols that limit the way an officer can conduct the search.

99 579 F3d 989 (9th Cir 2009) (en banc) (*CDT II*).

100 See id at 1006–07.

101 Both the Third and Seventh Circuits explicitly rejected the approach, finding it ill-advised. *Stabile*, 633 F3d at 241 n 16; *Mann*, 592 F3d at 785. Other circuits similarly arrived at this conclusion, albeit less explicitly. See, for example, *Richards*, 659 F3d at 539; *Cartier*, 543 F3d at 447; *Russian*, 848 F3d at 1245 n 1; *Khanani*, 502 F3d at 1290.

102 See generally *United States v Comprehensive Drug Testing, Inc*, 621 F3d 1162 (9th Cir 2010) (en banc) (*CDT III*). The requirement to use specific search protocols shifted from the lead opinion to a concurrence. See id at 1178 (Kozinski concurring). While the Ninth Circuit provided no official explanation for its change, the radical nature of *CDT II*'s guidance and its poor reception by other circuits immediately following the opinion may have contributed to the circuit's decision. See also *Untied States v Schesso*, 730 F3d 1040, 1049 (9th Cir 2013) (holding that the guidance from *CDT III* was only advisory and that warrants to search digital devices were still valid without search protocols).

103 See, for example, *United States v Burgess*, 576 F3d 1078, 1094 (10th Cir 2009) ("[I]t is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives.").

104 See, for example, id at 1092. See also *Mann*, 592 F3d at 785; *Richards*, 659 F3d at 538, quoting *Stabile*, 633 F3d at 237.

105 See Kerr, 96 Va L Rev at 1249 (cited in note 7).

106 See Part I.B. See also *Burgess*, 576 F3d at 1092–93.

judges are less familiar with forensic search tools than police officers are.[107] This lack of familiarity makes it difficult for a judge to know whether the search tool gives the officer access to a breadth of information that may or may not be responsive to the warrant. For example, in *United States v Schlingloff*,[108] a district judge granted a motion to reconsider after learning more about how a digital search tool functioned.[109] The judge previously believed that an officer had no ability to view the images identified by a search tool; however, upon discovering that the officer could view the images when he enabled a certain feature, the judge had no choice but to conclude that the officer's search had exceeded the scope of the warrant.[110] Moreover, when a magistrate judge considers a warrant application, only the government briefs the judge. This lack of an adversarial briefing increases the likelihood that a judge—unfamiliar with the details of digital searches—will fail to accurately assess the privacy interests at stake.[111] Due to these challenges, circuit courts have consistently rejected proposals to require warrants to include search protocols. This resounding rejection of ex ante search protocols indicates courts' discomfort with direct regulation.

Courts are also hesitant to directly regulate because of the pace at which technology is evolving.[112] Courts are keenly aware that any decision they make today will bind future courts. Changes in technologies might render any decision about digital searches inapposite in the future. For example, in one case about a digital search, the Third Circuit briefly wondered how its decision might affect the outcome of future cases that involved

---

107 See Kerr, 119 Harv L Rev at 575–76 (cited in note 9).

108 901 F Supp 2d 1101 (CD Ill 2012).

109 Id at 1103:

> The Court initially denied the Motion to Suppress based in part on the mistaken belief that the filters in the FTK system had to be applied on an all or nothing basis and that the agent lacked the ability to disable the portion of the KFF specifically alerting to known child pornography or other contraband.

110 See id at 1103–06.

111 See *Russian*, 848 F3d at 1245 n 1 ("[W]e note that, like other circuits, we have previously declined to require a search protocol for computer searches, since courts are better able to assess the reasonableness of search protocols . . . 'where evidence and experts from both sides can be entertained and examined.'"). See also Kerr, 96 Va L Rev at 1283 (cited in note 7).

112 See *United States v Perez*, 712 F Appx 136, 140 (3d Cir 2017) (expressing concern that emerging and evolving technologies would render its decisions about the scope of digital searches inapposite); *United States v Ganias*, 824 F3d 199, 219–20 (2d Cir 2016) (invoking the legislative history of the Wiretap Act to argue that legislators should play a role in regulating digital searches given the pace of technological change).

algorithmic searches.[113] The court noted that police departments are increasingly using search tools (like the one officers used in the case) in which a computer performs the initial search so no human sees the evidence.[114] Similarly, in *CDT II*, the Ninth Circuit pondered the implications that cloud computing would have on Fourth Amendment jurisprudence.[115] For example, the court highlighted that a warrant to search "Google's [ ] servers to look for a few incriminating messages could jeopardize the privacy of millions."[116] Crafting rules that effectively apply to a range of rapidly changing technologies is like trying to hit a moving target: it requires a court to assess how technology interacts with precedent today while also predicting how technology will evolve in the future.

Given the challenges of regulating changing technologies, some federal courts have suggested that legislatures should play a more prominent role in limiting the scope of digital searches.[117] For example, in *United States v Ganias*,[118] the Second Circuit, sitting en banc, discussed the difficulties of regulating searches of digital devices and asked for legislative intervention: "[W]e seek [ ] to suggest that search and seizure of electronic media may . . . merit . . . legislative analysis; courts need not act alone."[119] The Third Circuit has also expressed dissatisfaction with the lack of legislative involvement in addressing these issues. It urged Congress or the executive branch to step in to enact statutes that better address the problem of the "proverbial digital haystack."[120]

While judges may be able to weigh the privacy and law enforcement interests at a high level, many federal courts have concluded that they should not craft detailed rules telling officers how to conduct a digital search. Courts acknowledge that digital searches threaten suspects' privacy interests. But they simply do not want to be in the business of telling officers what steps to follow when conducting a search. As a result, many circuits have refused to take advantage of opportunities to directly regulate

---

113 *Perez*, 712 F Appx at 140.

114 See id.

115 See *CDT II*, 579 F3d at 1002.

116 Id.

117 *Ganias*, 824 F3d at 219 ("Statutory approaches . . . have, historically, provided one mechanism for safeguarding privacy interests while, at the same time, addressing the needs of law enforcement in the face of technological change.").

118 824 F3d 199 (2d Cir 2016) (en banc).

119 Id at 220.

120 *Perez*, 712 F Appx at 140.

digital searches, preferring instead that the legislative and executive branches step in.

B. Courts Have Adopted Default Rules to Encourage Legislative Action

As the prior Section explained, some circuits believe that legislators, rather than judges, are best positioned to regulate digital searches—and that is why courts engage in second-order regulation. But to actually engage in second-order regulation, courts must issue decisions that legislatures can effectively supplant. This Section claims that courts have done just that for digital searches. To ensure that police officers conduct constitutional digital searches—by narrowly tailoring their searches to find only the evidence described in the warrant—courts have adopted various placeholder default rules. Courts have stated that digital searches are likely reasonable if the officer: (1) conducts a pyramidal search, (2) looks at nonresponsive material very briefly, and (3) gets a second warrant after finding incriminating evidence outside the scope of the original warrant.

1. Pyramidal search process for searching a digital device.

The Second,[121] Third,[122] Sixth,[123] Seventh,[124] Ninth,[125] and Tenth Circuits[126] have found that a search is often reasonable if officers follow a high-level procedure when they search through digital devices. The Tenth Circuit developed this approach. The

---

[121] See *United States v Galpin*, 720 F3d 436, 451 (2d Cir 2013) (instructing reviewing courts to consider whether an officer's search methodology targeted folders and files outside the scope of the warrant).

[122] See *Stabile*, 633 F3d at 239–40 (favorably discussing an officer search that began by indexing all the files on the computer, searching the indexed files, and only opening the files that were responsive to the search tools used).

[123] See *Richards*, 659 F3d at 540 (finding that it is reasonable for an officer to use search tools to sort all the files on a computer and then examine the ones that appear to be the target of the warrant).

[124] See *Mann*, 592 F3d at 784–85 (concluding that an officer's use of a search program to sort the files on a computer was appropriate, but that the officer exceeded the scope of the warrant when he opened files that the program deemed were not responsive to the warrant).

[125] See *United States v Johnston*, 789 F3d 934, 942 (9th Cir 2015) (holding that an officer's search was not unreasonable when he first conducted a forensic preview to preserve the data on a computer, then conducted a "bare minimum forensic scan" and used software to sort the files for those related to the warrant) (quotation marks omitted).

[126] See *United States v Loera*, 923 F3d 907, 919 (10th Cir 2019) (finding that a search using a digital image preview program was reasonable because it was the best way to search for images).

Tenth Circuit wants "an officer executing a search warrant to first look in the most obvious places and as it becomes necessary to progressively move from the obvious to the obscure."[127] Said differently, officers should start by using search tools to find files that clearly respond to the warrant and then broaden the search if the initial inquiries fail to discover evidence—following a process that resembles a pyramid.[128] By using a pyramidal search method, the Tenth Circuit reasoned that officers "avoid[ ] conducting the kind of 'sweeping, comprehensive search of a computer's hard drive' that [is] prohibited."[129]

Other circuits have embraced the Tenth Circuit's broad framework. They have similarly found that an officer reasonably targets his search by looking first at the files that most likely respond to the warrant.[130] In *United States v Stabile*,[131] for example, the Third Circuit applied this pyramidal framework to find that the steps an officer followed when looking for evidence of tax fraud were reasonable:

> [The officer] began by physically inspecting the hard drive and creating a copy of the drive to ensure that the original drive was not damaged or corrupted during the search. Next, [the officer] examined the file signatures to see if any files had been corrupted. He then conducted a 'hash value analysis' to see if any files had been copied. Finally, he examined suspicious and out-of-place folders. . . . These procedures demonstrate that [the officer] engaged in a focused search of the hard drives rather than a general search.[132]

2. Time spent looking at nonresponsive files.

Courts have also created a default rule governing how long officers can examine information that is unrelated to the purpose of the warrant. When an officer spends too much time looking for unrelated evidence, courts have concluded that the search was

---

127 *Burgess*, 576 F3d at 1094.

128 Officers should start by first analyzing "the file structure, next looking for suspicious file folders, then looking for files and types of files most likely to contain the objects of the search by doing keyword searches." Id. "For instance, unless specifically authorized by the warrant there would be little reason for officers searching for evidence of drug trafficking to look at tax returns (beyond verifying [that] the folder labeled '2002 Tax Return' actually contains tax returns and not drug files or trophy pictures)." Id.

129 *Loera*, 923 F3d at 918.

130 See notes 121–25.

131 633 F3d 219 (3d Cir 2011).

132 Id at 239–40.

unreasonable.[133] To illustrate, compare two cases from the Tenth Circuit: *United States v Carey*[134] and *United States v Burgess*.[135] In *Carey*, an officer found a folder of child pornography while searching for evidence of drug trafficking on a computer.[136] After finding the folder, the officer spent five hours opening every image to confirm that it was child pornography.[137] The Tenth Circuit found that this was unlawful because it was clear by the length of time that the officer had "abandoned" his search for the evidence listed in the warrant and instead had embarked on a search for evidence of child pornography.[138] By contrast, in *Burgess*, when an officer stumbled upon an image of child pornography, the officer immediately closed the file and sought a second warrant.[139] The court distinguished this case from *Carey* in part by highlighting the difference in time spent looking at the nonresponsive material: less than one minute was acceptable, but five hours was not.[140] The Second,[141] Third,[142] and Sixth Circuits[143] have embraced a view similar to the Tenth Circuit's. These courts have concluded that a digital search may be unreasonable if the

---

133 See, for example, *Loera*, 923 F3d at 919. This rule stems from the case law regulating searches of filing cabinets. In *Andresen v Maryland*, 427 US 463 (1976), the Supreme Court held that when an officer searches a filing cabinet, the officer can look at every document in a cursory manner to see if it is responsive to the warrant. Id at 482 n 11. Arguably, filing cabinets pose many of the same challenges that computers pose. Filing cabinets and computers both contain lots of files, some of which are incriminating and others innocuous. It is difficult to know without looking at all the files which ones are incriminating: the labels cannot be trusted as that would easily evade law enforcement. Due to these similarities, courts have applied this precedent to digital searches and extrapolated that looking at nonresponsive evidence for a prolonged period of time can make a search unreasonable.

134 172 F3d 1268 (10th Cir 1999).

135 576 F3d 1078 (10th Cir 2009).

136 *Carey*, 172 F3d at 1270–71.

137 Id at 1273.

138 Id.

139 *Burgess*, 576 F3d at 1094–95.

140 See id.

141 See *United States v Ulbricht*, 858 F3d 71, 101–03 (2d Cir 2017) (finding that it was reasonable for an officer to "cursorily" inspect the files that were responsive to the search terms to see if they responded to the warrant).

142 See *United States v Highbarger*, 380 F Appx 127, 131 n 5 (3rd Cir 2010) (contrasting an officer's behavior with that of the officer in *Carey*: the officer in this case immediately closed the file after realizing that it was not responsive to the warrant instead of continuing to look at it for hours).

143 See *United States v Rarick*, 636 F Appx 911, 916 (6th Cir 2016) (concluding that an officer's search was reasonable in part because he immediately stopped looking at the nonresponsive evidence after realizing that it was outside the scope of the warrant).

officer conducts more than a cursory examination of data unrelated to the warrant.

3. Second warrant requirement.

Finally, courts in the Third,[144] Fourth,[145] Sixth,[146] and Seventh Circuits[147] have considered a default rule requiring officers to obtain a second warrant once they find incriminating evidence unrelated to the original warrant.[148] If the officer fails to get a second warrant, the officer cannot expand the scope of the search to encompass the new evidence.[149] For example, in *United States v Rarick*,[150] an officer had a warrant to look for a particular video on a cell phone.[151] Pursuant to the warrant, the officer scrolled through the thumbnails of photos on the phone.[152] As he did so, he thought he saw photos that looked like child pornography but did not open those photos to confirm his suspicions.[153] He eventually came across "an image of a beige wall that he thought could be the start of the video."[154] At this point, he opened the video file and soon discovered that it was child pornography.[155] He immediately turned off the video, closed the phone, and obtained a second warrant before proceeding with the search.[156] Because the officer stopped to get a second warrant after discovering unrelated evidence, the court found that the officer did not violate the Fourth Amendment when he found the evidence of child pornography.[157] This rule—the second warrant requirement—often goes hand in

144 See *Highbarger*, 380 F Appx at 131 (finding that evidence outside the scope of a warrant was admissible because the officer stopped searching after discovering it and acquired a second warrant).

145 See *United States v Nasher-Alneam*, 399 F Supp 3d 579, 594 (SD W Va 2019) (declining to admit evidence because the government failed to obtain a second search warrant).

146 See *United States v Lucas*, 640 F3d 168, 178–80 (6th Cir 2011) (same).

147 See *Mann*, 592 F3d at 780, 786 (stating that it was "troubled" by the officer's failure to obtain a second warrant, but upholding the search on other grounds).

148 See, for example, *Lucas*, 640 F3d at 179–80; *Mann*, 592 F3d at 786; *Nasher-Alneam*, 399 F Supp 3d at 594–95. But see *Loera*, 923 F3d at 921 (stating that officers who come across "evidence of incriminating, nonresponsive material" do not need to get a second warrant to continue searching pursuant to the first warrant, but instead must navigate away from the nonresponsive material).

149 See, for example, *Lucas*, 640 F3d at 178–80.

150 646 F Appx 911 (6th Cir 2016).

151 Id at 916.

152 Id.

153 Id.

154 *Rarick*, 636 F Appx at 916.

155 Id.

156 Id.

157 Id.

hand with the rule limiting the amount of time spent looking at nonresponsive files. If an officer finds evidence that is outside of the scope of the warrant, he or she should stop looking at it, and, if the officer wants to then use that evidence, the discovery should be legitimized by getting a second warrant.

* * *

Together, these three rules demonstrate what search practices tend to be reasonable. Some circuits (like the Tenth Circuit) have adopted all three of these rules.[158] Other circuits have adopted just one or two. But consistent across all of these circuits is the finding that compliance with one or all of these rules does not necessarily mean that a search is constitutional.[159] The Tenth Circuit, for example, has called these rules "instructive," and has emphasized that compliance with them is not dispositive.[160] In other words, these rules are just indicia of reasonableness; there may be other rules that officers must follow when conducting a digital search in order for a search to be reasonable. Because these rules are not the sum total of how to judge whether a digital search is reasonable, they are just placeholder default rules that the legislatures can supplement. In fact, as demonstrated in Part III.A, some circuits have even expressly asked legislators to step in and enact policies that narrow the scope of digital searches.

IV. HOW COURTS SHOULD ENCOURAGE NONJUDICIAL REGULATION OF DIGITAL SEARCHES

To induce legislators to regulate digital searches, courts have crafted a set of default rules that policymakers can replace with alternatives. This Part argues that the specific rules that court have adopted in the context of the Fourth Amendment have undercut their calls for legislative involvement. As Part IV.A explains, courts historically have succeeded in catalyzing nonjudicial policymaking when they adopted penalty default rules that disfavored the police. When courts disrupted favorable status quo

---

158 See, for example, *Loera*, 923 F3d at 919–20; *Burgess*, 576 F3d at 1095.

159 See, for example, *Stabile*, 633 F3d at 241 (stating that the application of the reasonableness standard in the context of digital searches will "vary from case to case in a common-sense, fact-intensive manner"); *Richards*, 659 F3d at 538 (emphasizing that the application of the Fourth Amendment's reasonableness requirement will vary on a "case-by-case basis").

160 *Loera*, 923 F3d at 917.

policing practices, legislatures were spurred into action. But, as Part IV.B demonstrates, the default rules governing digital searches are not disruptive—they reflect the status quo. As a result, these rules are failing to incentivize legislative action. As Part IV.C explains, this outcome is problematic because legislatures are better equipped to regulate rapidly changing technologies than courts are. Given the benefits of legislative action, Part IV.D provides a way to more effectively engage in second-order regulation: penalty default rules.

A. Penalty Default Rules Encourage Nonjudicial Policymaking

As discussed in Part II, courts typically regulate officer behavior directly. That said, courts have occasionally tried to encourage legislative or executive branches to regulate officer conduct. These efforts at second-order regulation have not always been successful. But the most successful instances have something in common: courts more effectively encourage legislative action when they adopt penalty default rules that disadvantage the police.[161]

A quintessential example of courts using penalty default rules to incentivize legislative action is the legislative history of the Wiretap Act.[162] In *Berger v New York*,[163] the Supreme Court concluded that a state statutory scheme governing wiretaps violated the Fourth Amendment.[164] The statutory scheme allowed officers to engage in "a series of intrusions . . . pursuant to a single showing of probable cause."[165] Thus, "rather than being 'carefully circumscribed' so as to prevent unauthorized invasions of privacy," the state scheme "actually permit[ted] general searches by electronic devices."[166] General searches are, of course, unconstitutional. In striking down the statute, the Court made it clear that any future legislation governing wiretaps would have to provide strong mechanisms to protect suspects' privacy.[167] Eavesdropping

---

[161] Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn L Rev 349, 379 (1974) ("Under the stimulus or apprehension of constitutional decisions by the courts, legislatures may be moved to act."); Rappaport, 103 Cal L Rev at 260–61 (cited in note 5). See also Stuntz, 119 Harv L Rev F at 155 (cited in note 88).

[162] Omnibus Crime Control and Safe Streets Act of 1968, Pub L No 90-351, 82 Stat 197, codified as amended at 34 USC § 10101 et seq.

[163] 388 US 41 (1967).

[164] See id at 58–60.

[165] Id at 59.

[166] Id at 58.

[167] See *Berger*, 388 US at 63–64.

could be sanctioned under the Fourth Amendment if "its use was 'under the most precise and discriminate circumstances.'"[168] If the law could not be drawn narrowly, the Court cautioned that it would find that "the 'fruits' of eavesdropping devices [were] barred under the Amendment."[169] Fearing that law enforcement agencies would be unable to use wiretaps without legislative action, Congress passed the Wiretap Act. The Act both ensured officers could utilize wiretaps in the future while providing heightened privacy protections for suspects.[170] This win-win outcome can be traced to the Supreme Court's threat to impose a default penalty rule.[171] By threatening to adopt a rule that would significantly hamper law enforcement, policymakers were prompted to legislate.[172]

Default rules that do not penalize the police, however, have a much weaker track record of spurring nonjudicial regulation. *Miranda v Arizona*[173] has the dubious reputation as being both the most famous example of a placeholder default rule and also a prime example of what not to do if a court's goal is to incentivize legislative activity.[174] In *Miranda*, the Supreme Court held that officers must inform suspects of their rights and do so by reciting a disclaimer; otherwise, a suspect's statements are inadmissible in court.[175] That said, the Court did not intend for the warnings to be permanently followed by all police departments. In its decision, the Court stated that *Miranda* warnings must be given "unless other fully effective means are devised to inform accused persons of their right of silence and to assure a continuous opportunity to exercise it."[176] The Court went on to "encourage Congress and the States to continue their laudable search for increasingly effective ways of protecting the rights of the individual while promoting efficient enforcement of our criminal laws."[177] In other words, the Court saw its holding as creating a placeholder default rule:

---

168 Id at 63.

169 Id.

170 See 18 USC § 2518..

171 See Rappaport, 103 Cal L Rev at 260–61 (cited in note 5).

172 See Stuntz, 119 Harv L Rev F at 155 (cited in note 88).

173 384 US 436 (1966).

174 See Rappaport, 103 Cal L Rev at 260–61 (cited in note 5); Mikkilineni, Note, 82 NYU L Rev at 1422–24 (cited in note 11).

175 *Miranda*, 384 US at 444–45.

176 Id at 444.

177 Id at 467.

reading suspects their rights was just one of several constitutional alternatives police departments could employ.[178]

Yet, to this day, no state or locality has fully replaced the *Miranda* warnings with an alternative policy.[179] One reason for this failure was the emerging realization that, despite widespread fears, the warnings had no significant effect on discouraging arrestees from making statements to the police.[180] In fact, *Miranda*'s holding was actually quite favorable to the police: the warnings themselves do not discourage suspects from making incriminating statements, but the warnings do immunize the police from future Fifth Amendment challenges.[181] Because *Miranda*'s default rule was one that police departments could tolerate, few police departments and legislatures expended political capital to experiment with alternatives.

Miranda is thus an example of how placeholder default rules can fail to stimulate policymaking. Academics like Professor Rappaport argue that *Miranda* is indicative of a larger concern about placeholder default rules: if courts "implement[ ] a second-order holding through a default rule, and the default rule is politically palatable and not obviously more costly than its alternatives," it is unlikely the default rule will lead to legislative action.[182] In other words, politically palatable placeholder rules can "let politicians off the hook; once the Court weighs in, legislators can move on to other questions."[183] Penalty default rules, in contrast, are not politically palatable. When they disadvantage the police, like in *Berger*, they can incentivize legislative activity.

B. Existing Digital Search Default Rules Will Not Lead to Legislation

Unfortunately, the placeholder default rules courts have adopted to narrow the scope of digital searches is subject to the same pitfalls as the rules in *Miranda*. Default rules motivate lawmakers to act when they are politically unpalatable among key

---

[178] See Ferejohn and Friedman, 33 Fla St U L Rev at 851–52 (cited in note 78); Rappaport, 103 Cal L Rev at 224–25 (cited in note 5).

[179] See Rappaport, 103 Cal L Rev at 225 (cited in note 5).

[180] See id at 259; Stephen J. Schulhofer, Miranda*'s Practical Effect: Substantial Benefits and Vanishingly Small Social Costs*, 90 Nw U L Rev 500, 504–06 (1996).

[181] See Louis Michael Seidman, Brown *and* Miranda, 80 Cal L Rev 673, 744–46 (1992).

[182] Rappaport, 103 Cal L Rev at 258 (cited in note 5).

[183] Id, quoting David Alan Sklansky, *Killer Seatbelts and Criminal Procedure*, 119 Harv L Rev F 56, 64 (2006).

constituencies like police officers. In *Miranda*, the default rule was palatable to police. So too are the default rules for digital searches. These rules reflect existing police practices that are privacy invasive. Because these digital search default rules do not interfere with the status quo, police departments feel no need to lobby policymakers to pass laws to change them. Policymakers thus are not motivated to replace the default rules with alternatives.

Consider, for example, the general framework that courts have provided for how officers should conduct searches. As discussed in Part III.B.1, some circuits have found that a search is often reasonable if the officer conducts a pyramidal search: the officer should start by using search tools to look through the entire computer for folders and files that are responsive to the warrant, and visually inspect only those files that respond to the search tools. But this general framework fails to meaningfully change how officers conduct digital searches. Officers already follow this process. Police manuals instruct officers to first sort the information on the device, then use software to search for relevant materials, and finally open only the materials that respond to the search tools.[184] In other words, this default rule reflects current police practices. Because the rule reflects the status quo, policymakers have no incentivize to replace the default rule with alternatives. Police are happy with the current rule and so do not lobby for change.

But this placeholder default rule is not desirable in the long term. While requiring officers to start their searches in the most obvious places is an intuitive rule, it does little to limit the scope of a search. If an officer fails to find evidence in the most obvious places, the rule allows the officer to expand the scope of the search to increasingly less obvious, more tangentially related folders. As a result, the rule does not prevent an officer from looking through everything on a digital device if the suspect has hidden the evidence well—or worse, if the suspect has committed no crimes at all.

The second warrant requirement, like the pyramidal search rule, is another example of a default rule that will fail to incentive policymakers to act. It too reflects existing, privacy-invasive police practices. According to this default rule, officers must get a

---

[184] See, for example Jarrett, et al, *Searching and Seizing Computers* at *86 (cited in note 16); INTERPOL, *Global Guidelines for Digital Forensics Laboratories* *42–48 (May 2019), archived at https://perma.cc/4WZB-UU45.

second warrant after discovering evidence unrelated to the subject of the original warrant.[185] But law enforcement agencies already provide similar guidance to officers. For example, the Department of Justice recommends that officers stop searching and apply for a second warrant if they discover digital evidence substantially outside the scope of the original warrant.[186] Because the second warrant requirement reflects existing police practices, it is not going to incentivize lawmakers to act. Police officers are content with the status quo and so will not feel the need to lobby legislatures for a change.

The second warrant requirement also provides illusory privacy protections. This requirement only applies *after* an officer has found incriminating evidence. Because the officer found the evidence while conducting an otherwise lawful search, the officer can invoke the plain view doctrine and include the incriminating evidence in the application for a second warrant. When presented with a warrant application that includes evidence of the kind the warrant is for, a magistrate judge will certainly approve it. As a result, if an officer finds unrelated evidence, the officer will be able to get a second warrant and the scope of the search will inevitably expand. The second warrant requirement and the rule requiring officers to look at nonresponsive material briefly, therefore, do not prevent an officer from looking for incriminating evidence outside the scope of the warrant. In fact, they arguably encourage officers to engage in generalized searches because officers know that if they find incriminating evidence outside the scope of the warrant, they just need to apply for a second warrant in order to legitimize its discovery.

Unfortunately, both the pyramidal search rule and the second warrant requirement are two placeholder default rules that reflect existing privacy-invasive police practices. Because these rules reflect the status quo, police departments are not going to lobby legislators to replace the placeholder default rules. Without that push, it is not likely that legislatures will act. Individuals may be concerned that their privacy interests could be infringed by police officers, but for most of us, this concern is small. Because the citizenry is a diffuse interest group, it is unlikely that this

---

[185] See Part III.B.3.

[186] See Jarrett, et al, *Searching and Seizing Computers* at *91 (cited in note 16) ("[I]t remains prudent to seek a second warrant upon discovering evidence of an additional crime not identified in the initial warrant.").

small concern about digital searches will be sufficient to mobilize citizens to lobby policymakers for more privacy-protective rules.

In contrast, law enforcement officials are a discrete and highly organized interest group. They are better positioned to successfully lobby legislatures to change default rules. As a result, default rules that disadvantage the police are more likely to spur legislative action. But unfortunately, the placeholder rules courts have adopted for digital searches reflect the status quo and will not incentivize nonjudicial policymaking. Without the enactment of new laws that narrow the scope of digital searches, suspects will have to rely on existing Fourth Amendment doctrines—doctrines that provide minimal privacy protections against expansive digital searches.

C. Why the Legislature Should Regulate Digital Searches

For the reasons discussed in the previous Section, it is unlikely that legislatures will replace the existing digital search default rules with alternatives: they're too politically palatable to motivate legislators to act. Such an outcome, however, forgoes the benefits of having legislatures regulate government searches of digital devices.

A comparison of institutional competencies suggests that the legislative branch is better equipped to regulate digital searches than the judiciary. This is in large part due to the pace at which technology is currently evolving. A central conceit of our judicial system is that legal doctrines are established over time.[187] Courts craft rules through the process of repeatedly hearing similar cases. But, as Professor Orin Kerr has argued, this process is undermined when technology is changing so fast that courts cannot repeatedly hear the same cases. For example, the detailed body of rules governing car searches evolved over a period of decades.[188] Judges were able to craft these detailed rules because the underlying technology (cars) has not changed significantly over time.[189] By contrast, a court's decade-old analysis of a case involving cell phones may already be outdated.[190] Crafting detailed direct

---

[187] See David A. Strauss, *Common Law Constitutional Interpretation*, 63 U Chi L Rev 877, 888 (1996).

[188] See Part II.A. See also Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich L Rev 801, 862–83 (2004).

[189] See id at 860–64.

[190] See, for example, the facts of *Riley v California*, 573 US 373, 378–81 (2014).

regulations requires stability that is not present for digital technologies.[191]

Of course, the legislature is not immune from the challenges posed by rapidly changing technologies: elected officials are also unable to predict the future. For example, the legislature failed to foresee the privacy risk that silent video surveillance would pose when Congress enacted the Wiretap Act.[192] That said, the legislature is better equipped to regulate evolving technologies because it is able to regulate in an anticipatory fashion. In contrast, courts are required to rule on the facts before them. Due to the slow pace of litigation, judges are often ruling on the legitimacy of investigatory tactics that occurred several years in the past. While the delay may not matter for police tools that never go out of style (such as police interrogations) this delay can be significant when digital devices are involved. Courts of appeal are often crafting rules to resolve cases about old technologies. For example, in *Riley v California*,[193] Chief Justice John Roberts lamented the fact that the focus of one of the consolidated cases before the court was on a flip phone.[194] Chief Justice Roberts himself noted that the flip phone is functionally much more limited than current technology and is no longer in popular use.[195] Moreover, while judges can anticipate future changes, they are limited in their ability to issue rules unrelated to the controversy before them.[196] The legislature, in contrast, does not have these constraints: it is able to launch investigations into future trends and fashion rules in a proactive manner.

This is not to say that courts are completely unable to devise flexible rules that are able to anticipate technological changes. Courts have done so before. In *Kyllo v United States*,[197] for example, the Supreme Court anticipated the evolution of heat-sensing technology when crafting its holding.[198] But when either

---

191 Kerr, 102 Mich L Rev at 860–64 (cited in note 188) (arguing that the similar fact patterns that arise when technologies do not substantially change over time permit courts to strike the proper balance between law enforcement needs and privacy interests while providing clear, workable rules).

192 See Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 Fordham L Rev 747, 763 (2005).

193 573 US 353 (2014).

194 See id at 380.

195 See id at 385.

196 Kerr, 102 Mich L Rev at 868 (cited in note 188).

197 533 US 27 (2001).

198 See id at 36 ("[T]he rule we adopt must take account of more sophisticated systems that are already in use or in development.").

institution tries to predict the future, errors sometimes occur. Policymakers and judges may be wrong about what the future holds and craft rules that are poorly suited to emerging technologies. In the event of such an error, the legislative and executive branches are better able to change the rules than courts are.[199]

Stare decisis binds courts' ability to turn a new leaf when past approaches do not adequately solve new problems. For example, in the years leading up to the Supreme Court's landmark decision in *Riley*, many courts found that a police officer could search a suspect's phone incident to arrest.[200] These courts reached this conclusion because it seemed compelled by existing precedent: an officer can search any "containers" found on a suspect's person, and a cell phone is a container.[201] But a cell phone is distinct in many ways from other containers (like a backpack, for example): cell phones contain much more information, and that information can be highly personal.[202] Nevertheless, many circuits, recognizing the privacy interests at stake, concluded that under stare decisis, they could not reach a different holding.[203] As technology evolves, tensions will continue to build as old legal doctrines are applied to new problems. Due to limitations like stare decisis, courts are constrained in ways that legislatures are not, and thus are not as well positioned to regulate rapidly evolving technology as legislatures are.

Legislatures have other advantages as well: they are more democratically accountable than courts are. As a result, they may be better positioned to make the difficult value trade-offs inherent in regulating digital searches.[204] Moreover, legislatures can experiment with different ways to make these trade-offs. Different states with varying value preferences can choose to express those preferences with different statutory schemes.[205] Federalism

---

199 See Kerr, 102 Mich L Rev at 807 (cited in note 188) ("Legislatures can enact comprehensive rules based on expert input and can update them frequently as technology changes.").

200 See, for example, *United States v Flores-Lopez*, 670 F3d 803, 806 (7th Cir 2012); *United States v Finley*, 477 F3d 250, 259–60 (5th Cir 2007); *United States v Wurie*, 612 F Supp 2d 104, 110 (D Mass 2009), affd, 728 F3d 1 (1st Cir 2013), affd as consolidated in *Riley v California*, 573 US 353 (2014).

201 See, for example, *Flores-Lopez*, 670 F3d at 806.

202 See *Riley*, 573 US at 393–95.

203 See, for example, *Flores-Lopez*, 670 F3d at 806–08; *Wurie*, 612 F Supp 2d at 110.

204 See Kerr, 102 Mich L Rev at 858–60 (cited in note 188).

205 See generally Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath U L Rev 373 (2006).

famously creates laboratories of democracy. By contrast, variation is more of a bug than a feature of the federal judiciary: there is only one Fourth Amendment after all. Given the inherent uncertainty around the future of technology and the best way to manage rapid change, a mechanism that facilitates experimentation may be better suited to regulate digital devices. Recognizing this, Justice Samuel Alito has joined lower courts in asking legislators to step in and resolve Fourth Amendment questions raised by changing technologies: "Legislation is much preferable to the development of an entirely new body of Fourth Amendment caselaw for many reasons, including the enormous complexity of the subject, the need to respond to rapidly changing technology, and the Fourth Amendment's limited scope."[206]

D. Salvaging the Second-Order Approach

While it is unlikely that the courts' current approach will motivate executive or legislative policymaking, courts should not abandon their commitment to second-order regulation. To incentivize legislative actors to regulate digital searches, this Comment argues that courts should adopt a penalty default rule. As discussed in Part IV.A, penalty default rules that disadvantage police departments have effectively catalyzed legislative action in the past. This Comment argues that courts should learn from these successes and eliminate the plain view doctrine during searches of digital devices until policymakers narrow the scope of digital searches. This Section first explains why temporarily banning the plain view doctrine is possible. It then goes on to explain why doing so is normatively desirable.

1. Courts can eliminate the plain view doctrine for digital searches.

Courts can eliminate the plain view doctrine in the context of digital searches because doing so is consistent with the rationale for the exception. As explained in Part I.A, when the Supreme Court first articulated the plain view doctrine, it made clear that the doctrine was intended to be a narrow exception to the warrant requirement. It was never supposed to enable an officer to engage in "a general exploratory search from one object to another until

---

[206] *Carpenter v United States*, 138 S Ct 2206, 2261 (2018) (Alito dissenting). See also *Riley*, 573 US at 407–08 (Alito concurring).

something incriminating at last emerges."[207] However, because courts have interpreted the Particularity Clause to allow an officer with a warrant to search a digital device to look at everything on that device, the plain view doctrine is no longer a narrow exception. Instead, it enables officers to engage in the very behavior that the Supreme Court has repeatedly emphasized is unconstitutional.

A court can eliminate a judicially constructed exception that contributes to unconstitutional searches. The Supreme Court has done this before in the context of searches incident to arrest. The search incident to arrest doctrine is an exception to the warrant requirement: after an arrest, an officer is able to search a suspect and the suspect's belongings. But, in *Riley*, the Court eliminated the exception in the context of cell phones.[208] The Court concluded that allowing an officer to search a suspect's cell phone incident to arrest would be unreasonable under the Fourth Amendment: cell phones contain far too much highly sensitive personal information. Given the unique problems that digital searches pose, courts should similarly restrict the scope of the plain view doctrine and temporarily prohibit the application of the doctrine to searches of digital devices.

Permanently eliminating the plain view doctrine in the context of digital searches has gained some traction among scholars and courts. Kerr first tentatively proposed eliminating the plain view doctrine in 2005.[209] He argued that the plain view doctrine should not be applicable in digital searches because it was too powerful a tool in the age of big data for many of the reasons discussed in Part I.B.2.[210] Other commentators, taking a less absolutist view, have also embraced the general principle that the plain view doctrine is too powerful when applied to digital searches as they are presently regulated.[211] Then in 2009, the proposal to eliminate the plain view doctrine from digital searches was briefly considered by a circuit court. In *CDT II*, the Ninth

---

[207] *Horton v California*, 496 US 128, 136 (1990), quoting *Coolidge v New Hampshire*, 403 US 443, 466 (1971) (Stewart) (plurality).

[208] See *Riley*, 573 US at 403.

[209] See Kerr, 119 Harv L Rev at 582–84 (cited in note 9).

[210] See id.

[211] See, for example, David C. Behar, Note, *An Exception to an Exception: Officer Inadvertence as a Requirement to Plain View Seizures in the Computer Context*, 66 U Miami L Rev 471, 493 (2012) (proposing an inadvertence requirement for plain view computer searches); Moshirnia, Note, 23 Harv J L & Tech at 626–29 (cited in note 9) (proposing a crime-based balancing test for the exception).

Circuit, sitting en banc, endorsed Kerr's view and required officers to "forswear reliance" on the plain view doctrine.[212] While the circuit subsequently relegated this idea to advisory status,[213] the legal environment in which it was embraced has not changed significantly. Digital searches are just as broad in scope, and the same Fourth Amendment risks exist.

While such a temporary ban on invoking the plain view doctrine in digital searches might seem radical, similar penalty default rules have been employed by the Supreme Court in the past. For example, in *Barker v Wingo*, the Supreme Court held that if a defendant is not given a speedy trial, the Sixth Amendment is violated.[214] But rather than remedy the constitutional violation through direct regulation, the Court adopted a default rule that was particularly undesirable for the government: an indictment must be dismissed if a defendant is not given a speedy trial.[215] Concerned that defendants who would otherwise be convicted would go free under *Barker*, Congress acted by passing the federal Speedy Trial Act.[216] The Act replaced the diffuse standard that *Barker* created with a set of rules that courts had to follow. In other words, the Court's adoption of a penalty default rule motivated the legislature to regulate criminal procedure.[217]

Another example of a radical penalty default rule is the Supreme Court's decision in *Colorado v Bertine*.[218] In *Bertine*, the Supreme Court banned police departments from conducting inventory searches until they adopted uniform policies that regulated those types of searches.[219] Inventory searches are very important to law enforcement: police officers need to be able to search cars that they impound for safety reasons as well as law enforcement needs. Not wanting to forgo this useful tool, police departments across the country ensured that they had policies that sufficiently restricted their inventory searches.[220] Both of these examples illustrate that temporarily adopting rules with

---

[212] *CDT II*, 579 F3d at 998. See also id at 1006 (listing all the requirements for a digital search).

[213] See generally *United States v Comprehensive Drug Testing, Inc*, 621 F3d 1162 (9th Cir 2010) (*CDT III*).

[214] See *Barker*, 407 US at 522.

[215] See id.

[216] See note 92 and accompanying text.

[217] See Mikkilineni, Note, 82 NYU L Rev at 1411–12 (cited in note 11).

[218] 479 US 367 (1987).

[219] See id at 374 n 6.

[220] See id. See also Rappaport, 103 Cal L Rev at 221 (cited in note 5).

negative law enforcement consequences to incentivize policymakers to act is not as radical as it might initially seem.

2. Eliminating the plain view doctrine for digital searches is desirable.

While such decisions are rare, the Supreme Court has endorsed radical approaches when the severity of the problem warrants it. And the problem of overbroad digital searches is one that certainly warrants such action.[221] Unless policymakers act, a single warrant to search our digital devices will continue to give officers access to much of the data we produce on a daily basis. And given our increasing reliance on digital devices, such expansive access poses a significant threat to both our privacy and autonomy interests. Therefore, while the rules that legislatures enact may not be perfect, they certainly will be better than the status quo.

This rule—a temporary ban on using the plain view doctrine in digital searches—will be more effective than the existing default rules at incentivizing legislatures to act because it disrupts the policing status quo in a way that disadvantages law enforcement interests. As discussed in Part I.B.2, the plain view doctrine is an extremely powerful tool that officers can wield when searching digital devices. The doctrine allows officers to use any immediately incriminating evidence they discover when searching a laptop or phone. Without it, officers would be severely circumscribed in their ability to benefit from incriminating evidence that was not listed in a warrant. Because the plain view exception is so central to digital searches, a rule that prevents officers from relying on the plain view doctrine until such searches are regulated will cause police departments and their associated interest groups to lobby legislatures for the necessary regulation.

Some may worry that police departments may be too effective at lobbying, and the resulting legislative solution will be skewed toward law enforcement interests. This has occurred in the past. A famous example is the USA PATRIOT Act.[222] Following the 9/11 terrorist attacks, the Act was rushed through Congress due to strong lobbying from law enforcement advocates.[223] It contained a number of controversial provisions that tried to make fighting

---

[221] See Part I.B.

[222] Pub L No 107-56, 115 Stat 272 (2001).

[223] See Solove, 74 Fordham L Rev at 770–71 (cited in note 192).

terrorism easier at the expense of privacy interests.[224] However, the ultimate fate of the PATRIOT Act illustrates what can happen if legislation enables broad surveillance. When the public learned that provisions of the Act enabled the federal government to engage in massive surveillance of their telephone calls (known as the telephony metadata program), the ensuing outrage prevented the program from ultimately being reauthorized. While other provisions of the Act were renewed, public sentiment prevented the program from continuing.[225] Given the ubiquity of digital devices in everyday life, it is conceivable that a regulatory scheme that allowed police officers to engage in generalized searches of digital devices would face similar widespread hostility.

Furthermore, this provision does not eliminate the role of the federal judiciary entirely. Courts should still operate as a check on police practices that clearly violate the Fourth Amendment—even those sanctioned by law.[226] Under existing federal circuit court precedent, police officers have to reasonably tailor their searches to find only what is specified in the warrant.[227] A regulatory regime that did not require police officers to tailor their searches in this manner would violate the Fourth Amendment. In this way, judicial review will act as a backstop preventing truly privacy-invasive policy regimes from being enacted by legislatures.[228]

Of course, an easy response to this proposal is to point out the risk that the legislature will not respond to the penalty default

---

[224] See generally Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 Geo Wash L Rev 1145 (2004).

[225] See Jennifer Steinhauer and Jonathan Weisman, *US Surveillance in Place Since 9/11 Is Sharply Limited* (NY Times, June 2, 2015), archived at https://perma.cc/GNM8-PNRB.

[226] While some scholars have argued that legislation should alter the constitutional standard, this Comment does not do so. Instead, it argues that courts should incentivize legislatures to act consistently with what courts judge to be the constitutional principle. Here, the constitutional principle is that searches must be narrowly tailored to find only what is specified in the warrant. For a discussion about the merits and drawbacks of having courts adjust constitutional standards based on legislative action or inaction, see generally Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 Mich L Rev 1117 (2017).

[227] See Part I.C.

[228] That said, this Comment recognizes that it may be difficult for a court to know whether a given regulatory scheme sufficiently requires an officer to tailor search protocols to the objectives specified in a warrant. To some extent, it will require the court to make the same trade-offs between privacy and law enforcement interests that it is hesitant to do now.

rule at all—or if they do, legislatures will take years to forge a compromise that can be passed into law. Such a delay would effectively mean that the temporary elimination of the plain view doctrine from digital searches will become a permanent ban due to legislative inaction. For the reasons explained in Part IV.A, such an outcome is unlikely. But if it does occur, there is reason to conclude that permanently banning the plain view doctrine is not as untenable of a solution as one might initially fear.

First, banning the plain view doctrine prevents officers from being incentivized to conduct overly broad searches. As Kerr argues, "it would allow the police to conduct whatever search they needed to conduct (to ensure recovery) and then limit use of the evidence found (to deter abuses)."[229] Furthermore, police officers can still rely on the independent source and inevitability doctrines to utilize incriminating evidence that is outside the scope of a warrant.[230] Under these two doctrines, evidence can be admitted in court when the police officer had either an independent way to obtain the information or when the officer would have discovered the same evidence irrespective of the warrantless search.[231] While these two doctrines would not apply in every situation, they would at least mitigate the impact of the plain-view ban in some scenarios.

CONCLUSION

Fourth Amendment doctrine as it has been applied to physical searches is unable to manage the unique threat that digital searches pose to privacy. While these doctrines may adequately balance privacy interests against law enforcement needs in an analog environment, they do not do so in a digital one. In the absence of effective constitutional safeguards, a warrant to search a digital device enables the police to indiscriminately rummage through your data for evidence of criminal activity—the exact harm that the Fourth Amendment was adopted to prevent.[232]

To combat this problem, commentators have focused on ways that courts can modify existing Fourth Amendment doctrine to better protect our privacy interests. But few commentators have

---

[229] Kerr, 119 Harv L Rev at 584 (cited in note 9).

[230] See id.

[231] See *Murray v United States*, 487 US 533, 536–41 (1988) (discussing the independent source doctrine); *Nix v Williams*, 467 US 431, 440–48 (1984) (explaining the inevitable discovery doctrine).

[232] See *Carpenter v United States*, 138 S Ct 2206, 2213 (2018).

grappled with the reality that most courts are simply not interested in directly regulating digital searches. While courts acknowledge the real problems that digital searches pose, they do not feel well equipped to get into the minutiae of digital search procedures.

Instead, courts have asked legislatures to step in and directly regulate digital searches. Unfortunately, this request for legislative intervention is likely to go unanswered. Judges have undercut their pleas for assistance by fashioning default rules that reflect existing privacy-invasive police practices. Because these rules reflect the status quo, legislators will be unlikely to expend the political capital necessary to replace the default rules with alternatives.

To incentivize nonjudicial policymaking, courts should adopt a penalty default rule that is viewed as untenable by institutional actors. Specifically, courts should temporarily ban officers from invoking the plain view exception during digital searches until nonjudicial policymakers adopt alternative policies that narrow the scope of digital searches. While such an approach seems radical, it reflects the gravity of the privacy problem we face. In the digital age, our lives are increasingly dominated by our devices. In 2018, one study reported that 90 percent of the world's data was created in the last two years.[233] All this information is stored on our digital devices. Access to these devices therefore provides a highly intimate picture of our lives. Until we limit the ability of the government to search through our data, our personal privacy in the digital age is under threat.

---

[233] See Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read* (Forbes, May 21, 2018), archived at https://perma.cc/729P-6WHL.