COURTING CHAOS: CONFLICTING GUIDANCE FROM COURTS HIGHLIGHTS THE NEED FOR CLEARER RULES TO GOVERN THE SEARCH AND SEIZURE OF DIGITAL EVIDENCE

Lily R. Robinton*

12 YALE J.L. & TECH. 311 (2010)

ABSTRACT

Today's digital devices allow users to store an astounding amount of personal information and data of all types. People now favor hard drives and e-mails over file cabinets and letters. When conducting criminal investigations in today's high-tech world, forensic analysts may compare digital fingerprints rather than physical ones. Investigators must obtain search warrants before examining any digital device for evidence of criminal activity, just as they would before searching a suspect's car, home, or office. In the digital context, however, the warrant requirement goes awry. Traditional search and seizure rules fail to prevent general, exploratory searches, which threaten individual privacy rights. Courts recognizing this problem have adopted "special approaches" for conducting digital media searches. Although these approaches provide greater protection for privacy rights, they often severely hamper legitimate law-enforcement interests. In order to both preserve privacy rights and promote justice, legislatures must enact laws directed at the search and seizure of digital media. These laws should (1) require investigators to follow narrow search protocols, but allow expanded searches where necessary; (2) require investigators to obtain a second warrant before seizing out-of-scope evidence, with a narrow exception; and 3) require a taint team to review digital media containing privileged or third party files.

---

* UCLA School of Law, J.D., Managing Editor, UCLA Law Review, Senior Articles Editor, UCLA Journal of Law & Technology, 2008-2009, U.C. San Diego, B.S., Biology. I would like to thank the attorneys at the U.S. Attorney's Office for the Northern District of California, San Jose, for inspiring me to write this article, with thanks in particular to Assistant U.S. Attorneys Hanley Chew, Jeffrey Schenk, Daniel Kaleba, Susan Knight, and Jeff Nedrow for taking the time to answer my questions and guide me to resources. I would also like to thank Chris Beeson, Director of the Regional District Forensics Lab for the Northern District of California, for setting aside time in his busy schedule to give me an overview of how forensics analysts proceed with the complicated task of searching for digital evidence. And of course, thanks to my friends and family for edits and encouragement.

TABLE OF CONTENTS

INTRODUCTION

On August 26, 2009, searches and seizures of digital property within the Ninth Circuit ground to a screeching halt.[1] The culprit? A landmark opinion authored on that date by the Chief Judge of the Ninth Circuit, Alex Kozinski, in a case already fraught with controversy: *United States v. Comprehensive Drug Testing, Inc.*[2] (*CDT*). *CDT* stemmed from the federal government's investigation into the illegal distribution and use of steroids in Major League Baseball (MLB), which implicated well-known players such as Barry Bonds, Alex Rodriguez, Sammy Sosa, and Manny Ramirez.[3] Several years of investigation gave the government probable cause to believe that at least ten Major League Baseball players had received illegal steroids from Bay Area Labs Cooperative. Federal investigators obtained a warrant to search the computer records of a private company retained by the MLB Players' Association to oversee its drug testing program.[4] The warrant authorized seizure of drug test records pertaining to those ten named players, but prosecutors discovered and reviewed a directory containing hundreds of records relating to other sports' drug testing programs. Prosecutors then sought additional warrants to seize records and specimens pertaining to approximately one hundred other players who had tested positive for steroids. This move led to a heated debate in several lower courts over whether the government acted properly in reviewing and seeking additional warrants for data that fell outside the scope of the initial search.[5]

In *CDT*, a limited en banc panel comprised of eleven judges overturned an earlier Ninth Circuit opinion written by a three-judge panel in favor of the government.[6] The *CDT* majority

---

[1] *See* Brief for the United States in Support of Rehearing En Banc by the Full Court at 1, 6, United States v. Comprehensive Drug Testing, Inc. (*CDT II*), 579 F.3d 989 (9th Cir. 2009) (en banc) (Nos. 05-10067, 05-15006, 05-55354) ("The government is accordingly laboring under the direct effects of this new legal regime. Many United States Attorney's Offices have been chilled from seeking any new warrants to search computers.").

[2] *CDT II*, 579 F.3d.

[3] *See id.* at 993; 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, 1151 (2007); Paul Elias, *Feds Seek Rehearing of Baseball Drug List Ruling*, ASSOCIATED PRESS, Nov. 25, 2009.

[4] *See* United States v. Comprehensive Drug Testing (*CDT I*), 513 F.3d 1085, 1090-94 & n.5 (9th Cir. 2008), *rev'd en banc and vacated*, 579 F.3d 989.

[5] *See CDT II*, 579 F.3d at 993-94.

[6] *See CDT I*, 513 F.3d 1085 (9th Cir. 2008), *rev'd en banc and vacated*, 579 F.3d 989.

held that the government had willfully disregarded the limitations of the search warrant to obtain out-of-scope evidence illegally; however, it was not the majority's disapproval of the government's actions that catalyzed the ensuing squall. In his August 26, 2009, opinion, Chief Judge Kozinski wrote, "This case is about a federal investigation into steroid use by professional baseball players. More generally, however, it's about the procedures and safeguards that federal courts must observe in issuing and administering search warrants and subpoenas for electronically stored information."[7] After determining that the government had acted improperly, the opinion set forth extremely restrictive guidelines to govern the search and seizure of digital property.[8] The majority took a significant step in shifting its focus from the facts of the case to the general issue of how magistrates and federal agents should issue and execute search warrants for electronically stored information. Styled as "guidelines," but viewed by magistrate judges as mandatory, the new rules set forth in *CDT* have wreaked havoc on government investigations in the Ninth Circuit, and have been criticized for departing from controlling precedent.[9] The opinion has caused such a stir that Solicitor General Elena Kagan, along with every U.S. Attorney's Office in the Ninth Circuit, and

---

[7] 579 F.3d at 993.

[8] Chief Judge Kozinski summarized his rules as follows:

> 1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
>
> 2. Segregation and redaction must be either done by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.
>
> 3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.
>
> 4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.
>
> 5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

Id. at 1006 (internal citations omitted); *see* Hugh Kaplan & Christine Mumford, *Attorneys, Academics Sort Through Landmark Case on Computer Searches*, 85 CRIM. L. REP. 688 (2009).

[9] *See* Brief for the United States in Support of Rehearing En Banc by the Full Court, *supra* note 1, at 1, 5, 8-14.

five top attorneys from Main Justice, have petitioned the full twenty-seven member court to reconsider the decision.[10]

This is not the first controversy to arise over the search and seizure of digital property. Crooks and innocents alike store information relating to every facet of their lives on digital devices, making them attractive targets for criminal investigators.[11] Courts across the nation have struggled to apply Fourth Amendment principles to digital searches to ensure the searches do not expand into exploratory hunts that threaten individual privacy. Their attempts have produced a tangle of conflicting authority, and as demonstrated by *CDT*, a digital search resolution remains elusive. To add to the confusion, different government agencies may disagree about how to approach and execute a search and seizure of digital property.[12]

Regardless of whether the Ninth Circuit accepts or declines the federal government's petition to reconsider its decision in *CDT*, or whether the Court overturns the decision, the storm of controversy created by *CDT* has underscored the need for a uniform set of rules that successfully balances individual privacy concerns against legitimate law enforcement interests. As Chief Judge Kozinski stated, "Everyone's interests are best served if there are clear rules to follow that strike a fair balance between the legitimate needs of law enforcement and the right of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment."[13] His rules, however, along with the rules of other courts, have thus far fallen woefully short of achieving this balance. This Article addresses these conflicting interests and argues for a legislative solution that combines and harmonizes existing rules.

Part I of this Article begins by introducing the history and framework of the warrant requirement, which grew from the Fourth Amendment. Part I also addresses the significance of the threat to privacy posed by unlimited digital searches in response to those who claim that law-abiding citizens need not worry about privacy intrusions. Part II addresses the complications introduced by digital media, and Part III explains the conflicting ways in which courts have responded to these complications. Part IV argues that legislatures should create statutory schemes to address

---

[10] *See* Elias, *supra* note 3; Laura Ernde, *Prosecutors: Steroid Ruling Hurting Other Investigations: Obama Asks 9th Circuit To Reconsider Steroid Ruling*, DAILY J., Nov. 27, 2009. Due to the large size of the Ninth Circuit, a limited en banc panel consisting of eleven judges usually convenes to hear appeals. *See* Elias, *supra* note 3.

[11] *See infra* Part II.

[12] *See* Kaplan & Mumford, *supra* note 8.

[13] *CDT II*, 579 F.3d 989, 1006 (9th Cir. 2009).

the issue. Part IV goes on to propose rules governing search and seizure of digital property, which would tackle the unique privacy concerns raised by these searches without hampering government investigations.

I. THE WARRANT REQUIREMENT, AND THE "I HAVE NOTHING TO HIDE" RETORT

A. The History and Framework of the Warrant Requirement

In 1761, the citizens of Massachusetts lived without the protections of the Fourth Amendment.[14] They lived in a world where "writs of assistance," a type of general warrant, authorized meticulous searches of their private homes and businesses, and allowed searching officials to pry open locks, cast aside bars, and seize offending articles on no more than bare suspicion.[15] In February of 1761, a lawyer named James Otis gave a passionate, five-hour speech against the perils of the "writ of assistance."[16] What Otis lacked in brevity, he made up for in emotion as he effectively conveyed the fear incited by the specter of the general warrant:

> Every one with this writ may be a tyrant; if this commission be legal, a tyrant in a legal manner, also, may control, imprison, or murder any one within the realm. In the next place, it is perpetual; there is no return. A man is accountable to no person for his doings. Every man may reign secure in his petty tyranny, and spread terror and desolation around him, until the trump of the

[14] *See* JOHN CLARK RIDPATH, JAMES OTIS, THE PRE-REVOLUTIONIST: A BRIEF INTERPRETATION OF THE LIFE AND WORK OF A PATRIOT 37-45 (1898); *see also* Writs of Assistance: Colonial America, http://www.u-s-history.com/pages/h1205.html (last visited Mar. 28, 2010).

[15] *See* RIDPATH, *supra* note 14; Samantha Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, 10 YALE J.L. & TECH. 120, 123 (2008); James Otis, Against Writs of Assistance (Feb. 1761), *available at* http://www.nhinet.org/ccs/docs/writs.htm; James Otis, In Opposition to Writs of Assistance (Feb. 1761) [hereinafter Otis, In Opposition to Writs of Assistance], *reprinted in* 8 THE WORLD'S FAMOUS ORATIONS 27 (William Jennings Bryan ed., 1906).

[16] *See* RIDPATH, *supra* note 14, at 48; Otis, In Opposition to Writs of Assistance, *supra* note 15; *see also* Akhil Reed Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, 30 SUFFOLK U. L. REV. 53, 53 (1996). James Otis represented a group of Boston Merchants opposing the writs before the Superior Court of Massachusetts. *Id.* at 76.

> Archangel shall excite different emotions in his soul.[17]

Otis' plea to banish the writ of assistance fell on deaf ears,[18] but a few years later, in the cases of *Wilkes v. Wood*[19] and *Entick v. Carrington*,[20] the English court refused to allow the government to rely on general warrants lacking probable cause to justify the arrests of political activists and subsequent searches of their homes and belongings. These two cases have been called "the O.J. Simpson and Rodney King cases of their day,"[21] and likely influenced the Framers of the Constitution as they drafted an amendment that would protect the American citizens against the terrors preached by James Otis.[22]

The Fourth Amendment, straight from the quills of the Framers, ensures that

> [t]he 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.[23]

A government-instigated search of anything a person deems private must be reasonable to pass muster under the Fourth Amendment.[24] The Supreme Court has developed two procedural tools to ensure the protections of the Fourth Amendment. The first

---

[17] *See* RIDPATH, *supra* note 14, at 53; Otis, In Opposition to Writs of Assistance, *supra* note 15.
[18] Writs of Assistance, *supra* note 14.
[19] Wilkes v. Wood, (1763) 98 Eng. Rep. 489 (C.P.); Lofft 1.
[20] Entick v. Carrington, (1765) 95 Eng. Rep. 807 (C.P.); 2 Wils. K. B. 275.
[21] Amar, *supra* note 16, at 65.
[22] *See id.* at 64-65; Trepel, *supra* note 15, at 123-24.
[23] U.S. CONST. amend. IV.
[24] *See id.*; Carroll v. United States, 267 U.S. 132, 155 (1925) (setting forth a reasonableness standard for probable cause); *Investigations and Police Practices,* 38 GEO. L.J. ANN. REV. CRIM. PROC. 3, 43-44 (2009) ("Under the Fourth Amendment, every search or seizure by a government agent must be reasonable."); Regensburger, *supra* note 3, at 1156. The Fourth Amendment protects individuals from government intrusions that invade privacy. *Investigations and Police Practices*, *supra*, at 5-8. A person must have a legitimate expectation of privacy to merit protection under the Fourth Amendment. *Id.* If a person has a subjective expectation of privacy, and society accepts that expectation as objectively reasonable, the Supreme Court will deem that expectation legitimate. *Id.*

is the warrant requirement. With some exceptions, warrantless searches are per se unreasonable under the Fourth Amendment.[25]

Before investigators can obtain a search warrant, they must have probable cause to believe they will discover evidence of the alleged crime during the search. A neutral magistrate must consider the facts and circumstances presented in a warrant application, and may issue the warrant only after finding a substantial basis that probable cause exists to search the named area and seize any evidence.[26] The warrant must describe with particularity the places investigators plan to search and items they hope to seize. The particularity requirement defines the scope of the warrant, and protects the privacy interests in a person's home and possessions from broad, exploratory rummaging by ensuring that each search is narrowly tailored to the justifications presented to the magistrate.[27]

A warrant contains sufficient particularity when it leaves nothing to the discretion of the executing officers and officers "can with reasonable effort ascertain and identify the place intended."[28] However, an overbroad warrant, or a warrant containing mistaken information may be "cured" if executing officers can rely on personal knowledge to narrow and identify the place intended to be searched.[29] An affidavit incorporated by reference or attachment to

---

[25] The warrant requirement applies to any place in which a person holds a reasonable expectation of privacy. *See* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 80 (1994).

[26] *See id.*; *see also* Illinois v. Gates, 462 U.S. 213, 238 (1983) ("The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place."); *Investigations and Police Practices*, *supra* note 24, at 21-28 (2009).

[27] *See* U.S. CONST. amend. IV (requiring that warrants shall "particularly describe[e] the place to be searched, and the persons or things to be seized"); Andresen v. Maryland, 427 U.S. 463, 480 (1976) ("[T]he problem [posed by the general warrant] is 'not that of intrusion Per se, but of a general, exploratory rummaging in a person's belongings.' . . . [The Fourth Amendment addresses the problem] by requiring a 'particular description' of the things to be seized." (alterations in original) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971)); *Investigations and Police Practices*, *supra* note 24, at 27-28; Winick, *supra* note 25, at 86.

[28] Steele v. United States, 267 U.S. 498, 503 (1925); *see also Andresen*, 427 U.S. 463; *Investigations and Police Practices*, *supra* note 24, at 28-31.

[29] *See, e.g.*, United States v. Judd, 889 F.2d 1410, 1413 (5th Cir. 1989) (holding that a warrant that failed to describe a company's second office still sufficiently particular because agents checked city business license records, bank records, corporate filings, and the address on the company's letterhead to determine the location to be searched; the offices were only 25-30 feet apart; and the company had only leased the second office three weeks prior to the search). *But see* United States v. Ellis, 971 F.2d 701, 704 (11th Cir. 1992) (holding that officers'

the warrant that lists items not mentioned in the warrant itself may also cure an overbroad warrant.[30]

When a defendant challenges the particularity of a warrant authorizing the search of his or her records, courts will deem the warrant particular if it has been narrowed as much as the information available to the agents will allow. For example, in *United States v. Gardiner*,[31] the Sixth Circuit found a warrant listing a variety of personal and business records to be sufficiently particular because it sought items pertaining to the time frame of the crime, and all of the listed records would logically relate to the alleged financial crimes.[32] In *United States v. Mathison*,[33] the Eighth Circuit deemed particular a warrant seeking *all* records pertaining to the suspect's seventeen distinct businesses, as well as information with respect to eleven individuals. The Eighth Circuit reasoned that the affidavit supporting the warrant contained considerable evidence of the suspect's involvement in illegal activities and demonstrated that the records sought would substantiate the suspect's involvement.[34] In finding the warrant sufficiently particular, the court in *Mathison* declined to employ the exclusionary rule, which is the second procedural tool designed to ensure the protections of the Fourth Amendment.[35] The exclusionary rule functions to suppress from the record any evidence obtained through an illegal search and seizure. This can include evidence obtained during execution of an overbroad warrant and evidence that falls outside the scope of the warrant.[36]

The exclusionary rule does not proceed directly from the Fourth Amendment as a means of "cur[ing] the invasion of the defendant's rights which he has already suffered,"[37] but rather developed as a judicially created remedy designed to deter

---

personal knowledge of the suspect's name and a neighbor's word that the suspect lived in the "fifth mobile home" could not cure a warrant that failed to name the suspect, did not describe the premises to be searched, and erroneously pinpointed the premises as the "third mobile home" when none of the searching officers had previously observed the mobile home and thus had no other knowledge by which to narrow the search).

[30] *See, e.g.*, *In re* Search of Office of Tylman, 245 F.3d 978, 980-81 (7th Cir. 2001); United States v. Towne, 997 F.2d 537, 548 (9th Cir. 1993).

[31] 463 F.3d 445 (6th Cir. 2006).

[32] *Id.* at 471.

[33] 157 F.3d 541 (8th Cir. 1998).

[34] *Id.* at 547-49.

[35] *Id.* at 549.

[36] *See* Mapp v. Ohio, 367 U.S. 643, 654 (1961); Weeks v. United States, 232 U.S. 383, 398 (1914); *Investigations and Police Practices*, *supra* note 24, at 40-41; Winick, *supra* note 25, at 80, 85.

[37] United States v. Leon, 468 U.S. 897, 906 (1984) (quoting Stone v. Powell, 428 U.S. 465, 540 (1976) (White, J., dissenting)).

constitutional violations.[38] Thus, where the exclusion of evidence would not advance the purpose of the rule, the court will allow its introduction under the so-called good faith exception.[39] For example, in *United States v. Leon*,[40] the district court found that the magistrate who had granted the warrant had done so in error, as the evidence submitted with the warrant application failed to establish probable cause.[41] Nevertheless, the Supreme Court declined to suppress evidence on the grounds that the exclusionary rule "cannot be expected, and should not be applied, to deter objectively reasonable law enforcement activity."[42] The good faith exception to the exclusionary rule thus highlights the importance of issuing warrants based on a proper articulation of places to be searched and items to be seized.

B. The "I Have Nothing To Hide" Retort

A person will likely feel that the government has violated his right to privacy if agents begin rummaging through the medicine cabinet to search for stolen fifty-inch flat screens, which clearly cannot fit next to the Aspirin. The same person, however, may fail to perceive an examination of every file on his computer as intrusive. The obscure nature of the digital search, and the lack of any spatial correlation between the evidence sought and the files examined, can mask potential privacy violations. It is easy to discount the danger of the general digital search and argue complacently, "So what if the government looks through every file on my computer? I have nothing to hide. I'd rather sacrifice a little privacy for the sake of bringing criminals to justice." On this view, justice should trump privacy: government intrusion into digital data would be a threat to criminals, but not to law abiding citizens. Most people do not sympathize with the white-collar criminal who gets caught with child pornography during a search of his computer for evidence of investment fraud. Most proponents of the "nothing to hide" viewpoint would argue that only criminals need fear a general search of digital media.[43]

---

[38] *See Leon*, 468 U.S. at 906; *Investigations and Police Practices*, *supra* note 24, at 201.
[39] *See Leon*, 468 U.S. at 919-20; *Investigations and Police Practices*, *supra* note 24, at 204-06.
[40] 468 U.S. 897 (1984).
[41] *Id.* at 900-03.
[42] *Id.* at 919.
[43] *See* Daniel J. Solove, *"I've Got Nothing To Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 746-47 (2007) ("The argument that no privacy problem exists if a person has nothing to hide is frequently made in connection with many privacy issues. . . . The nothing to

Scholar Daniel Solove addresses this common retort by pointing out that "[p]rivacy . . . is not the trumpeting of the individual against society's interests, but the protection of the individual based on society's own norms and values. . . . [P]rivacy has a social value."[44] Solove argues persuasively that a society without the cushion of privacy would be unlivable; life in a free society necessitates rules that may unintentionally shield criminal behavior.[45]

Furthermore, even those who think they have nothing to hide might find themselves unpleasantly surprised by what might turn up in a probing search of their digital media. Solove captures this possibility with a colorful quotation from Friedrich Durrenmatt's novella *Traps*, in which a man who believes himself innocent inquires as to his crime: "'An altogether minor matter,' the prosecutor replie[s] . . . 'A crime can always be found.'"[46] In a world where computers facilitate and store oceans of data about every aspect of our lives, it seems certain that some type of crime can always be found among the bits and bytes of the average hard drive.

II. LET'S GET DIGITAL! DIGITAL!

Fourth Amendment jurisprudence has evolved to suit searches conducted in a physical world with the human senses.[47] "In the time before the atom, what we could see with our eyes was all there was. Similarly, when the country was young and the universe of searchable data was limited to 'papers, and effects,' law enforcement agents were able to literally see everything covered by Fourth Amendment protections."[48] This is no longer true. Technology now allows us to conduct much of our social and professional lives in cyberspace, while storing hoards of information of all types in digital format. People today use computers to store images, movies, documents, personal records, and correspondence.[49] Computers double as "photo albums,

---

hide argument is one of the primary arguments made when balancing privacy against security.").

[44] *Id.* at 763.

[45] *Id.*

[46] *Id.* at 750 (quoting FRIEDRICH DURRENMATT, TRAPS 23 (Richard & Clara Winston trans., 1960)).

[47] *See* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 290 (2005); *infra* notes 96-100 and accompanying text (discussing the plain view doctrine and its sensory corollaries).

[48] Aaron Stanley, Note, *The Continuing Evolution of Consent and Authority in Digital Search and Seizure*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 179, 188 (2008).

[49] *See* RayMing Chang, *Why the Plain View Doctrine Should Not Apply To Digital Evidence*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31, 35 (2007),

stereos, telephones, desktops, file cabinets, waste paper baskets, and televisions,"[50] "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more."[51] The storage capacity of computers today is astonishing. As of April of 2009, the highest capacity commercial hard drives were capable of storing two terabytes of data. A terabyte can hold approximately 1000 hours of video, 250,000 four-minute songs, 1,000,000 thick books of about 500 pages each, or as much information as can be printed on the paper from 50,000 trees. A desktop hard drive might store between 120 gigabytes and two terabytes.[52] Even a measly 80-gigabyte desktop drive stores the equivalent of 40 million pages of text.[53]

When investigators decide to search a suspect's computer, they face vast quantities of information. If stored in written form, that data might fill an entire library. As technology advances to allow a user to squeeze larger quantities of data into tinier spaces, the amount of information that can be contained in digital format will continue to grow.[54] Furthermore, in addition to the wealth of information stored on files purposely saved by an individual, investigators mine the hard drive for deleted files and glean information from metadata.[55]

---

http://ssrn.com/abstract_id=949575. *See generally* Encyclopedia Britannica Online, Living in Cyberspace, http://www.britannica.com/EBchecked/topic/130429/computer/216089/Living-in-cyberspace (last visited Mar. 28, 2010).

[50] Trepel, *supra* note 15, at 128.

[51] United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007) (quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005)).

[52] *See* Darren Murph, *Western Digital's 2TB Caviar Green HDD on sale in Australia*, ENGADGET (Jan. 26, 2009, 11:47 PM) http://www.engadget.com/2009/01/26/western-digitals-2tb-caviar-green-hdd-on-sale-in-australia (Jan. 26, 2009, 11:47 p.m.); Hard Drive Help, The Spacious Terabyte Hard Drive, http://www.hard-drive-help.com/terabyte-hard-drive.html (last visited Mar. 28, 2010); Wisegeek, How Much Text Is in a Kilobyte or Megabyte?, http://www.wisegeek.com/how-much-text-is-in-a-kilobyte-or-megabyte.htm (last visited Mar. 28, 2010).

[53] Trepel, *supra* note 15, at 128-29.

[54] "North Carolina State University engineers have created a new material that would allow a fingernail-size computer chip to store the equivalent of 20 high-definition DVDs or 250 million pages of text, far exceeding the storage capacities of today's computer memory systems." *Researchers Develop Material That Could Boost Data Storage, Save Energy*, PHYSORG.COM, Oct. 20, 2009, http://www.physorg.com/news175252581.html.

[55] Metadata consists of information that characterizes the digitally stored data and answers the "who, what, when, where, why, and how about every facet of the data that are being documented" on a digital storage device. USGS, Frequently-Asked Questions on FGDC Metadata, http://geology.usgs.gov/tools/metadata/tools/doc/faq.html (last visited Oct. 14, 2009); *see also* Trepel, *supra* note 15, at 129.

A. Digital Context Complications

The advanced storage capabilities of today's digital media complicate the scope of digital searches. For one, the particularity requirement can malfunction in the digital context because searching for evidence of a crime on a computer is akin to searching for a needle in a haystack. Investigators usually cannot predict where, or in what format, they might find the relevant information, and thus cannot "particularly describ[e]" the "place to be searched" or the "things to be seized."[56] As Professor Orin Kerr points out, "[i]n the physical world, different spatial regions are used for different purposes. This allows the police to make educated guesses as to where evidence may or may not be found . . . ."[57] In the physical world, one might look for an incriminating letter in a file folder or a desk drawer. Drugs or guns might be stored in shoeboxes or bedside tables. The money might be under the mattress. In the computer context, however, the location of evidence does not necessarily depend on the character of the evidence itself. Information stored on a computer is represented by "zeros and ones of electricity,"[58] making the format and location of any stored information flexible, and difficult to predict. Investigators searching a suspect's house for stolen stereo equipment can logically rule out the medicine cabinet as a possible location, but anticipating the location of electronic evidence is inherently more difficult because "electronic evidence can be located anywhere. . . . [T]he investigator can never rule out a particular part of the hard drive ex ante."[59]

Some courts resolve the issue by allowing warrants to describe the media to be searched in general terms, without requiring investigators to pinpoint the particular files they plan to search.[60] This rule recognizes the concern that investigators might not be able to predict whether evidence will be located on a suspect's computer, an external hard drive, a CD, a flash drive, or some other external storage device.[61] Other courts have taken a

---

[56] U.S. CONST. amend. IV; *see* Kerr, *supra* note 47, at 303.
[57] Kerr, *supra* note 47, at 303.
[58] *Id.* at 284.
[59] *Id.* at 304.
[60] *See* United States v. Lacy, 119 F.3d 742, 746 (9th Cir. 1997) ("[T]his type of generic classification is acceptable 'when a more precise description is not possible.'" (alteration in original) (quoting *United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982)).
[61] Regensburger, *supra* note 3, at 1157; Stanley, *supra* note 48, at 217; *see, e.g.*, United States v. Lacy, 119 F.3d 742, 746-47 (9th Cir. 1997) ("The government knew Lacy had downloaded computerized visual depictions of child pornography, but did not know whether the images were stored on the hard drive or on one or more of his many computer disks . . . there was no way to specify

more restrictive approach by requiring investigators to name at least the type of evidence sought.[62] Most courts, however, allow broad particularity designations when investigators cannot predict precisely which files contain evidence. These courts recognize that investigators may need to seize information that appears innocuous, but that may later prove incriminating in conjunction with other evidence.[63]

B. Current Law Enforcement Methods for Conducting Digital Searches

So how might investigators wade through this quagmire of data? The simplest option would be for the officer to sit down at the suspect's computer and examine the data manually. The officer would simply turn the computer on, and begin opening files one-at-a-time in search of something incriminating.

Practical drawbacks, however, preclude the use of this method.[64] For one, the investigator would have to sift through a forest's worth of documents, making the search extremely inefficient. Such a search would fail to locate incriminating files deleted by the suspect, and the officer would risk destroying evidence during the search process. Simply opening a file or turning on a computer can overwrite deleted data, and may alter time stamps on the data, which investigators might need to show

---

what hardware and software had to be seized to retrieve the images accurately.").

[62] *See, e.g.*, United States v. Riccardi, 405 F.3d 852, 862 (10th Cir. 2005).

[63] *See* United States v. Wuagneux, 683 F.2d 1343, 1349 (11th Cir. 1982) ("[C]rimes may require the assembly of a 'paper puzzle' from a large number of seemingly innocuous pieces of individual evidence: 'The complexity of an illegal scheme may not be used as a shield to avoid detection when the State has demonstrated probable cause to believe that a crime has been committed and probable cause to believe that evidence of this crime is in the suspect's possession.' It is universally recognized that the particularity requirement must be applied with a practical margin of flexibility, depending on the type of property to be seized, and that a description of property will be acceptable if it is as specific as the circumstances and nature of activity under investigation permit." (quoting Andresen v. Maryland, 427 U.S. 463, 481 n.10 (1976))); Regensburger, *supra* note 3, at 1156-57; *see also* United States v. Jacob, 657 F.2d 49, 52 (4th Cir. 1981) (recognizing the complexity of the alleged crime as a factor in determining whether the warrant met with particularity requirements); United States v. Abrams, 615 F.2d 541, 548 (1st Cir. 1980) (Campbell, J., concurring) ("The investigators usually do not, and often cannot, know in advance precisely what they will find when they search through files pursuant to a warrant. They, therefore, may find it difficult to describe what they are seeking, other than to say that they expect to find, and will seize, documents constituting evidence of the particular fraud.").

[64] *See* G. Robert McLain, Jr., Note, United States v. Hill*: A New Rule, But No Clarity for the Rules Governing Computer Searches and Seizures*, 14 GEO. MASON L. REV. 1071, 1092-93 (2007).

the time the suspect created or last accessed a file. Not only would this method erase possibly relevant information, it would also defeat investigators' attempts to authenticate the evidence and disprove tampering. An investigator might as well "walk[] into a murder scene with muddy boots, remov[e], bare-handed, a knife from the victim, drop[] it in his coat pocket and return[] to the office."[65]

It is nearly impossible to search a hard drive without the assistance of some kind of software program.[66] To search digital media properly, investigators elicit the help of digital forensics specialists, who use a number of tools and forensics techniques.[67] Courts have consistently recognized that requiring police to search digital media at the suspect's home or office could create an extreme burden on both the individual's privacy, as well as on police resources. Investigators might need to camp out for days to conduct a thorough search, which would severely disrupt the suspect's life or business. Forensic analysts would need to cart their own computers, equipped with forensic tools and special programs, to the scene of every search. This would create an enormous hassle and burden investigative resources. To alleviate these concerns, courts generally permit removal of digital media to an off-site location for examination by experts, although some courts urge investigators to return equipment as soon as possible to minimize disruption of an individual's activities.[68]

---

[65] *Id.* at 1094.

[66] United States v. Long, 425 F.3d 482, 487 (7th Cir. 2005) ("[W]e observe that it is impossible to search computer hardware or software without using some type of software."); Interview with Chris Beeson, Director of the Regional District Forensics Lab for the Northern District of California (Dec. 2, 2009). The Regional District Forensics Lab for the Northern District of California is one of fourteen regional computer forensics laboratories across the country. Regional computer forensic labs conduct digital forensic examinations for all law enforcement agencies, including the Federal Bureau of Investigation, within each region. Interview with Chris Beeson, *supra*.

[67] Interview with Chris Beeson, *supra* note 66; *see also* McLain, *supra* note 64, at 1093; Regensburger, *supra* note 3, at 1155. *See generally* U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, *available at* http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf [hereinafter DOJ GUIDELINES] (setting forth guidelines for searches and seizures of digital media).

[68] *See* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizure: A Perspective and a Primer*, 75 MISS. L.J. 193, 267 (2006); Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 541 (2005); McLain, *supra* note 64, at 1093-94; *see also, e.g.*, United States v. Walser, 275 F.3d 981, 985 (10th Cir. 2001); United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000); United States v. Upham, 168 F.3d 532, 535-36 (1st Cir. 1999) (upholding seizure and subsequent off-site search of computer for "needles in the computer haystack"); United States v. Hill, 322 F. Supp. 2d 1081, 1089 (C.D. Cal. 2004) ("To be certain that the medium in question does

To avoid contaminating or damaging any digital evidence, forensic investigators first make a "bitstream" copy of the media they plan to search. The bitstream image captures every piece of information on the target drive, including files accessible by the normal user, deleted files, metadata, and empty space. Investigators save the bitstream copy in "read only" format to ensure they do not accidentally alter the evidence during analysis.[69] Forensic investigators then narrow the set of data to be searched using "known fingerprints" or "hash value" programs, and forensic tools such as EnCase or Forensic Tool Kit (FTK).[70]

Before analyzing investigators' search methods under the Fourth Amendment, one must have a basic understanding of how hash value programs operate. A "hash value" is an identifier that characterizes a data set. The relationship between a hash value and its data set compares roughly to the relationship between an organism and its DNA sequence; analysis of two separate data sets will rarely return the same hash value. Just as forensic analysts use DNA to determine the identities of criminal suspects or victims, digital forensic investigators use hash values to identify data—programs, images, files, etc.—on a computer.[71]

A hash value program converts each data set on the target drive into its corresponding identifier and matches the resulting identifiers with known identifiers. For example, investigators might suspect an individual of using a specific hacking program, or of downloading a particular image of child pornography. By comparing hash values from the suspect's computer with known values for the hacking program or the image, investigators can

---

not contain any seizable material, the officers would have to examine every one of what may be thousands of files on a disk—a process that could take many hours and perhaps days. Taking that much time to conduct the search would not only impose a significant and unjustified burden on police resources, it would also make the search more intrusive." (internal citation omitted)); *cf.* United States v. Leveto, 343 F. Supp. 2d 434, 441 (W.D. Pa. 2004) (approving of investigators' steps to minimize upheaval of defendant's business, including downloading and copying files at the scene rather than removing them for off-site review); *United States v. Hunter*, 13 F. Supp. 2d 574, 583 (D. Vt. 1998) ("At the very least, the government should copy and return the equipment as soon as possible.").

[69] *See* Clancy, *supra* note 68, at 265-67; Interview with Chris Beeson, *supra* note 66.

[70] McLain, *supra* note 64, at 1094; Interview with Chris Beeson, *supra* note 66; Interview with Hanley Chew, Assistant U.S. Att'y, U.S. Attorney's Office, San Jose Branch (Nov. 16, 2009).

[71] Interview with Chris Beeson, *supra* note 66; Interview with Hanley Chew, *supra* note 70; *see also* Kerr, *supra* note 68, at 541 ("A hash is a complicated mathematical operation, performed by a computer on a string of data, that can be used to determine whether two files are identical.").

determine if either exists on the suspect's hard drive.[72] Hash programs can also recognize "normal" files, such as Microsoft Windows or Word Perfect, which commonly turn up on computers. Forensic investigators negatively screen out these common operating system files and applications to reduce the size of the data set they will search.[73]

Forensic tools such as EnCase and FTK allow investigators to access deleted files, eliminate common operating system files, preview image files, flag encrypted files, and search the entire hard drive or active files by keyword or phrase. These tools also allow investigators to identify mismatched file extensions. For instance, if a suspect attempts to hide incriminating evidence and mislead investigators by changing the .jpg extensions on images of child pornography to .doc extensions, the forensic program will alert the investigator to the altered files.[74] However, criminals may devise other strategies for disguising incriminating evidence, which forensic tools will not detect. For example, the suspect might embed the image of child pornography within a word document, as opposed to changing the file extension. A forensic investigator searching for images in .jpg files may overlook the embedded evidence in the .doc file. The forensic program will not flag such files as altered or suspicious.[75]

III. DEVELOPING DIGITAL RULES

As digital media searches have become more frequent, courts face the challenge of applying Fourth Amendment principles, which were designed for discrete physical-world searches, to vast and amorphous digital spaces. Courts and scholars remain divided on the issue, and have roughly separated into two camps.[76] Adherents of one viewpoint advocate for application of existing rules to digital searches, and argue that computers are nothing more than glorified containers holding files that represent physical documents.[77] Followers of the other viewpoint argue that the "container analogy" is inadequate, and search of digital media

[72] Kerr, *supra* note 68, at 541; Interview with Hanley Chew, *supra* note 70. Forensic analysts also use hashes to ensure the bitstream copy accurately matches the original drive. Kerr, *supra* note 68, at 546.
[73] Interview with Chris Beeson, *supra* note 66.
[74] McLain, *supra* note 64, at 1094-95.
[75] Interview with Chris Beeson, *supra* note 66.
[76] *See* Clancy, *supra* note 68, at 196.
[77] *See, e.g.*, *id.* at 271 (arguing that "there is nothing 'special' in the nature of computer searches that differentiate [sic] them in any principled way from other document and container searches.").

requires a "special approach" with new rules and procedures.[78] The prevailing concern in both camps remains the same: whether existing principles suffice in the digital arena to prevent every digital search from becoming the kind of general, exploratory search prohibited by the Fourth Amendment.

A. Traditional Rules Allow Investigators To Scan All Digital Media Files—No Search Protocol Required

Courts willing to compare computers to file cabinets recognize that the versatility and massive storage capacity of computers complicate the task of parsing through intermingled files. Investigators examining computers face a plethora of intermingled data and cannot avoid combing through oceans of material not specified in the warrant.[79] Courts have resolved this issue with respect to physical documents by allowing investigators to scan all documents in order to ascertain their relevancy.[80] In *Andresen v. Maryland*, the court noted:

> We recognize that there are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable. In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they

[78] *See, e.g.*, United States v. Carey, 172 F.3d 1268, 1275 & n.7 (10th Cir. 1999) (discrediting the comparison of computer searches to searches of file cabinets, and advocating for a "special approach" with respect to search and seizure of digital evidence); Winick, *supra* note 25, at 110 ("An analogy between a computer and a container oversimplifies a complex area of Fourth Amendment doctrine and ignores the realities of massive modern computer storage.").

[79] *See* United States v. Hunter, 13 F. Supp. 2d 574, 583 (D. Vt. 1998) ("Computer searches present the same problem as document searches—the intermingling of relevant and irrelevant material—but to a heightened degree.").

[80] *See, e.g.*, Andresen v. Maryland, 427 U.S. 463 (1976); United States v. Schandl, 947 F.2d 462, 465 (11th Cir. 1991) ("It was inevitable that some irrelevant materials would be seized as agents searched through numerous documents for evidence of tax evasion and failure to file, crimes that are generally only detected through the careful analysis and synthesis of a large number of documents."); United States v. Slocum, 708 F.2d 587, 604 (11th Cir. 1983) ("[A]n officer acting pursuant to such a warrant is entitled to examine any document he discovers, but that 'the perusal must cease at the point of which the warrant's inapplicability to each document is clear.'" (quoting United States v. Heldt, 668 F.2d 1238, 1267 (D.C. Cir. 1981))); United States v. Abbell, 963 F. Supp. 1178, 1198 (S.D. Fla. 1997) ("When executing a search warrant for documents, searching agents are entitled to at least cursorily examine each document at the specified search location.").

> are, in fact, among the papers authorized to be seized.[81]

By allowing investigators to peruse all documents in a suspect's possession, as opposed to only those stored in folders with relevant labels, courts "recognize[] the reality that few people keep documents of their criminal transactions in a folder marked 'drug records.'"[82]

Accordingly, most courts that accept the comparison between computers and file cabinets allow investigators to open and scan *all* digital files to ascertain the responsiveness of the data.[83] In *United States v. Gray*,[84] the court noted that "[c]omputer records are extremely susceptible to tampering, hiding, or destruction" and concluded that the searching agent "was not required to accept as accurate any file name or suffix and limit his search accordingly."[85] The courts in *United States v. Hunter* and *United States v. Hill* also declined to limit investigators' search methods on the grounds that criminals can easily mask incriminating evidence so it will not be discovered using rigid, predictable protocols.[86] In *United States v. Fumo*,[87] the court stated that

> regardless of the search protocols or keywords used by the government, the government may open and briefly examine each computer file to determine whether it is in the description recited in the warrant. . . . 'no tenet of the *Fourth Amendment* prohibits a search merely because it cannot be performed with surgical precision.'[88]

Some scholars argue that limiting the ability of investigators to scour digital media might encourage criminals to hide evidence outside the range of the search. They contend that

---

[81] *Andresen*, 427 U.S. at 482 n.11.
[82] United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990).
[83] *See* Clancy, *supra* note 68, at 198. For example, *United States v. Gray* compared digital evidence to paper records and documents, which "unlike illegal drugs or other contraband, may not appear incriminating on their face. As a result, in any search for records or documents, 'innocuous records must be examined to determine whether they fall into the category of those papers covered by the search warrant.'" 78 F. Supp. 2d 524, 528 (E.D. Va. 1999) (quoting United States v. Kufrovich, 997 F. Supp. 246, 264 (D. Conn. 1997)).
[84] 78 F. Supp. 2d 524.
[85] *Id.* at 529.
[86] United States v. Hill, 322 F. Supp. 2d 1081, 1090-91 (C.D. Cal. 2004); United States v. Hunter, 13 F. Supp. 2d 574, 583 (D. Vt. 1998).
[87] No. 06-319, 2007 U.S. Dist. LEXIS 80543 (E.D. Pa. Oct. 7, 2007).
[88] *Id.* at *16-17.

because criminals can disguise files, investigators have probable cause to view every file and should not be forced to employ restrictive search methods.[89] Supporting the stance against search protocols, the Supreme Court has ruled outside the digital search context that warrants need not outline the methods investigators plan to employ in conducting a search:

> Often in executing a warrant the police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant. . . . It would extend the Warrant Clause to the extreme to require that, whenever it is reasonably likely that Fourth Amendment rights may be affected in more than one way, the court must set forth precisely the procedures to be followed by the executing officers.[90]

This reasoning has been applied in the digital search scenario.[91] In fact, DOJ tuidelines expressly direct prosecutors to oppose restrictions imposed by magistrates that require the government to specify how it will examine digital media to find evidence responsive to the warrant.[92] Nevertheless, allowing agents to search every digital media file creates very real concerns. Many courts and commentators have reacted to this broad authorization by claiming that it operates with the plain view doctrine to transform every digital search into the type of general search prohibited by the Fourth Amendment.[93]

---

[89] *See, e.g.*, Chang, *supra* note 49, at 48-50; Clancy, *supra* note 68; Regensburger, *supra* note 3, at 1196-97.

[90] Dalia v. United States, 441 U.S. 238, 257-58 (1979) (holding that government agents need not specify the means by which they would execute installation of a wiretap authorized by warrant).

[91] *See, e.g.*, United States v. Vilar, No. S3 05-CR-621, 2007 U.S. Dist. LEXIS 26993, at *121-25 (S.D.N.Y. Apr. 4, 2007) (citing *Dalia* for the proposition that officers should not be required to specify ahead of time how they planned to search defendants computers, and stating that "[t]he majority view rejecting a protocol requirement makes good sense as there is no principle in the law that requires law enforcement officers to limit their investigative techniques ex ante, before conducting any kind of search.").

[92] DOJ GUIDELINES, *supra* note 67, at 80.

[93] *See* Chang, *supra* note 49, at 43-44; Kerr, *supra* note 47, at 304-05; Trepel, *supra* note 15, at 137-38; Winick, *supra* note 25, at 107-09.

B. Problems with the Plain View Doctrine in the Context of Digital Searches

The plain view doctrine operates as one of several exceptions to the warrant requirement.[94] Under the plain view doctrine, investigators may seize incriminating evidence without a warrant if they encounter the evidence in plain view during lawful observation of the area.[95] *Horton v. California*[96] established three requirements that investigators must meet before lawfully seizing evidence in plain view. First, the investigator must have lawful authority to be in the position from which he had occasion to observe the evidence. Second, the evidence must be in plain view. Third, the incriminating character of the evidence must be "immediately apparent"—the plain view doctrine does not authorize further investigation to determine the evidentiary value of the evidence.[97] A number of courts have expanded the plain view doctrine to encompass "plain touch,"[98] "plain smell,"[99] and "plain hearing,"[100] corollaries.

The plain view doctrine applies easily to items that appear incriminating at first glance, such as drugs or guns, and some documents such as fake ID's, gambling records, and documents

---

[94] *See Investigations and Police Practices*, *supra* note 24, at 44 ("[C]ertain kinds of searches and seizures are valid as exceptions to the probable cause and warrant requirements, including investigatory stops, investigatory detentions of property, warrantless arrests, searches incident to a valid arrest, seizures of items in plain view, searches and seizures justified by exigent circumstances, consent searches, searches of vehicles, searches of containers, inventory searches, border searches, searches at sea, administrative searches, and searches in which the special needs of law enforcement make the probable cause and warrant requirements impracticable.").

[95] *See id.* at 74-75.

[96] 496 U.S. 128 (1990).

[97] *See id.* at 136-37; Arizona v. Hicks, 480 U.S. 321, 326-28 (1987) (noting that allowing further investigation beyond a cursory examination would "especially erode the plurality's warning in *Coolidge* that the 'plain view' doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges'" (quoting Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971)).

[98] *See* Minnesota v. Dickerson, 508 U.S. 366, 375 (1993) ("We think that [the plain view] doctrine has an obvious application by analogy to cases in which an officer discovers contraband through the sense of touch during an otherwise lawful search.").

[99] *See, e.g.*, United States v. Staula, 80 F.3d 596, 602 (1st Cir. 1996) ("[O]lfactory evidence furnishes the officer with probable cause to conduct a search of the confined area.").

[100] *See* United States v. Ceballos, 385 F.3d 1120, 1124 (7th Cir. 2004) (citing a "'plain hearing' exception to the search warrant requirement"); United States v. Fisch, 474 F.2d 1071, 1077 (9th Cir. 1973) (likening the plain view doctrine to a situation in which officers eavesdropped on suspects from their rented hotel room).

linking co-defendants.[101] It is less clear that incriminating evidence is in "plain view" when discovered as investigators examine intermingled documents in an attempt to separate responsive from non-responsive items. Difficult cases are easy to conceive. For example, imagine investigators have obtained a warrant to search a suspect's belongings for evidence of bank fraud. The warrant allows the investigators to scan each letter in a stack of letters to determine which, if any, contain evidence of bank fraud. An investigator reads the first paragraph of one letter, but cannot determine whether the letter is relevant, so he continues reading. In the middle of the second paragraph, he reads the statement, "I hid the cocaine in the cookie jar. Just ask Jim for the 'fresh baked goods' and leave the money with him." Assuming the remainder of the letter contains nothing relevant to bank fraud, its contents clearly fall outside the scope of the investigators' warrant. The investigators would like to use the evidence against the suspect in a subsequent drug trial. Given that the investigator had to read the first two paragraphs of the letter before discovering any evidence of drug trafficking, was the evidence really "immediately apparent" as required by the plain view doctrine?

Courts answer this question with respect to physical evidence by allowing a "brief perusal of documents in plain view in order to determine whether probable cause exists for their seizure under the warrant. If in the course of that perusal, their otherwise incriminating character becomes obvious, they may be seized."[102] Courts have generally permitted investigators to seize documents discovered in "plain view," accepting without much discussion that the investigators must conduct some degree of perusal to ascertain the relevance of the documents.[103] Investigators need not be "absolutely certain" that documents or other items discovered in plain view constitute evidence of the crime at hand,[104] and may "test their belief by proceeding with a limited inspection of the 'incriminating object.'" However, "perusal must cease at the point at which the warrant's inapplicability to each document is clear."[105]

---

[101] *See* Regensburger, *supra* note 3, at 1197.
[102] United States v. Heldt, 668 F.2d 1238, 1267 (D.C. Cir. 1981).
[103] *See* United States v. Ochs, 595 F.2d 1247, 1258 n.8 (2d Cir. 1979).
[104] *See, e.g.*, *id.* at 1258; United States v. Duckett, 583 F.2d 1309, 1314 (5th Cir. 1978) ("There is no rule of law which requires an officer to know with absolute certainty that all elements of a putative crime have been completed when he seizes an article which reasonably appears to be incriminating evidence."); United States v. Pugh, 566 F.2d 626, 627 (8th Cir. 1977); Mapp v. Warden, 531 F.2d 1167 (2d Cir. 1976); United States v. Smollar, 357 F. Supp. 628, 632 (S.D.N.Y. 1972) ("The plain view exception would be worthless if officers had to be 'absolutely certain' that what they saw was seizable").
[105] *Heldt*, 668 F.2d at 1267.

Courts have begun to apply this reasoning to digital data. Most cases involve application of the plain view doctrine to digital evidence that is incriminating on its face. The visual nature of child pornography makes it the most common type of evidence seized under the plain view doctrine during searches of digital property.[106] However, courts have suggested the plain view doctrine would apply to admit evidence that is not graphic in nature if found after a brief scan of data on a computer screen.[107]

This practice arguably transforms all digital search warrants into general warrants and raises the question: what if investigators are always in a position from which they can view everything on the computer screen? If courts authorize investigators to scan every piece of data on a hard drive to determine its relevancy, then investigators will *always* be in a lawful position from which to view evidence of unrelated crimes. The warrant's scope would lose all relevance because any evidence not covered by the warrant could be seized under the plain view doctrine. Digital searches would become fishing expeditions.[108] The majority joining Chief Judge Kozinski's ruling in *CDT* must have recognized this danger. The majority took the drastic view that to "avoid this illogical result, the government should, in future warrant applications, forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data."[109]

The plain view doctrine, however, serves an important function in both physical and digital contexts. If police come upon out-of-scope evidence during the course of an otherwise lawful search it could be "dangerous—to the evidence or to the police

---

[106] *See, e.g.*, United States v. Wong, 334 F.3d 831 (9th Cir. 2003); Frasier v. State, 794 N.E.2d 449, 465-66 (Ind. Ct. App. 2003) (applying the plain view doctrine when police searching a suspect's computer for evidence of marijuana happened upon child pornography).

[107] *See, e.g.*, United States v. Gray, 78 F. Supp. 2d 524, 531 n.11 (E.D. Va. 1999) ("Agent Ehuan could have continued his systematic search of defendant's computer files pursuant to the first search warrant, and, as long as he was searching for the items listed in the warrant, any child pornography discovered in the course of that search could have been seized under the 'plain view' doctrine."); State v. Mays, 829 N.E.2d 773, 779 (Ohio Ct. App. 2005) (holding that an officer's observation of the words "he will die today" on defendant's computer screen while lawfully present in defendant's home fell within the ambit of the plain view doctrine); Commonwealth v. Hinds, 768 N.E.2d 1067 (Mass. 2002) (holding that the officer "was not obligated to disregard files listed in plain view on the 'Chuck' directory whose titles suggested contents that were contraband").

[108] *See* Chang, *supra* note 49 (arguing for the abolition of the plain view doctrine in order to prevent general searches of digital property).

[109] *CDT II*, 579 F.3d 989, 998 (9th Cir. 2009).

themselves—to require them to ignore it."[110] A search for evidence of tax evasion might yield evidence that the suspects plans to kill his wife for insurance money. Police may need to seize out-of-scope evidence to prevent a heinous crime.

Requiring investigators to forswear reliance on the plain view doctrine in the Ninth Circuit has already had deleterious effects on law enforcement efforts to uphold the law and protect vulnerable individuals. In the Western District of Washington,

> federal agents received information from their counterparts in San Diego that two individuals had filmed themselves raping a four-year-old girl and traded the images via the internet. The agents did not obtain a warrant to search the suspects' computers, however, because of concerns that any evidence discovered about other potential victims could not be disclosed by the filter team.[111]

Fortunately, federal agents could refer the case to state authorities, who are not bound by the restrictions outlined in *CDT*. This example stresses that a blanket elimination of the plain view doctrine could create more threats to society than it prevents.

Eliminating the plain view doctrine may have less dramatic, but equally serious effects. If investigators could not seize out-of-scope evidence in plain view, investigators might "result in the loss of highly probative evidence about the very crime under investigation."[112] This could occur, for example, "when a warrant contains a date restriction but the resulting search turns up evidence that the crime began or continued after officers previously had reason to believe."[113] Investigators have a legitimate interest in pursuing out-of-scope evidence to uphold society's laws and thwart criminal activity, when possible.

C. Plain View Problems for Privileged Data and Third Parties

The view-all-use-all practices that result from the direct application of traditional rules to digital searches also raise hackles where privileged documents and third parties are concerned.[114]

---

[110] Coolidge v. New Hampshire, 403 U.S. 443, 468 (1971).
[111] Brief for the United States in Support of Rehearing En Banc by the Full Court, *supra* note 1, at 6-7.
[112] *Id.* at 14.
[113] *Id.*
[114] *See* United States v. Abbell, 963 F. Supp. 1178, 1198-99 (S.D. Fla. 1997) (allowing perusal of all files, and approving of the government's use of a taint team to protect privileged materials); State v. Viatical Servs., Inc., 741 So. 2d

Investigators may peruse all intermingled data to ascertain its relevancy, and in doing so may examine privileged documents or third party information regardless of whether it falls within the scope of the warrant. Incriminating information in "plain view" may be seized and used to charge third parties previously considered innocent.[115]

In order to protect third party privacy, the Attorney General has issued rules requiring federal officers to pursue relevant evidence in the hands of disinterested third parties by issuing subpoenas rather than warrants.[116] Pursuant to these rules, federal officers may only seek a warrant to obtain materials from a disinterested third party when it appears that "the use of a subpoena, summons, request, or other less intrusive alternative means of obtaining the materials would substantially jeopardize the availability or usefulness of the materials sought."[117] This policy sounds promising, but third parties receive little protection once the government decides to pursue evidence with a warrant because "failure to comply with this policy 'may not be litigated, and a court may not entertain such an issue as the basis for the suppression or exclusion of evidence.'"[118]

560, 563 (Fla. Dist. Ct. App. 1999) ("[T]he court must fashion a remedy to protect the privacy rights of innocent third parties while still allowing the state to proceed with its criminal investigation."); Chang, *supra* note 49, at 58 (discussing privilege as a possible limitation on the plain view doctrine); Regensburger, *supra* note 3, at 1153, 1170-72 (expressing concern that a third party will get "caught up in the government's dragnet," and analyzing the use of taint teams to prevent prosecutors from accessing privileged data).

[115] *See, e.g.*, *CDT II*, 579 F.3d 989, 1005 (9th Cir. 2009) (The directory searched by the government "contained a huge number of drug testing records, not only of the ten players for whom the government had probable cause but hundreds of other professional baseball players, thirteen other sports organizations, three unrelated sporting competitions, and a non-sports business entity—thousands of files in all, reflecting the test results of an unknown number of people, most having no relationship to professional baseball except that they had the bad luck of having their test results stored on the same computer as the baseball players.").

[116] *See* DOJ GUIDELINES, *supra* note 67, at 111 (citing 28 C.F.R. § 59.4(a)(1) (2009)).

[117] 28 C.F.R. § 59.4(a)(1).

[118] *See* DOJ GUIDELINES, *supra* note 67, at 111 (quoting 28 C.F.R. § 59.5(b)). Congress has enacted statutory schemes to offer a higher degree of protection to third party internet service providers, and third party publishers, journalists, authors, or other individuals where a search of his or her possessions may implicate First Amendment concerns. *See id.* at 101-09, 112-33. The Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712 (2006), regulates government access to electronic records stored by third-party service providers. *See* DOJ GUIDELINES, *supra* note 67, at 112. The Privacy Protection Act (PPA), 42 U.S.C. § 2000aa, governs federal computer searches when agents have reason to believe they will encounter materials relating to freedom of expression. *See* DOJ GUIDELINES, *supra* note 67, at 101. However, both acts

Where the government has obtained a warrant to search digital media containing privileged information, the DOJ Guidelines offer strategies for reviewing privileged computer files:

> First, the court itself may review the files *in camera*. Second, the presiding judge may appoint a neutral third party known as a "special master" to the task of reviewing the files. Third, a team of prosecutors or agents who are not working on the case may form a "filter team" or "taint team" to help execute the search and review the files afterwards. The filter team sets up a so-called "ethical wall" between the evidence and the prosecution team, permitting only unprivileged files to pass over the wall.[119]

To protect privileged information, the Department of Justice prefers to segregate data using taint teams composed of attorneys or agents who are not members of the prosecution team. However, the use of taint teams is not mandatory, nor do all jurisdictions condone the use of taint teams.[120] Computers belonging to medical and legal professionals often contain a spectrum of confidential or privileged material such as client or patient communications, medical records, or attorney work product.[121] "[T]he use of computerized equipment for the storage and exchange of sensitive confidential information has become commonplace."[122] If a comprehensive search requires investigators to review *every* file, it seems that privileged documents must suffer some type of scrutiny. The fact that the scrutinizing eyes do not belong directly to the

---

harbor loopholes with respect to warrants. If the government obtains a warrant to search data held by an internet service provider, the SCA allows investigating agents to obtain everything associated with an account, and does not require agents to notify customers or subscribers that the agents have obtained information from the provider. *See* 18 U.S.C. § 2703. The PPA purports to require the use of a subpoena to obtain materials relating to freedom of expression, but "[t]he PPA does not apply in a search for or seizure of 'documentary materials' as defined by § 2000aa-7(a), if a subpoena has proven inadequate or there is reason to believe that a subpoena would not result in the production of the materials." DOJ GUIDELINES, *supra* note 67, at 104; *see* 42 U.S.C. § 2000aa(b)(3)-(4).

[119] *See* DOJ GUIDELINES, *supra* note 67, at 110. The "ethical wall" is also referred to as a "Chinese wall." *See In re* Search Warrant for Law Offices, 153 F.R.D. 55, 57 (S.D.N.Y. 1994).

[120] *See* Chang, *supra* note 49, at 58.

[121] *See id.*; United States v. SDI Future Health, Inc., 464 F. Supp. 2d 1027, 1037 (D. Nev. 2006).

[122] Black v. United States, 172 F.R.D. 511, 514 (S.D. Fla. 1997).

prosecution team may offer little comfort.[123] Courts have vacillated on whether in camera review, review by special master, or review by a taint team most effectively protects privileged digital materials without unduly hampering the government's investigation.

The court in *United States v. SDI Future Health, Inc.*[124] noted, "[f]ederal courts have taken a skeptical view of the Government's use of 'taint teams' as an appropriate method for determining whether seized or subpoenaed records are protected by the attorney-client privilege."[125] The court in *In re Grand Jury Subpoenas*[126] cautioned that taint teams might leak confidential information. The government has an interest in uncovering every scrap of evidence to further the investigation, and while some leaks occur through human error, human nature may lead taint-team attorneys to violate their ethical obligations.[127] "[T]he government's fox is left in charge of the appellants' henhouse, and may err by neglect or malice, as well as by honest differences of opinion."[128]

Courts have also noted the drawbacks to using a special master or neutral magistrate to separate privileged materials. In *Black v. United States*[129] the court pointed out that using special masters can incur high costs and fees, and they may take a prohibitive amount of time to review the contested materials. In one instance, appointment of a special master delayed a criminal trial for two and a half years.[130] Such a delay could "effectively deprive the Government of any access to any of the seized information."[131] A magistrate or special master might have many duties that conflict with the task of reviewing millions of computer

---

[123] *See id.* at 516 ("The Plaintiffs have a serious concern that disclosure to taint team prosecutors would not protect the confidentiality and privacy rights they here assert.").
[124] *SDI Future Health*, 464 F. Supp. 2d 1027.
[125] *Id.* at 1037.
[126] *In re* Grand Jury Subpoenas, 454 F.3d 511 (6th Cir. 2006).
[127] *Id.* at 523.
[128] *Id.*; *see also* United States v. Abbell, 914 F. Supp. 519 (S.D. Fla. 1995) (deciding that privileged materials should be reviewed by a special master despite the government's appointment of a taint team); *In re* Search Warrant for Law Offices, 153 F.R.D. 55, 59 (S.D.N.Y. 1994) ("[T]his Court notes that reliance on the implementation of a Chinese Wall, especially in the context of a criminal prosecution, is highly questionable, and should be discouraged."); *cf.* United States v. Neill, 952 F. Supp. 834, 841 n.14 (D.D.C. 1997) (criticizing the use of taint teams, but noting that "[h]owever unwise this policy decision may be, absent a showing of harm, it does not offend the Constitution").
[129] Black v. United States, 172 F.R.D. 511, 514 (S.D. Fla. 1997).
[130] *Id.* at 514 n.4, 516 (citing *Abbell*, 914 F. Supp. 519).
[131] *Id.* at 516.

files, whereas a taint team specifically designated to segregate privileged materials could do so in a timely manner.[132]

The court in the case of *In re 5444 Westheimer Rd. Suite 1570*[133] determined that the lengthy amount of time a special master or magistrate judge would require to review privileged materials outweighed the protection this method might afford. Instead, the court allowed the government to proceed with taint team review.[134] The court noted that the government's taint team procedure did not prejudice defendants because the use of a taint team gave defendants the opportunity to challenge the taint team's privilege determinations in front of the court. The court would then resolve any privilege disputes before the taint team could disclose materials classified as unprivileged to the prosecution team.[135] In contrast, a neutral magistrate or special master may not offer the defendants the same opportunity to challenge privilege determinations.[136]

The controversy incited by the government's seizure of third party drug records in *CDT* demonstrates how computers' massive storage capacities have magnified the problem. The fact that the targeted computers contained vast quantities of third party data allowed the government to seize "thousands of medical records and test results involving every single Major League Baseball player," and "thousands of other medical records for individuals in thirteen other major sports organizations, three unaffiliated business entities, and three sports competitions," despite the fact that the government only had a search warrant for a small handful of MLB players, and none of the other individuals were the subject of any criminal inquiry.[137] This result highlights the distinction between physical and digital searches: "people now have personal data that are stored with that of innumerable strangers. Seizure of, for example, Google's email servers to look

[132] *See* DOJ GUIDELINES, *supra* note 67, at 110; *Black*, 172 F.R.D. at 516 n.8.
[133] No. H-06-238, 2006 U.S. Dist. LEXIS 48850 (S.D. Tex. July 6, 2006).
[134] *Id.* at *9.
[135] *Id.* at *9, *11 n.5.
[136] See *United States v. Grant*, which approved the use of a taint team. No. 04 CR 207, 2004 U.S. Dist. LEXIS 9462 (S.D.N.Y. May 25, 2004). The court noted that "after the initial privilege determination is made by the special master or judicial officer, the Government would not have the opportunity to brief or argue the ruling aided by the contents of the documents. Without the benefit of such a review, the privilege team would likely be unable to argue, for example, that no attorney-client privilege attached to the communication because of the crime-fraud exception, or that a document should be available for use at trial, regardless of work-product contents, because of necessity and unavailability by other means." *Id.* at *4-5.
[137] *CDT I*, 513 F.3d 1085, 1116-17 (9th Cir. 2008) (Thomas, J., dissenting).

for a few incriminating messages could jeopardize the privacy of millions."[138]

Investigators searching a suspect's home or office could rarely net such an abundance of evidence. The court in *Black v. United States* might have been speaking to privileged documents when it called for "a re-thinking of some of the traditional approaches Courts have made in years gone by,"[139] but it was not alone in seeking a new approach to regulating search and seizure of digital media.

D. The Carey-*Winick "Special Approach" to Digital Searches*

Both scholars and courts have referenced the enormous storage capabilities of digital media to justify the viewpoint that digital searches cannot and should not be compared to physical-world searches.[140] In his influential article, Ralph Winick emphasized that the "very quantity and variety of information" on a computer "increases the likelihood that highly personal information, irrelevant to the subject of the lawful investigation, will also be searched or seized."[141] Winick recognized the threat created by allowing investigators to examine intermingled documents, and argued that application of traditional rules to searches of digital media "allows officers to gain a window into all aspects of a suspect's life."[142] Instead, Winick advocated for applying the "intermingled-document" approach outlined in *United States v. Tamura*[143] to digital media searches. In his proposal for a new approach, Winick discredited the theory that comprehensive computer searches require investigators to peruse every file on the hard drive. Instead of conducting a full review of digital files, he proposed investigators limit their search of the data by file type, or use key word searches to locate relevant files. He opined that government agents should seal any intermingled files, and submit specific search protocol to a neutral magistrate for approval before proceeding with review of those files.[144]

---

[138] *CDT II*, 579 F.3d 989, 1005 (9th Cir. 2009).
[139] 172 F.R.D. 511, 514 (S.D. Fla. 1997).
[140] *See, e.g.*, United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999); Chang, *supra* note 49, at 35-36; Kerr, *supra* note 47, at 301-03.
[141] Winick, *supra* note 25, at 105.
[142] *Id.* at 111.
[143] 694 F.2d 591, 595-96 (9th Cir. 1982) ("In the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, we suggest that the Government and law enforcement officials generally can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search . . . .").
[144] Winick, *supra* note 25, at 107-09.

The Tenth Circuit has been the strongest proponent of using a "special approach" for digital media searches.[145] The court in *United States v. Carey*[146] became the first to adopt Winick's "special approach" explicitly.[147] *Carey* expanded upon Winick's "special approach" by suggesting that investigators should obtain a second warrant before seizing out-of-scope evidence discovered in plain view.[148]

While some have approved of the "*Carey*-Winick" approach,[149] others have been quick to point out its flaws. Courts rejecting the approach have continued to allow investigators to peruse all intermingled documents because requiring search methods would be too restrictive.[150] Scholars also questioned the wisdom of limiting the extent to which investigators could open and view files, citing the argument that criminals may disguise evidence in ways investigators may not be able to predict.[151]

---

[145] Regensburger, *supra* note 3, at 1157.

[146] United States v. Carey, 172 F.3d 1268 (10th Cir. 1999).

[147] *See id.* at 1275-76; Trepel, *supra* note 15, at 130.

[148] *Carey*, 172 F.3d at 1271, 1276. DOJ guidelines note that when agents discover evidence in plain view that is not identified by the warrant, it would be a "safe practice" to obtain a second warrant. However, this practice is not mandatory. *See* DOJ GUIDELINES, *supra* note 67, at 90.

[149] The term "*Carey*-Winick" was coined by David Ziff in a 2005 piece criticizing the approach's limitations. *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, 842 & n.4 (2005). For examples of courts approving of the *Carey*-Winick limitations, see United States v. Riccardi, 405 F.3d 852, 862 (10th Cir. 2005); United States v. Walser, 275 F.3d 981, 986-87 (10th Cir. 2001); Trulock v. Freeh, 275 F.3d 391, 411 n.2 (4th Cir. 2001); and People v. Carratu, 755 N.Y.S.2d 800 (N.Y. Sup. Ct. 2003).

[150] *See* United States v. Adjani, 452 F.3d 1140, 1149-50 (9th Cir. 2006); United States v. Hill, 322 F. Supp. 2d 1081, 1090-91 (C.D. Cal. 2004) ("Forcing police to limit their searches to files that the suspect has labeled in a particular way would be much like saying police may not seize a plastic bag containing a powdery white substance if it is labeled 'flour' or 'talcum powder.' There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it."); United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999); Commonwealth v. McDermott, 864 N.E.2d 471, 488-89 (Mass. 2007) (specifically declining to adopt the special approach outlined in *Carey*).

[151] *See* Clancy, *supra* note 68, at 207-08 ("[T]here are significant reasons to reject [*Carey*'s] position that a search be restricted by file names or file types. Professional investigators recognize that computer users attempt to conceal criminal evidence by storing it 'in random order with deceptive file names,' thus requiring a search of all the stored data to determine whether it is included in the warrant." (citation omitted)); Trepel, *supra* note 15, at 134 ("According to Kerr, the process required by the *Carey*-*Tamura* approach is flawed for the very practical reason that 'computer forensics is contingent, fact-bound, and quite unpredictable.' An investigator will not know beforehand which operating system is on the device to be searched, which software is on it, or whether the suspect attempted to hide or disguise any incriminating files." (footnote

Others have criticized the suggestion that a neutral magistrate should determine which files the government should access. When Winick first outlined his proposal, the idea of magistrate oversight was plausible: computers at that time only held 100 megabytes of data, the equivalent of 100,000 typed pages. Investigators could reasonably print the file directory for magistrate review. Modern computers, however, store considerably more information, and it would be prohibitively time consuming for lawyers to quibble in front of a magistrate over the contents of a huge volume of files.[152]

Finally, some have found fault with the use of a second warrant to pursue evidence discovered outside the scope of the original warrant. A second warrant may fail to protect privacy concerns implicated by the plain view doctrine because investigators will have already discovered the out-of-scope evidence without previous probable cause. Assume for the sake of argument that investigators should forswear reliance on the plain view doctrine when conducting digital searches. Under this rule, if investigators searching for evidence of bank fraud come across child pornography, they cannot seize it as evidence "in plain view," but they can apply for a second warrant to expand their search based on the image they have just discovered. The application will likely be granted since investigators now have concrete evidence of a possible second crime. For the purposes of the second warrant, it matters not whether the evidence fell within the scope of the first. Therefore, the second warrant procedure creates a loophole to the ban on seizing evidence in plain view by authorizing investigators to seize the same out-of-scope evidence without relying on the plain view doctrine.[153] According to critics, this "easy-to-meet" procedure is "functionally equivalent to the plain view doctrine."[154]

There has been no consensus amongst different factions as to how investigators should execute search warrants for digital media without violating the Fourth Amendment. This dissonance has led to conflicting rules and results, highlighting the dire need for lawmakers to issue guidance or regulation in this area.

IV. A STATUTORY SOLUTION

To effect a solution, federal and state legislatures should adopt a set of rules that augment the Fourth Amendment with

---

omitted)); *supra* Parts II.A, III.A (discussing the argument that investigators must peruse all files to circumvent attempts to conceal evidence).

[152] *See* Ziff, *supra* note 149, at 860-61.

[153] *See* Chang, *supra* note 49, at 48, 50.

[154] *Id.* at 50.

respect to search and seizure of digital media. For example, Rule 41 of the Federal Rules of Criminal Procedure currently governs search and seizure pursuant to a warrant for federal investigations.[155] This rule and corresponding state rules could be amended to incorporate specific sections pertaining to warrants for search and seizure of digital property. Legislative action offers several advantages over the solutions implemented by courts. Legislatures are not limited by stare decisis, and thus have more flexibility to design new rules.[156] While courts may stray from precedent when changed conditions and increased knowledge render existing rules unworkable,[157] a court's influence may extend only as far as its jurisdiction. Legislatures can promulgate rules that span jurisdictions, thus facilitating consistent practices.

An opinion issued by the Supreme Court could settle controversy across jurisdictions, but the Supreme Court may only address issues presented in the case before it. The Supreme Court will never hear a case presenting every nuanced issue raised by a digital media search. Legislatures, on the other hand, do not need to wait until a problem presents itself. Legislatures can also effect changes much more quickly than many courts across many jurisdictions.[158]

Additionally, legislatures may be more competent than courts to address the problem of digital media searches, because "it is difficult for judges to fashion lasting guidance when technologies are new and rapidly changing."[159] While legislatures receive information from a wide range of sources, including legislative hearings, advocacy groups, constituent and public input, national media, and special caucuses, judges receive information funneled through the briefs and oral arguments of two parties.[160] Legislative branches are better situated to gather information about the developing technologies that both complicate and facilitate digital searches.

A. With Privacy and Justice for All

To walk the line between privacy and justice, legislatures need to adopt rules for digital property searches that offer more protection than the traditional approach to search and seizure, but fewer restrictions than the "special approach" described by the

---

[155] FED. R. CRIM. P. 41.
[156] *See* Kerr, *supra* note 47, at 308.
[157] *See* Trepel, *supra* note 15, at 142.
[158] *Id.*; Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 868-70 (2004).
[159] Kerr, *supra* note 158, at 858.
[160] *Id.* at 875-76.

Carey-Winick doctrine. The following three subsections each describes a rule that legislatures should adopt to strike this balance. Legislatures should: 1) require narrow search protocols, but allow file-by-file searches where necessary; 2) require a second warrant for the seizure of ambiguous out-of-scope evidence, but allow investigators to seize contraband under the plain view doctrine; and 3) require a taint team to review privileged or third party files. The taint team should afford the defense the opportunity to challenge privileged determinations. The third subsection also recommends a procedure for the taint team to follow if it encounters evidence that incriminates a third party.

1. The Narrow Search Protocol Requirement

As explained in Section IV.A, the traditional approach to search and seizure in theory allows investigators to scan every file in search of evidence. Investigators need not follow a pre-specified protocol to examine digital records. In reality, however, investigators have neither the time nor the resources to scan every piece of data on a hard drive. Forensic investigators will use whatever methods they can to narrow the subset of data they must search in order to discover evidence that responds to the warrant.[161] Creating a rule that requires investigators to use reasonable methods to narrow their searches would serve the interests of both the Fourth Amendment and government investigators. Where less intrusive, more effective search methods exist, it would be unreasonable not to require investigators to employ those methods.[162]

Legislatures should therefore require forensic investigators to begin searching digital media with available forensic tools such as hashing programs, EnCase, FTK, or other tools on the market. Due to the rapid pace of technological development, it would not be wise for legislatures to require the use of specific tools. Such a rule would tie investigators to outdated programs upon the invention of new search technology.

A new rule requiring the use of these programs will assuage fears that investigators will examine *every* piece of data, because investigators will always conduct hashes and key word searches as an initial step. If these steps returned the sought-after evidence, the search should cease. This rule would not hinder searches because most investigators already use these programs to narrow the set of data to be searched.

If the warrant authorizes investigators to search for images, and hashes or key word searches cannot locate the images sought,

[161] Interview with Chris Beeson, *supra* note 66.
[162] *See* McLain, *supra* note 65, at 1097-98.

investigators may scan *all* digital images, but should not extend this file-by-file search to word documents or other file types. However, the rule should recognize that criminals might disguise evidence. If an investigator discovers a file with an altered extension, the investigator would have reason to believe the suspect attempted to conceal evidence. In this case, the investigator may open the altered file even if that file type would not normally contain evidence associated with the alleged crime.

Forensic tools will not flag misnamed files in all cases, therefore, legislatures should allow investigators to begin opening and scanning all files if, and only if, narrow search methods fail to produce results. Investigators should not be required to obtain permission from the court before expanding their search. Some might argue that such a permissive rule would encourage unscrupulous investigators to ignore the narrow search requirement. However, codification of the narrow search requirement will keep law enforcement in check; if a defendant challenges the legality of the search, the law should place the burden on investigators to prove to the court that they conducted a narrow search before proceeding with a more intrusive one. The above-described rules align with many restrictions described by the *Carey*-Winick doctrine, but also square with traditional doctrine by authorizing investigators to conduct a more comprehensive search where required.

2. The Plain View Doctrine and the Second Warrant Requirement

Requiring investigators to waive the plain view doctrine, as described in *CDT*, is a drastic and dangerous step. "A search of a computer for evidence of fraud, for example, could reveal evidence of a planned terrorist attack or a search aimed at drug trafficking could reveal evidence of an ongoing violent crime or sexual abuse."[163] Abolishing the plain view doctrine with respect to digital searches may create risks to society that outweigh those created by governmental intrusion into individual privacy.[164]

Furthermore, if legislatures pass laws that limit digital searches as described above in Subsection V.A.1, the plain view doctrine becomes less problematic. Investigators will no longer have the authority to search every file in all cases, which diffuses the threat of the general search. If investigators discover out-of-scope evidence during the course of their search under the new rule, investigators may pursue evidence under the plain view

[163] *See* Brief for the United States in Support of Rehearing En Banc by the Full Court, *supra* note 1, at 14.
[164] *See supra* Part III.B.

doctrine if that evidence clearly demonstrates criminal behavior. For example, a person cannot legally possess child pornography. Thus, if child pornography exists on a person's hard drive, a crime has occurred and investigators may seize this contraband under the plain view doctrine.

However, investigators should obtain a second warrant before seizing out-of-scope evidence if questions arise as to whether the evidence meets the "immediately incriminating" requirement of the plain view doctrine. In this scenario, the second warrant requirement will ensure that investigators indeed have probable cause to seize the potentially incriminating evidence. For example, suppose investigators searching for images for child pornography stumble upon an image of a letter that reads, "How much would it cost to hire a hit man to kill Joe and his family on Thursday night?" Either this statement could be evidence of murder for hire, or it could simply be exaggerated venting, or the exercise of a person's right to free speech under the First Amendment.[165] Requiring investigators to submit a second warrant application to a neutral magistrate will ensure that the government can legally admit this evidence at trial, and shields government agents from claims of misconduct.

In addition, a second warrant may authorize investigators to continue searching for evidence related to the second crime. Investigators could gather the evidence needed to bring charges quickly, which could prevent a dangerous person from committing an act of violence.

3. Protecting Third Parties and Privileged Documents

Searches of digital media containing privileged data, or data pertaining to third parties require special considerations.[166] Where investigators must issue a warrant to search computers containing either type of data, the case agents and forensic investigators should first narrow the set of data to be searched by using forensic tools and other reasonable limitations. If the in-scope evidence exists amongst privileged data or data pertaining to third parties, the most practical and protective measure would be to allow a taint team to review those materials. The taint team should be composed of disinterested forensic investigators, agents, and

[165] Interview with Chris Beeson, *supra* note 66 (explaining an example of out-of-scope evidence that does not necessarily point to illegal activity, and emphasizing THAT this evidence must be treated with "kid gloves," unlike evidence of child pornography, which is illegal in-and-of itself to possess).

[166] *See supra* Part III.C (discussing the threats posed by the plain view doctrine to third parties and privileged documents, and different methods courts endorse to mitigate these threats).

attorneys who would review privileged and third party materials to cull non-responsive items.

For cases involving privileged documents, the government should provide the defense with the opportunity to review any data categorized as unprivileged, and allow the defense to challenge that categorization in front of the court. *In re 5444 Westheimer Rd. Suite 1570*[167] approved of this procedure and noted that it did not prejudice the defendant because privilege disputes would be resolved by the court before the taint team could disclose materials to the prosecution team.[168] A neutral magistrate or special master would not offer the government the same opportunity to challenge privilege determinations. Additionally, use of a special master or neutral magistrate would strain government and judicial resources and slow the investigation, as described in Section IV.C.

Where an investigation involves examination of digital media containing the data of unrelated third parties, members of the prosecution team should not view the intermingled data. A disinterested individual or taint team should segregate the data and provide the prosecution team with information pertaining to the suspect. If the taint team discovers evidence that incriminates a third party, the taint team may disclose that information to the prosecution team if doing so will prevent harm to another person or entity. The taint team should consult a disinterested attorney to determine whether the team has an ethical obligation to disclose the evidence to prevent harm. It should be noted that the taint team would not be authorized to scan every privileged or third party file. Unless the narrower search failed, the taint team would be required to conduct a narrow search using forensic tools as described in Subsection IV.A.1. Additionally, if the taint team refers a piece of evidence that incriminates an unrelated third party to the prosecution team, the prosecution team must obtain a second warrant before pursing that evidence. The second warrant requirement would be waived if the evidence is contraband or clearly demonstrates that a crime has occurred. These safeguards deter unscrupulous conduct, and ensure that the prosecution team will not conduct an exploratory search of third party data in an effort to discover evidence with which to charge new crimes.

CONCLUSION

Digital media has become an integral part of the lives of many Americans, and advancements in technology will continue to blur the line between physical and digital worlds. As we import,

[167] *In re* 5444 Westheimer Rd. Suite 1570, No. H-06-238, 2006 U.S. Dist. LEXIS 48850 (S.D. Tex. July 6, 2006).
[168] *Id.* at *9, *11 n.5.

upload, or download more of our personal lives onto digital media, privacy stakes rise. Without clarity from legislatures, courts will continue to grapple over the application of the Fourth Amendment to digital media searches. Courts applying traditional Fourth Amendment principles risk eroding the relevancy of search warrants by allowing every warrant authorize an exploratory search. Courts crafting new guidelines risk tying the hands of investigators and hopelessly frustrating the legitimate purposes of law enforcement. In order to formulate sound rules for governing the search and seizure of digital property, legislatures must strike a balance between these competing factions. To strike this balance, legislatures should:

> 1) Require narrow search protocols, but allow file-by-file searches where necessary;
> 2) Require a second warrant for the seizure of out-of-scope evidence that does not immediately demonstrate that a crime has occurred. Investigators may seize contraband without a second warrant under the plain view doctrine; and
> 3) Require a taint team to review privileged or third party files. The taint team should afford the defense the opportunity to challenged privileged determinations. If the taint team encounters evidence incriminating a third party it should consult a disinterested attorney to determine whether the team should disclose the evidence.

Legislatures adopting this approach will provide courts with the clarity needed to enforce privacy protections while preserving the legitimate goals of law enforcement.