The Constitutional Right to Deletion: The Latest Battle in the War of Technology v. Privacy

Kelsey Joy Smith*

ABSTRACT

This note explores the murky waters that surround the execution of search warrants on computer files in the twenty-first century and the effect on Federal Rule of Criminal Procedure 41. Currently, the Supreme Court provides severely limited guidance on the seizure of digital files that has allowed for prosecutorial overreach throughout the nation. While the Fourth Amendment and Federal Rules of Criminal Procedure provide citizens with protection against unreasonable searches and seizures, technology has eroded these protections. The attempt of several recent circuit court decisions to answer novel questions pertaining to Rule 41 and the Fourth Amendment illustrates the dire need for the Supreme Court to provide constitutional protection against unreasonable searches and seizures and the right to privacy.

I. INTRODUCTION

The Framers drafted the Fourth Amendment as a response to the British Crown's habit of effectuating general warrants that were "not grounded upon sworn oath[s] of specific infraction[s] by particular individual[s], and thus not limited in scope and application."[1] Executing general warrants, the King's officials were permitted to enter one's home and seize all of the homeowner's books and papers, hoping to find evidence

* Candidate for Juris Doctor, New England Law | Boston (2016); B.S. in Political Science at the University of Central Florida 2013. I would like to thank my parents Charles and Maureen, for their endless love and support. In addition, I would like to thank the editors and associates of Volumes 41 and 42 for their dedication and efforts in the publication of this Note.

[1] Maryland v. King, 133 S. Ct. 1958, 1980 (2013) (Scalia, J., dissenting); United States v. Galpin, 720 F.3d 436, 445 (2d Cir. 2013); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 536 (2005).

of criminal activity.[2] With that in mind, the Framers ensured that the Fourth Amendment barred general warrants.[3]

The text of the Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[4]

Thus, every search and seizure must be reasonable, and a warrant may only be issued if it describes, with accuracy, the place to be searched and the person or thing to be seized.[5]

The Fourth Amendment was drafted to regulate searches of homes and physical property; hence, ambiguity exists where law enforcement officials encounter evidence contained within computer hard drives and electronic storage devices.[6] Stemming from the lack of clarity regarding Fourth Amendment procedures for computer search warrants, the over seizure of data is common; Federal Rule of Criminal Procedure 41(g) has failed to adequately protect an individual's right to his or her property and right to privacy. The increasing popularity of storing information digitally creates a strong need to revisit an individual's right to privacy in this digital context.[7]

This Note explores the latest battle in the war of technology versus privacy. Part II frames the discussion by providing a historical look at reasonableness for Fourth Amendment searches and seizures and the effect of technology on Federal Rule of Criminal Procedure 41.[8] Part III exposes the inconsistencies among recent circuit court cases in adequately balancing the evolution of technology and its impact on searches and seizures.[9] Part IV of this note argues that the ambiguity regarding computer searches pursuant to the Fourth Amendment has spiraled out of control and consequently, Federal Rule of Criminal Procedure 41(g) has

---

[2] Stanford v. Texas, 379 U.S. 476, 481 (1965); Kerr, *supra* note 1.

[3] *See* Kerr, *supra* note 1.

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

[5] U.S. CONST. amend. IV; *see* Payton v. New York, 445 U.S. 573, 584 (1980); Kerr, *supra* note 1.

[6] *See generally* Kerr, *supra* note 1, at 533–38 (comparing the differences between the retrieval of digital evidence from electronic storage devices versus physical property).

[7] Alain Leibman, *Computer Search and Seizure Under the Fourth Amendment: The Dilemma of Applying Old-Age Principles to New-Age Technology*, 88 CRIM. L. REP. 644, 644 (2011) (discussing how "[e]ighteenth-century words must be given new meaning to maintain their currency in the twenty-first century").

[8] *See infra* Part II.

[9] *See infra* Part III.

been subject to abuse.[10] Finally, this note concludes in Part V by contending that it is time to create a new categorical rule for the return of property in the digital context.[11]

II. THE THRESHOLD OF THE FOURTH AMENDMENT AND THE AMBIGUITY OF THE REASONABLENESS REQUIREMENT

A. Threshold Questions of a Fourth Amendment Search

When an individual challenges government conduct alleging a Fourth Amendment violation has occurred, the threshold question is: whether the conduct at issue constitutes a "search" or a "seizure."[12] Under the Fourth Amendment, "a seizure of property occurs, not when there is a trespass, but 'when there is some meaningful interference with an individual's possessory interests in that property.'"[13] Historically, the more complex inquiry between the two questions is whether a "search" has taken place.[14] Over the years, the Supreme Court put forth different measures for resolving threshold "search" issues.[15]

In *Katz v. United States*, the defendant used a public telephone booth to transmit wagering information across the country in violation of federal law.[16] After extensive investigation, the FBI placed a listening device to the top of the booth and recorded the defendant's conversations that were later

---

[10] *See infra* Part IV.

[11] *See infra* Part V.

[12] U.S. CONST. amend. IV; *see, e.g.*, Katz v. United States, 389 U.S. 347 (1967); Hoffa v. United States, 385 U.S. 293 (1966); Lopez v. United States, 373 U.S. 427 (1963); On Lee v. United States, 343 U.S. 747 (1952); Goldman v. United States 316 U.S. 129 (1942); Olmstead v. United States, 277 U.S. 438 (1928); Boyd v. United States, 116 U.S. 616 (1886); Clinton v. Virginia, 130 S.E.2d 437, 441–42 (Va. 1963), *rev'd per curiam*, 377 U.S. 158 (1964).

[13] United States v. Jones, 132 S. Ct. 945, 951 n.5 (2012) (citation omitted); *see* U.S. CONST. amend. IV; *see also Katz*, 389 U.S. at 353 (explaining that property rights are not the sole measure of Fourth Amendment violations).

[14] *See, e.g.*, *Katz*, 389 U.S. at 346–47; *Hoffa*, 385 U.S. at 300–02; *Lopez*, 373 U.S. at 437–40; *On Lee*, 343 U.S. at 753–54; *Goldman*, 316 U.S. at 134–36; *Olmstead*, 277 U.S. at 464–66; *Boyd* 116 U.S. at 621–25; *Clinton*, 130 S.E.2d at 441–42.

[15] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) (illustrating the reasonable expectation of privacy test); *see also Jones*, 132 S. Ct. at 951–52 (stating that government trespass by itself is not a search, however when coupled with the attempt to find or obtain information is an unlawful search); Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that the utilization of a device, not in the public use, to detect otherwise unknowable actions is a "search"); Bond v. United States, 529 U.S. 334, 336–39 (2000) (applying the *Katz* test and holding that the tactile probing of a person's suitcase to be an unreasonable search).

[16] *Katz*, 389 U.S. at 348.

used as evidence against him at trial.[17] In his concurrence, Justice Harlan stated that there is a twofold requirement: (1) a person must exhibit an actual expectation of privacy; and (2) that the expectation be one that society is prepared to recognize as "reasonable."[18] *Katz* established that individuals may have a justifiable expectation of privacy in objects or activities in public areas.[19] Thus, under the *Katz* "reasonable expectation of privacy" test, official observation does not constitute a search in these circumstances.[20]

In 2001, the U.S. Supreme Court reviewed a new threshold question: "[d]id the government use technology, not in general public use, to inspect activities in the home?"[21] In *Kyllo* v. *United States*, the police obtained evidence of a marijuana-growing operation inside the defendant's home by using a thermal-imaging device from outside the home.[22] The thermal-imaging device helped police to determine whether the amount of heat emanating from the home was consistent with the high-intensity lamps typically used for indoor marijuana growth.[23] The government then used the evidence gathered from the device to support the issuance of a search warrant for the home.[24] The Supreme Court held that if the government uses an instrument that is not in general public use to obtain information, then a warrant is necessary.[25] Given this rationale, the imaging was deemed to be an unlawful search because the thermal imager was not in general public use.[26] The Court supported its reasoning by stating that the device yielded "details of the home that would previously have been unknowable without physical intrusion."[27]

While the "reasonable expectation of privacy test" articulated in *Katz*, remains the "touchstone of the modern Fourth Amendment," questions of how the Fourth Amendment applies to developing technologies still trouble the courts.[28] In *United States v. Jones*, the government acquired a search

---

[17] *Id.*

[18] *Id.* at 361 (Harlan, J., concurring) (discussing the subjective and objective requirements of the Fourth Amendment).

[19] *Id.*

[20] *See id.*; *see also* Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 815 (2004).

[21] Kyllo v. United States, 533 U.S. 27, 28 (2001).

[22] *Id.*

[23] *Id.*

[24] *Id.* at 30.

[25] *Id.* at 40.

[26] *Id.*

[27] *Id.*

[28] Kerr, *supra* note 20, at 808; *see* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

warrant allowing the installation of a Global Positioning System (GPS) tracking device on a vehicle registered to the defendant's wife.[29] The government tracked the vehicle's movements for twenty-eight days before securing an indictment of Jones on drug trafficking conspiracy charges.[30] In a 5-4 decision, the Supreme Court "struggled to figure out how they could fit open movements on public roads back inside the doctrinal box of reasonable expectations of privacy."[31] Setting aside the preexisting *Katz* test as the basis for their decision, Justice Scalia purported to resurrect the pre-*Katz* trespass test, defining a "search" as "an[y] activity involving (1) an enumerated protected category from the text of the Amendment, (2) a physical intrusion, and (3) a purpose to obtain information."[32] The *Jones* threshold requires a physical trespass into or upon the relevant protected category in question and further requires that the trespass must have been *investigatory in nature*.[33] While these threshold questions coupled with intricate case law guide the Court's analysis, Fourth Amendment procedures still contain much uncertainty, especially in the growing technological age.[34] Since the Court stated that *Katz* did not replace *Olmstead*, each test is still good law.[35]

B. Threshold Questions of a Fourth Amendment Seizure

Fourth Amendment analysis is only necessary where law enforcement officers "seize" an individual or an individual's property.[36] "[N]ot all personal intercourse between policemen and citizens involves 'seizures' of persons. Only when the officer, by means of physical force or show of authority, has in some way restrained the liberty of a citizen may we conclude that a 'seizure' has occurred."[37] These police encounters can be

---

[29] United States v. Jones, 132 S. Ct. 945, 946 (2012) (explaining that the warrant authorized installation within ten days in the District of Columbia, but agents installed the device on the eleventh day in Maryland).

[30] *Id.*

[31] Benjamin J. Priester, *Five Answers and Three Questions After* United States v. Jones *(2012), The Fourth Amendment "GPS Case,"* 65 OKLA. L. REV. 491, 495 (2013).

[32] *Id.* at 498; *see Jones*, 132 S. Ct. at 949 (limiting the threshold to enumerated protected categories in the Fourth Amendment: "persons, houses, papers, and effects").

[33] *Jones*, 132 S. Ct. at 949 (explaining that the new requirement as a trespass must be "for the purpose of obtaining information").

[34] *See generally* Leibman, *supra* note 7 (discussing how "Fourth Amendment jurisprudence has struggled to balance legitimate law enforcement needs with modern expectations of privacy in electronic storage media").

[35] *Jones*, 132 S. Ct. at 959.

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

[37] Terry v. Ohio, 392 U.S. 1, 19 n.16 (1968); *see also* State v. Johnson, 980 S.W.2d. 414, 422 (Tenn. Crim. App. 1998) ("Whenever an officer accosts an individual and restrains the

distinguished into three categories: (1) voluntary encounters that fall outside Fourth Amendment protection, (2) brief "stops" that must be based upon reasonable suspicion, and (3) full-scale "arrests" that demand a showing of probable cause.[38] The Supreme Court articulated an objective test to be applied when assessing if a seizure of persons has taken place under the Fourth Amendment: "a court must consider all the circumstances surrounding the encounter to determine whether police conduct would have communicated to a reasonable person that the person was not free to decline the officer's request or otherwise terminate the encounter."[39]

The seizure of an individual's physical property is usually easier to identify. A seizure of property occurs under the Fourth Amendment when there is meaningful interference with an individual's possessory interest in the property.[40] An individual challenging a seizure must have a reasonable expectation of privacy in the item or items being seized.[41] In assessing whether a reasonable expectation of privacy exists, courts typically examine four factors: "(1) the precautions taken to maintain privacy as to the item, (2) the Framers' intent when drafting the United States Constitution, (3) the property rights the defendant had in the searched item, and (4) the legitimacy of the defendant's possession of the property searched."[42]

The Search Clause has evolved to keep the protections of the Fourth Amendment relevant in the age of digital evidence, global social media networks, and increasingly sophisticated and invasive surveillance capabilities; however the Seizure Clause remains stuck in the property-based context created in *Olmstead*.[43] In *Olmstead*, the Court interpreted the

---

freedom to walk away, the officer has 'seized' that person for Fourth Amendment purposes.").

38 State v. Moats, 403 S.W.3d 170, 178 (Tenn. 2013); State v. Daniel 12 S.W.3d 420, 424 (Tenn. 2000); State v. Hawkins, 969 S.W.2d 936, 939 (Tenn. Crim. App. 1997) (referring to voluntary encounters as involving "community caretaking or public safety functions that involve no coercion or detention").

39 *Daniel*, 12 S.W.2d at 425 (quoting Florida v. Bostick, 501 U.S. 429, 439 (1991)).

40 United States v. Jacobsen, 466 U.S. 109, 113 (1984); Pepper v. Vill. of Oak Park, 430 F.3d 805, 809 (7th Cir. 2005); Fleming v. City of Bridgeport, 935 A.2d 126, 141 (Conn. 2007).

41 *See Daniel*, 982 F.2d at 149 (stating that the defendant did not possess a legitimate expectation of privacy in a package being shipped by an airline when the package was addressed to someone else and thus had no standing to challenge a search and seizure of the package); *see also* Brown v. State, 691 N.E.2d 438, 443 (Ind. 1998).

42 Miller v. State, 217 P.3d 793, 801 (Wyo. 2009).

43 *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 949 (2012); Kyllo v. United States, 533 U.S. 27, 31 (2001); Katz v. United States, 389 U.S. 347, 353 (1967); Olmstead v. United States, 277 U.S. 438, 463 (1928).

Seizure Clause to protect only physical property rights and to regulate the deprivation of tangible things.[44] Not so ironically, Justice Brandeis accurately predicted that "[w]ays may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."[45] Indeed, police practices have adapted to the profound shifts in technology that Brandeis predicted. These practices include duplicating the data stored on electronic devices and making "mirror images" that can be searched at any time after the initial seizure.[46] While counter-intuitiveness, unpredictability, and the difficulty in application should mandate the Supreme Court to re-evaluate Fourth Amendment precedent, the Federal Rules of Criminal Procedure are also open to abuse in the digital context.[47]

C. Assessing a Search and Seizure in the Twenty-First Century

The twenty-first century's extensive dependence on computers for a plethora of uses has led to a new type of search and seizure—involving data stored on computer hard drives and other electronic storage devices.[48] As the Tenth Circuit Court of Appeals noted, "the modern development of the personal computers and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs."[49] Digital evidence amplifies the ambiguity surrounding the Fourth Amendment.[50] For example, how do the reasonableness and particularity requirements apply to digital files? To answer these questions, the lower

---

[44] *Olmstead*, 277 U.S. at 455, 457 (analyzing the situation in which police wiretapped several phone lines at homes and offices while investigating bootleg and liquor smuggling during the Prohibition-era and the court refused to suppress the communication).

[45] *Id.* at 474 (Brandeis, J., dissenting).

[46] *See, e.g.*, United States v. Ganias, 755 F.3d 125, 135 (2d Cir. 2014).

[47] *See generally* United States v. Gladding, 775 F.3d 1149, 1154 (9th Cir. 2014) (holding that the cost of segregation was a "legitimate reason" for the government to retain Gladding's property).

[48] Kerr, *supra* note 1, at 544; *see also* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 281 (2005).

[49] *Ganias*, 755 F.3d at 135 (quoting United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009)); *see also* Kerr, *supra* note 1, at 569 (explaining that computers have become the equivalent of "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more").

[50] *See The Fourth Amendment "Reasonableness" Requirement*, FINDLAW, http://criminal.findlaw.com/criminal-rights/the-fourth-amendment-reasonableness-requirement.html (last visited Apr. 4, 2015).

courts aim "to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools."[51]

The Supreme Court has yet to come forward with a bright-line rule or mode of analysis for lower courts to utilize when evaluating the reasonableness of a computer search and seizure.[52] Not only does this allow law enforcement officers to go unregulated in many contexts, it also creates ambiguity in the application and enforcement of other Federal Rules of Criminal Procedure, such as Rule 41. The threat of unreasonable searches, which the Framers crafted the Fourth Amendment to forbid, have resurfaced in a digital context. An individual's right to privacy is at stake.[53] Due to the increasing popularity of storing information digitally, a strong need to revisit Federal Rule of Criminal Procedure 41 and its adaptability in this digital age is required.[54]

D. Federal Rule of Criminal Procedure 41

An individual alleging that his or her property was unlawfully seized during the execution of a search warrant has two options. Assuming that the property at issue is incriminatory and being offered against the individual in a criminal case, the individual may (1) file a motion to suppress or (2) file a motion for its return.[55] Federal Rule of Criminal Procedure 41 provides the procedure for an individual who is seeking to challenge a search warrant prior to and after the commencement of formal charges.[56] The Supreme Court's reluctance to clarify the boundaries of a computer search and seizure has forced Congress to continually amend its rules in an attempt to keep up with the twenty-first century's advancements.[57] Amended in 1989, Rule 41(e) was expanded to allow a person to file a motion based upon an illegal search.[58] A later amendment

---

[51] *Ganias*, 755 F.3d at 134.

[52] *See generally* U.S. CONST. amend. IV. *See* Kerr, *supra* note 48, at 279.

[53] Payton v. New York, 445 U.S. 573, 583 (1980); Stanford v. Texas, 379 U.S. 476, 481 (1965); United States v. Galpin, 720 F.3d 436, 445 (2d Cir. 2013); *see also* Kerr, *supra* note 1, at 536.

[54] Leibman, *supra* note 7 (discussing the obstacles that arise when applying old-age principles to new-age technology).

[55] *See* FED. R. CRIM. P. 12.

[56] *See generally* FED. R. CRIM. P. 41(g) (providing that an individual "aggrieved by an unlawful search and seizure or by the deprivation of property may move for the property's return").

[57] *See* FED. R. CRIM. P. 41; *see also* Ian M. Comisky et al., *Fourth Amendment Privilege—Search and Seizure Issues*, TAX FRAUD & EVASION ¶ 14.02 (2014).

[58] *See* FED. R. CRIM. P. 41(e) (noting that prior to the amendment in 1989 an individual could only file a motion under Rule 41 based upon a deprivation of property).

was made that required the exclusion of evidence including circumstances where the government illegally seized evidence, but in "good faith."[59] Next, a 2002 revision moved the language of Rule 41(e) to 41(g).[60] Rule 41(g)—formerly Rule 41(e) provides:

> A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.[61]

Applying this rule in the twenty-first century presents a multitude of challenges for law enforcement officials and Congress. Perhaps this is because computers can be viewed as a physical piece of evidence, yet the information contained within them is not as simple as the contents of a file cabinet.[62] Today, an individual can store a wide array of data on a computer that is less than one inch in height, twelve inches in width, eight inches in depth, and weighs two and a half pounds.[63] As a result, a federal rule that only addresses the physical aspect of the evidence fails to protect an individual's right of privacy in this day in age.[64]

Unlike in a traditional search and seizure, computers have the ability to store not only large quantities of an individual's personal data, but also, thousands or millions of non-responsive data belonging to a third-party.[65] Consequently, on-site review of the data creates a significant burden on both the individual and the government agents executing the search warrant.[66] In 2009, as a response to this problem, Federal Rule of Criminal Procedure 41(e)(2)(b) was amended to authorize the seizure and duplication of electronic storage media. Unless otherwise specified, the

---

59 FED. R. CIV. P. 41 advisory committee's note to 1989 amendment; *see also* FED. R. CRIM. P. 41.

60 FED. R. CRIM. P. 41(e), (g).

61 FED. R. CRIM. P. 41(g).

62 *See generally* Kerr, *supra* note 1, at 531 (explaining how personal computers that allow individuals to store personal papers in a single place has increased law enforcement's ability to search private information).

63 *See generally Apple 11-inch Macbook Air*, APPLE, http://www.apple.com/macbook-air/specs.html (last visited Apr. 4, 2015).

64 *See generally* Kerr, *supra* note 1, at 569 (illustrating the evolution of the digital world).

65 *Id.*

66 *See generally* United States v. Ganias, 755 F.3d 125, 136 (2d Cir. 2014) (stating that because of the significant burdens on-site review would place on both the individual and the Government, the creation of mirror images for offsite review is constitutionally permissible in most instances, "even if the wholesale removal of tangible papers would not be").

warrant authorizes a later view of the media or information consistent with the warrant.[67] Computer examiners and law enforcement officials executing a search warrant on a computer are permitted to make identical copies, or forensic mirror images of a hard drive.[68] These mirror images permit off-site searching of the duplicate as if it were the actual hard drive, but without interfering with the individual's use of his home, computer, or files.[69]

But what happens to the mirror images when a motion for the return of property is filed? Should the government be permitted to retain a copy of the seized material when the original documents are ordered to be returned?[70] The Advisory Committee noted that the return or destruction of all copies of seized records is warranted only where "'equitable considerations' justify such an approach."[71] Issues arise particularly where the property in question is no longer needed for evidentiary purposes, either because the trial is complete, the defendant has pleaded guilty, or the government has abandoned its investigation.[72] Under these circumstances, the defendant "is presumed to have a right to [the property's] return, and the government has the burden of demonstrating that it has a 'legitimate reason' to retain the property."[73]

The easiest way for the government to meet its burden is to prove "the property . . . is contraband or subject to forfeiture."[74] Nevertheless, the government's legitimate reason for retaining the property must be "reasonable under all of the circumstances."[75] An individual's property is

---

[67] *See* FED. R. CRIM. P. 41(e)(2)(B) (addressing the warrant requirement for a warrant seeking electronically stored information).

[68] *Ganias*, 755 F.3d at 135.

[69] *Id.* at 136 (discussing how off-site review is constitutionally permissible, the "off-site review of these mirror images, however, is still subject to the rule of reasonableness").

[70] *See, e.g.*, *id.* at 139; Ramsden v. United States 2 F.3d 322, 327 n.2 (9th Cir. 1993); Patron v. LaPrade, 524 F.2d 862, 867–69 (3d Cir. 1975).

[71] FED. R. CRIM. P. 41(g) advisory committee's note to 1989 amendment.

[72] *See* FED. R. CRIM. P. 41(g); United States v. Harrell, 530 F.3d 1051, 1054 (9th Cir. 2008); *see also* United States v. Gladding, 775 F.3d 1149, 1152 (9th Cir. 2014) (explaining that a "defendant's Rule 41(g) motion should presumptively be granted if the government no longer needs the property for evidence"); United States v. Kriesel, 720 F.3d 1137, 1144 (9th Cir. 2013); United States v. Martinson, 809 F.2d 1364, 1369 (9th Cir. 1987) (internal quotation marks and citation omitted).

[73] FED. R. CRIM. P. 41(g); *see also Gladding*, 775 F.3d at 1152; *Kriesel*, 720 F.3d at 1144; *Martinson*, 809 F.2d at 1369.

[74] *Martinson*, 809 F.2d at 1369; *see Gladding*, 775 F.3d at 1152; United States v. Fitzen, 80 F.3d 387, 388 (9th Cir. 1996).

[75] *See Krisel*, 720 F.3d at 1158 (Reinhardt, J., dissenting). *See generally* FED. R. CRIM. P. 41(g) advisory committee's note to 2009 Amendment ("Rule 41(g) . . . provides a process for the 'person aggrieved' to seek an order from the court for a return of property, including

"contraband per se if its possession, without more, constitutes a crime; or in other words, if there is no legal purpose to which the object could be put."[76] For example, child pornography would be considered contraband because its mere possession is a crime.[77] However, showing that the property is contraband or subject to forfeiture are not the only ways the government can justify retaining an individual's property; the government can otherwise keep possession of the property if it can adequately demonstrate a "legitimate reason" for doing so.[78] Ordinarily, district courts have held files on computers that were seized after having been used to commit crimes are forfeitable along with the physical computers themselves.[79] The Supreme Court has yet to adopt a bright line rule in order to produce certainty and clear guidance for law enforcement officials when executing a search warrant on a computer.[80] Thus, the Federal Rules of Criminal Procedure are being manipulated to self-serve the government officials involved.[81] The lack of uniformity among the Fourth Amendment and the Federal Rules of Criminal Procedure allow abuse of discretion across the circuit courts to remain.[82] The struggle remains to balance the public safety and privacy in the digital world.

---

storage media or electronically stored information, under reasonable circumstances.").

[76] United States v. Harrell, 530 F.3d 1051, 1055–57 (9th Cir. 2008); *see* United States v. McCormick, 502 F.2d 281, 288 (9th Cir. 1974).

[77] *See, e.g.*, *Gladding*, 775 F.3d at 1152 (discussing the preliminary order of forfeiture made final as to the contraband items however there were non-contraband items i.e. family photos mixed in with the contraband items).

[78] *See, e.g.*, *Kriesel*, 720 F.3d at 1144–47 (holding that the government's retention of the defendant's blood sample was "reasonable under all of the circumstances" because the government needed the sample to ensure the accuracy of future DNA identifications); *see also* Ramsden v. United States, 2 F.3d 322, 326 (9th Cir. 1993) ("Rule 41 provide[s] that 'reasonableness under all of the circumstances must be the test when a person seeks to obtain the return of property'") (quoting FED. R. CRIM. P. 41(e) advisory committee's note to 1989 amendment).

[79] *See* Hugh B. Kaplan, *Search and Seizure: Cost of Sorting Seized Computer Files Can Justify Refusal to Return Untainted Files*, 96 CRIM. L. REP. 351 (BNA) (Jan. 5, 2015).

[80] *See, e.g.*, United States v. Ganias, 755 F.3d 125, 129 (2d Cir. 2014); *Gladding*, 775 F.3d at 1153; United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010) [hereinafter *CDT II*].

[81] *See, e.g.*, *Ganias*, 755 F.3d at 135; *Gladding*, 775 F.3d at 1173; *Kriesel*, 720 F.3d at 1145–47; *CDT II*, 621 F.3d at 1162.

[82] Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exceptions*, 111 MICH. L. REV. 485, 543 (2013).

III. INCONSISTENCY AMONG THE CIRCUITS IN ADEQUATELY BALANCING THE EVOLUTION OF TECHNOLOGY AND ITS IMPACT ON SEARCHES AND SEIZURES

Conducting computer searches generally requires fewer people, but more time than physical searches.[83] For years, courts have struggled to identify what the Fourth Amendment requires of law enforcement officers when they seize electronic records containing private information intermingled with tainted information.[84] Due to the Fourth Amendment's murky waters regarding computer searches, the effect of this ambiguity continues to spread to the return of the property under the Federal Rules of Criminal Procedure.[85] The protocols required to adequately search a computer dilute the two traditional limits on searches and seizures.[86] In effect, the particularity requirement, which assumes a physical item is being seized, is diminished in the digital world.[87] Under existing standards, the warrant to seize a computer hard drive would satisfy the particularity requirement, despite the fact that the computer may have "an entire virtual world of information stored in it."[88] And while the police can easily make reasonable inferences with respect to the location of physical evidence based on the size and shape of the evidence, the same cannot be said of digital evidence.[89] As such, the particularity requirement is undermined in the digital context.[90] The plain view doctrine is also curtailed, as a search for specific digital evidence often unveils a remarkable amount of other evidence; therefore, a great deal can be considered in plain view.[91] Stemming from these ambiguities, it is unclear how long the government can retain mirror images of an individual's hard drive and also, at what point must the government destroy or return non-responsive data? This vagueness also fails to answer what standard must be met to adequately demonstrate a "legitimate reason" to justify retaining an individual's property after a motion for return has been filed?

---

83 Kerr, *supra* note 1, at 544; *see also* Kerr, *supra* note 48, at 288.

84 Lance J. Rogers, *Police Can't Indefinitely Hold Digital Files That Are Beyond Scope of Search Warrant*, 95 CRIM. L. REP. 499 (2014).

85 *See* U.S. CONST. amend. IV; *see also* FED. R. CRIM. P. 41(g).

86 *See* U.S. CONST. amend. IV. *See generally* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 503 (2007) (discussing how no single test can accurately and consistently distinguish troublesome police practices that are reasonable); Kerr, *supra* note 1, at 544.

87 Kerr, *supra* note 1, at 544; *see also* Kerr, *supra* note 48, at 289.

88 Kerr, *supra* note 1, at 569; *see also* Kerr, *supra* note 48, at 289.

89 Kerr, *supra* note 1, at 569; *see also* Kerr, *supra* note 48, at 289.

90 Kerr, *supra* note 1, at 569; *see also* Kerr, *supra* note 48, at 289.

91 Kerr, *supra* note 1, at 544; *see also* Kerr, *supra* note 48, at 289.

A. Right to Over-Seize is Temporary—United States v. Ganias

In *United States v. Ganias*, the IRS and FBI were investigating the defendant for fraudulent accounting services.[92] Several search warrants were issued to search the offices of Ganias's accounting business, including one dated for November 17, 2003.[93] Upon execution, the computer specialists made forensic mirror images of all three of Ganias's computer hard drives and in doing so, copied files that were beyond the scope of the warrant, including files containing Ganias's personal financial records.[94] Not surprisingly, the agents failed to purge or delete the non-responsive files.[95] Two-and-a-half years later, the government had reason to believe that Ganias was underreporting income for not only his clients, but himself as well.[96] Because the non-responsive files were never purged or deleted after the 2003 seizure, an IRS case agent was able to review Ganias's personal financial records two-and-a-half years later and use these records to indict him for conspiracy and tax evasion.[97]

The Second Circuit held that the Fourth Amendment does not permit officials executing a warrant for the seizure of particular data on a computer to indefinitely retain every file on that computer for use in future criminal investigations.[98] The government argued that Ganias was precluded from seeking suppression on appeal because he failed to bring a motion for the return of property pursuant to Rule 41(g).[99] Contrary to the district court's ruling, the Second Circuit found no governing authority that concluded that a Rule 41(g) motion is a prerequisite to a motion to suppress.[100] The Second Circuit determined that retaining Ganias's personal financial records for two-and-a-half years was a substantial interference with his "possessory rights in those files," which constituted an

---

[92] United States v. Ganias, 755 F.3d 125, 125 (2d Cir. 2014).

[93] *Id.* at 128 (authorizing the seizure of, "all books, records, documents, materials, computer hardware and software and computer associated data relating to the business").

[94] *Id.* (stating that when Ganias verbally expressed concern about his personal files being obtained, an agent assured him that only the files relating to the investigation would be opened and everything else would be "purged").

[95] *Id.* at 129.

[96] *Id.*

[97] *Id.* (noting, however, that the government did ask Ganias and his counsel for permission to access these files in February 2006, but received no response).

[98] *Id.* at 137.

[99] *Id.* at 139; *see* FED. R. CRIM. P. 41(g) ("A person aggrieved . . . *may* move for the property's return.") (emphasis added); *see also* FED. R. CRIM. P. 41(h) ("A defendant may move to suppress evidence. . . .").

[100] *Ganias*, 755 F.3d at 139.

unreasonable seizure under the Fourth Amendment.[101]

The Second Circuit's decision places a duty on government officials to return, delete, or destroy non-responsive data, even in the absence of a Rule 41(g) motion to return property.[102] In this circuit, it is unmistakably clear that two years of retention is too long; government officials cannot open-endedly hold digital files that are beyond the scope of a search warrant.[103] While this decision logically branches from the general purpose of the Fourth Amendment in protecting the privacy of an individual, no language in Rule 41 expresses that the right to over seize is temporary.[104] Perhaps the reasoning behind this is because Congress has yet to find a way to articulate the dichotomy between a physical seizure of property and a digital seizure of property. In the twenty-first century, one can argue there are three types of seizures: (1) the seizure of a person, previously discussed; (2) the seizure of physical property where there is some meaningful interference with an individual's possessory interest; and (3) a digital seizure where a mirror image that can be searched at any later time interferes with an individual's privacy interest.[105] The gray area surrounding a digital seizure leaves the possibility of prosecutorial overreach.

B. Innocent Third-Party Records Which are Intermingled with Lawfully Seized Data— United States v. Comprehensive Drug Testing, Inc.

Since the threat of Fourth Amendment over-seizure is so prominent in the digital context, one could presume Rule 41(g) adequately extends to protect the privacy concerns of innocent third parties whose records are intermingled with tainted files.[106] However, under the Ninth Circuit's

---

[101] *Id.* at 129; *see also* United States v. Place, 462 U.S. 696, 703 (1983) (detaining a traveler's luggage while awaiting the arrival of a drug-sniffing dog constituted a seizure). *See generally* Soldal v. Cook Cty., 506 U.S. 56, 62–64 (1992) (explaining that a seizure occurs when one's property rights are violated, even if the property is never searched and the owner's privacy was never violated).

[102] FED. R. CRIM. P. 41(g); *see Ganias*, 755 F.3d at 125; *see also* Orin Kerr, *Court Adopts a Fourth Amendment Right to the Deletion of Non-Responsive Computer Files*, THE WASH. POST (Nov. 2, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/18/court-adopts-a-fourth-amendment-right-to-the-deletion-of-non-responsive-computer-files/.

[103] *Ganias*, 755 F.3d at 129; *see* Kerr, *supra* note 102.

[104] *See* U.S. CONST. amend. IV; FED. R. CRIM. P. 41.

[105] *See supra* Part II.B.

[106] *See* Derek Regensburger, *Bytes, Balco, and Barry Bonds: An Exploration of the Law Concerning the Search and Seizure of Computer Files and an Analysis of the Ninth Circuit's Decision in* United States v. Comprehensive Drug Testing, Inc., 97 J. CRIM. L. & CRIMINOLOGY 1151, 1153 (2007). *But see CDT II*, 621. F.3d 1162, 1177 (9th Cir. 2010).

holding in *United States v. Comprehensive Drug Testing, Inc*. (CDT), Rule 41(g) fails to protect their privacy.[107] This case stems from the ongoing grand jury investigation into illegal steroid use by professional athletes that began in 2002.[108] Shortly after the investigation was underway, federal agents developed enough probable cause to believe that at least ten major league baseball players, including Barry Bonds, obtained steroids from Bay Area Lab Cooperative (BALCO).[109] In 2003, the Major League Baseball Players Association (MLBPA) agreed with the MLB that all players would be anonymously tested for steroid use.[110] This collective bargaining agreement further stipulated that the results would be used only to determine the extent of the steroid problem in baseball and the results of the tests would be kept confidential.[111]

Despite the collective bargaining agreement, in early 2004 the testing records for all MLB players were subpoenaed by the government.[112] The government obtained search warrants which permitted the "seizure of drug test records and specimens" at two CDT lab locations.[113] The warrants expressly named "ten BALCO-connected players."[114] Designated government authorities that were deemed "computer personnel" were permitted to search computer equipment, including storage devices, and in addition, were directed that "where an on-site search would be impracticable, to seize either a copy of the data or the computer equipment itself."[115] The appropriate course of conduct was to be determined by the computer personnel exclusively.[116]

While executing the search, agents copied an entire electronic database (Tracey Directory) containing "all of the computer files for CDT's sports drug testing programs."[117] Agents also seized a twenty-five page master list of all MLB players tested during the 2003 season and a thirty-four page list

---

[107] United States v. Comprehensive Drug Testing, Inc., 473 F.3d 915, 919–20 (9th Cir. 2006) [hereinafter *CDT I*]; *see also CDT II*, 621 F.3d at 1177.

[108] *CDT I*, 473 F.3d at 919–20; *see also CDT II*, 621 F.3d at 1178.

[109] *CDT I*, 473 F.3d at 920; *see also CDT II*, 621 F.3d at 1177.

[110] Gordon Edes, *Baseball Gets Tougher over Steroid Use*, BOSTON.COM (Nov. 14, 2003), http://www.boston.com/sports/baseball/articles/2003/11/14/baseball_gets_tougher_over_steroid_use/; *see also CDT II*, 621 F.3d at 1177.

[111] Edes, *supra* note 110; *see also CDT II*, 621. F.3d at 1177.

[112] *CDT I*, 473 F.3d at 920 (stating that these testing labs were disinterested third parties, Comprehensive Drug Testing, Inc. and Quest Diagnostics, Inc.).

[113] *Id.* at 921.

[114] *Id.*

[115] *Id.*

[116] *Id.* (noting that the computer personnel were trained in searching and seizing computer data).

[117] *Id.* at 922.

of the drug testing results that were positive for eight of the ten BALCO players, which coincidentally was intermingled with positive test results for twenty-six other players.[118] Using the Tracey directory as its guide, the government sought additional search warrants for another expressly named 100 MLB Players.[119]

The MLBPA filed a Rule 41(g) Motion for return of property seized pursuant to the warrants and additionally filed motions to quash the subsequent subpoenas.[120] Before the Ninth Circuit, the MLBPA argued that the government used the warrants aimed at the BALCO test results as a pretext for obtaining records of other non-BALCO players who had tested positive for steroids in order to indict them.[121] The court reasoned that because agents were lawfully on the property and were authorized to seize records of the ten BALCO players being investigated, the seizure of the records of the non-BALCO players was not unlawful because they were intermingled with relevant records.[122] Did the non-BALCO players, whose test results were intermingled with those of the ten BALCO players actually being investigated, even stand a chance? This left many wondering if perhaps a neutral third party should have been required to segregate the confidential material prior.[123]

The privacy interest of the non-BALCO players appeared to take a back seat in this context.[124] The court reasoned that the return of the property was not warranted because the intermingled files and data were seized legally under the search warrant, and thus, the government had a continuing need for the property as evidence.[125] Regardless of the Ninth Circuit's reasoning, how would a neutral third-party in this situation—like the non-BALCO players—even know to file a motion to return property under Rule 41(g)? Under this holding, anytime the government retains responsive data that is intermingled with non-responsive data, it has no duty to segregate and return the non-responsive files, failing to adequately protect the privacy concerns of innocent third-parties.[126] The failure to

---

[118] *Id.* at 923 (noting copies of all seized documents were provided to CDT directors several days later).

[119] *Id.* at 923–24 (stating that every player named had tested positive for steroids).

[120] *Id.* at 924–25. *See generally* FED. R. CRIM. P. 41(g).

[121] *CDT I*, 473 F.3d at 932.

[122] *Id.* ("Because the agents saw that the spreadsheet clearly contained information within the scope of the warrant, they seized the spreadsheet for off-site review.").

[123] *See generally* Regensburger, *supra* note 106, at 1187 ("The government should have . . . used a taint team to segregate the confidential material.").

[124] *See id.* at 1189.

[125] *CDT I*, 473 F.3d at 937.

[126] *See* Regensburger, *supra* note 106, at 1152.

protect the privacy interests of innocent third-parties stems from the lack of Fourth Amendment protocol governing computer searches and seizures.[127]

C. The Cost of Segregation as a Basis for Denying the Return of Property—United States v. Gladding

Rule 41(g) continues to prove circuit court holdings contrary to public interest.[128] Most recently, in *United States v. Gladding*, the cost of sorting seized computer files was used as grounds to justify refusal to return property.[129] The defendant, Justin Paul Gladding, was indicted on two counts related to his possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B).[130] The indictment further included allegations that Gladding's three computers and other hard drives were subject to forfeiture under 18 U.S.C. § 2253 because they contained evidence of child pornography.[131] Gladding did not dispute that his electronic storage devices were forfeited, instead he requested that the government return copies of certain non-contraband computer files on those devices.[132] In his Rule 41(g) motion to return property, Gladding alleged that there were thousands of pictures of his family and personal emails on the devices that he wanted returned.[133]

The district court entered a forfeiture order solely as to the contraband items, directed the parties to work together to determine which files Gladding was seeking to have returned, and asked the government to provide copies of those files to Gladding.[134] However, the parties were unable to agree on how to return the non-contraband files, and in response, Gladding filed a second Rule 41(g) motion to return property.[135] "The

---

[127] *See generally CDT I*, 473 F.3d at 932 ("Because the agents saw that the spreadsheet clearly contained information within the scope of the warrant, they seized the spreadsheet for off-site review.").

[128] United States v. Gladding, 775 F.3d 1149, 1154 (9th Cir. 2014).

[129] *Id.*

[130] *Id.* at 1150–51. *See generally* 18 U.S.C. § 2252(a)(2), (4)(B) (governing certain activities relating to material involving sexual exploitation of minors).

[131] *Gladding*, 775 F.3d at 1151. *See generally* 18 U.S.C. § 2253 (addressing property subject to criminal forfeiture).

[132] *Gladding*, 775 F.3d at 1151.

[133] *Id. See generally* FED. R. CRIM. P. 41(g) ("A person aggrieved . . . by the deprivation of property may move for the property's return.").

[134] *Gladding*, 775 F.3d at 1151; *see* Answering Brief of the United States at 2, United States v. Gladding, 775 F.3d 1149 (9th Cir. 2014) (No. 12–10544), 2013 WL 6823849, at *5.

[135] *Gladding*, 775 F.3d at 1151; *see* Answering Brief of the United States at *5, *Gladding*, 775 F.3d 1149 (No. 12–10544) (noting that Gladding did not specifically identify the items that he wanted returned to him). *See generally* FED. R. CRIM. P. 41(g).

government attached three exhibits to its opposition brief: (1) a document listing some of Gladding's property the government found to be non-contraband; (2) an email correspondence between counsel; and (3) the transcript of a hearing on a similar dispute in a different case."[136] In response to Gladding's second 41(g) motion, the district court requested the parties attempt to resolve the issue on their own again.[137] At the third and final hearing, the district court denied Gladding's motion stating that it was "not going to require the Government to . . . spend days or hours, or whatever, having an agent go through 100,000 images to figure out which ones are and which ones are not contraband."[138] However, while Gladding's appeal to the third motion was pending, the government allowed Gladding's expert to retrieve a portion of the forfeited electronic storage devices.[139] Ironically enough, Gladding's expert was able to retrieve a large number of Gladding's non-contraband files.[140] Before the Ninth Circuit, Gladding continued to allege that there were still other non-contraband files the government was obligated to return.[141]

The Ninth Circuit explicitly admitted that they had yet to articulate the contours of a Rule 41(g) motion in the context of intermingled computer files.[142] In light of limited guidance on this topic, the court avoided answering the pressing question: whether files on computers that were seized after having been used to commit crimes are forfeitable along with the computers themselves.[143] Instead, the Ninth Circuit stated that the cost of segregation constitutes a "legitimate reason" for keeping defendants' computers in order to rebut the presumption that defendants are entitled to a return of their personal files once criminal proceedings are over.[144] In the

---

[136] *Gladding*, 775 F.3d at 1151. *See generally* FED. R. CRIM. P. 41(g).

[137] *Gladding*, 775 F.3d at 1151; *see also* Answering Brief of the United States at * 7, *Gladding*, 775 F.3d 1149 (No. 12–10544) (stating that Gladding "did not appear to be cooperating with the government because he was not providing any assistance in locating the files that he wanted returned").

[138] Answering Brief of the United States at * 7, *Gladding*, 775 F.3d 1149 (No. 12–10544).

[139] *Gladding*, 775 F.3d at 1151.

[140] *Id.*

[141] *Id.*

[142] *Id.* at 1153.

[143] *See generally id.* at 1154 (noting that the court remanded the issue back to the district court for proceedings consistent with its opinion).

[144] *Id.* at 1153 (noting however, that the district court did not expressly state whether Gladding or the government had the burden of proof on the motion, but impliedly conceded that the court incorrectly put the burden on Gladding); *see* FED. R. CRIM. P. 41(g). *But cf.* United States v. Kriesel, 720 F.3d 1137, 1144 (9th Cir. 2013) (explaining that a "defendant's Rule 41(g) motion should presumptively be granted if the government no

Ninth Circuit's opinion, if the parties dispute the cost of segregating data, they should submit supporting evidence and the district court is directed to hold an evidentiary hearing to resolve the dispute.[145]

The Court relied on the advisory committee's note to Rule 41(e)(2), which addresses the difficulties posed by electronic data in this context: "A substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs."[146] The Ninth Circuit also left open the possibility that, on remand, the lower court could potentially amend its prior ruling to hold that all of the files on the defendant's devices were forfeitable.[147] This decision significantly downplays the general purpose of a Rule 41(g) motion, that a defendant holds a right to have his property.[148] Subsequently criminals who store both important aspects of their personal lives as well as digital contraband on their own electronic devices assume the risk of losing all their data when it is lawfully seized.[149]

IV. ANALYSIS

Today, more than ever, balancing an individual's privacy with public safety poses great difficulty for not only the Supreme Court, but Congress as well.[150] The problem stems from the absence of bright line rules, which are needed to produce certainty and clear guidance for law enforcement officials executing search warrants on computers under the Fourth Amendment.[151] Such a trend is frightening because the Fourth Amendment prefers bright line rules in place when an individual's constitutional rights are at jeopardy.[152] In addition, the effect of such little guidance from the

---

longer needs the property for evidence") (internal quotation marks and citation omitted).

[145] *Gladding*, 775 F.3d at 1154 (stating that on remand, "[t]he district court should deny Gladding's motion if the government has carried its burden of proof by producing evidence which preponderates to show the government's costs concerns are 'reasonable under the circumstances'") (citing *Kriesel*, 720 F.3d at 1144).

[146] *Id.* at 1154 (referring to FED. R. CRIM. P. 41(e)(2) advisory committee's note to 1989 amendment).

[147] *Id.* at 1153 n.1; *see also* Kaplan, *supra* note 79, at 24.

[148] *See Gladding*, 775 F.3d at 1153–54; *see also* FED. R. CRIM. P. 41(g).

[149] *Gladding*, 775 F.3d at 1150 (noting that "many people store every aspect of their lives on electronic devices").

[150] Jason Weinstein & William Drake, *Public Safety, Privacy and Particularity: A New Approach to Search Warrants for Digital Evidence*, 95 CRIM. L. REP. 227 (2014). *See generally* U.S. CONST. amend. IV; FED. R. CRIM. P. 41 (dealing with the lack of privacy caused by traditional search and seizure when evidence is digital).

[151] *See* U.S. CONST. amend. IV.

[152] *See* Thornton v. United States, 541 U.S. 615, 627 (2004); New York v. Belton, 453

Supreme Court on Fourth Amendment protocol trickles further down and allows for the abuse of discretion in the application of Rule 41.[153] While ruling with caution in the context of evolving technology can be wise, it should not come at the cost of clarity.[154]

Historically, the seizure of an individual's property has occurred not when there is a trespass, but when there is "some meaningful interference with an individual's possessory interests in that property."[155] However, in the twenty-first century, advancements in technology have allowed computer examiners and police officials to search mirror images of an individual's hard drive off-site.[156] The problem with this practice is that the examiners are searching mere copies, never truly interfering with the individual's possessory interest in that property because the individual retains the physical computer throughout the process.[157] Failure to account for this modern procedure results in the failure to protect an individual's right of privacy as well, because Rule 41(g) does not address the return of copied material when the original is never physically seized.[158]

Regardless of whether the court orders the return of the original data pursuant to Rule 41(g), examiners still retain the mirror images of the data and are able to search them at their convenience without depriving the individual of his or her possessory interest in the property.[159] In *Ganias*, although the Second Circuit held that government officials have no authority to retain non-responsive data indefinitely, the court failed to specify when the government is required to return, delete, or destroy such data.[160] Due to this ambiguity, Fourth Amendment jurisprudence and Rule

---

U.S. 454, 458 (1981); United States v. Robinson, 414 U.S. 218, 235 (1973).

[153] *See, e.g.*, United States v. Ganias, 755 F.3d 125, 129 (2d Cir. 2014); *Gladding*, 775 F.3d at 1153; *CDT II*, 621 F.3d 1162, 1177 (9th Cir. 2010).

[154] Kerr, *supra* note 20, at 805 ("When technology is in flux, Fourth Amendment protections should remain relatively modest until the technology stabilizes.").

[155] *See* U.S. CONST. amend. IV. *But see* United States v. Jones, 132 S. Ct. 945, 951 (2012); Katz v. United States, 389 U.S. 347, 353 (1967) (explaining that property rights are not the sole measure of Fourth Amendment violations).

[156] *Ganias*, 755 F.3d at 135; *see also* Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 113 (2011) (finding that the FBI, alone has more than 200 full-time forensic examiners).

[157] *Ganias*, 755 F.3d at 135 (noting that mirror images for off-site review are constitutionally permissible).

[158] FED. R. CRIM. P. 41(g); *see Ganias*, 755 F.3d at 135; *see also* Kerr, *supra* note 48, at 282.

[159] FED. R. CRIM. P. 41(g); *see Ganias*, 755 F.3d at 135.

[160] *Ganias*, 755 F.3d at 141 (stating that eventually the retention of data can go on for so long that it is "unreasonable" to retain it any longer).

41(g) are susceptible to abuse of discretion.[161]

The lack of clarity regarding Fourth Amendment procedures for computer search warrants makes the over seizure of data not only probable, but way too common.[162] Law enforcement officials and computer specialists in most circuits can execute search warrants on computers with very few restraints.[163] Where unrestrained search warrants result in the over seizure of data, often times a single file contains tainted information relevant to the search intermingled with untainted information on an innocent third party.[164] Under these circumstances, Rule 41 fails to protect the privacy interests of innocent third parties; and within the Ninth Circuit, can even result in the indictment of third parties.[165] As Judge Thomas discussed in his dissent in *CDT I*, the problem there was that the government failed to protect the "constitutionally protected privacy interest in avoiding disclosure of personal matter," such personal matters being the medical records of the third party non-BALCO players.[166] Rule 41(g) failed to effectively protect these players, and this resulted in an unconstitutional invasion when their records were seized without a warrant.

Rule 41(g) was unable to protect the non-BALCO players' privacy interest in *CDT I* because it provides zero guidance for law enforcement agents on what to do when they are presented with computer data intermingling tainted and non-tainted information.[167] The failure to protect the privacy of innocent third parties would not be such a prominent issue if the Fourth Amendment properly regulated the execution and seizure of computer data.[168] The uncertainty regarding search warrants on computers

---

[161] U.S. CONST. amend. IV; FED. R. CRIM. P. 41(g); *see Ganias*, 755 F.3d at 141.

[162] *See generally Gladding*, 775 F.3d at 1154 (9th Cir. 2014) (laying out the situation in which over seizure of data resulted in the loss of personal untainted files due to the cost of suppression); *CDT I*, 473 F.3d 915, 962 (9th Cir. 2006) (Thomas, J., concurring in part and dissenting in part) (articulating the situation in which over seizure of data resulted in the indictment of innocent third parties).

[163] *See generally* United States v. Williams, 592 F.3d 511, 520–21 (4th Cir. 2010) (articulating different protocol in each circuit when executing a search on a computer); United States v. Mann, 592 F.3d 779, 780 (7th Cir. 2010) (describing the particularity requirement of a warrant for digital evidence); United States v. Burgess, 576 F.3d 1078, 1093 (10th Cir. 2009) (describing the importance of a warrant's scope requirement for purposes of searching digital evidence).

[164] *See, e.g.*, *CDT I*, 473 F.3d at 962 (Thomas, J., concurring in part and dissenting in part) (laying out the situation in which over seizure of data resulted in the indictment of innocent third parties).

[165] *See, e.g.*, *id.*

[166] *Id.* at 970.

[167] *See generally* FED. R. CRIM. P. 41(g) (discussing motions to return evidence wrongfully after search and seizure).

[168] *See CDT I*, 473 F.3d at 974–75.

has invited prosecutors to push to establish self-serving rules, such as the one in *Gladding*.[169] The cost of suppression is not addressed in Rule 41(g), yet the court relied on this argument as a "legitimate reason" for keeping the defendant's personal property.[170] By failing to specify, the court left unanswered how difficult or how expensive sorting must be in a particular case for a court to deny a Rule 41(g) motion.[171]

V. CONCLUSION

The ubiquitous use of computer technology in the twenty-first century has instigated a brutal war between technology and privacy rights. With little to no guidance from the Supreme Court regarding the proper protocol for law enforcement officials when executing search warrants on computers, abuse of discretion is commonplace. In effect Rule 41(g), which grants an individual the constitutional right to the return of property, has been exploited to allow abuse of discretion as well. In order to adequately protect citizens' privacy rights and rights of intangible property in the twenty-first century, Congress should create a new categorical rule for the return of property in the digital context.[172]

---

[169] *See* United States v. Gladding, 775 F.3d 1149, 1153 (9th Cir. 2014).

[170] *See id.* at 1153–54.

[171] *See id.*; *see also* Kaplan, *supra* note 79, at 14 (discussing the problems with the Ninth Circuit's holding).

[172] *See supra* Part IV.