DIGITAL SEARCHES, GENERAL WARRANTS, AND THE CASE FOR THE COURTS

SAMANTHA TREPEL

10 YALE J. L. & TECH. 120 (2007)

ABSTRACT

Translating Fourth Amendment rules designed to regulate searches and seizures of physical property into rules that regulate digital investigations raises numerous questions. This Note seeks to address one narrow subset of the issues digital evidence collection presents: the execution of computer searches conducted pursuant to warrants, and the threat of general searches—searches effectively unlimited in scope by the warrant—they raise. Both courts and academics have called attention to this risk of general searches, and many have proposed solutions that seek to preserve the Fourth Amendment's traditional balance between individual privacy and government need. However, a single workable rule remains elusive. While the proposed solutions do not provide answers in every context, many of the rules do have merit in specific factual situations. At least while digital technology continues to change at a rapid pace, lower courts should be encouraged to develop a toolbox of rules to address the problem. Reviewing courts should take the lead, exploring the contours and boundaries of the problem and developing different tools in various factual contexts through the process of common law decision-making.

TABLE OF CONTENTS

I. INTRODUCTION 122
II. THE DEVELOPMENT OF FOURTH AMENDMENT JURISPRUDENCE . 123
III. GENERAL SEARCHES: THE PROBLEM WITH DIGITAL INVESTIGATIONS 126
IV. AN ELUSIVE SOLUTION 133
V. THE CASE FOR THE COURTS 139
VI. CONCLUSION 150

I. INTRODUCTION

Over the past several decades, computers have increasingly become an unavoidable part of everyday life. Since 1984, the number of U.S. households with a computer has grown more than eight-fold to sixty-six percent of all homes.[1] Over the last ten to fifteen years, courts and legal academics have been responding to this trend with increasing regularity, struggling to apply Fourth Amendment jurisprudence to the new contexts presented by these omnipresent tools.[2]

Translating Fourth Amendment rules designed to regulate searches and seizures of physical property into rules that regulate digital investigations raises numerous questions.[3] This Note seeks to address one narrow subset of the issues digital evidence collection presents: the execution of computer searches conducted pursuant to warrants, and the threat of general searches—searches effectively unlimited in scope by the warrant—they raise. Both courts and academics have called attention to this risk of general searches, and many have proposed solutions that seek to preserve the Fourth Amendment's traditional balance between individual privacy and government need. However, a single workable rule remains elusive. While the proposed solutions do not provide answers in every context, many of the rules do have merit in specific factual situations. At least while digital technology continues to change at a rapid pace, lower courts should be encouraged to develop a toolbox of rules to address the problem. Reviewing courts should take the lead, exploring the contours and boundaries of the problem and developing different tools in various factual contexts through the process of common law decision-making.

---

[1] U.S. Census Bureau, *Home Computers and Internet Use in the United States: August 2000*, 1-2 (2001), www.census.gov/prod/2001pubs/p23-207.pdf; *see also* U.S. Government Accountability Office, Telecommunications Report, *Broadband Deployment Is Extensive Throughout the United States, but It Is Difficult to Assess the Extent of Deployment Gaps in Rural Areas*, GAO-06-426, 11 (2006), *available at* http://www.gao.gov/.

[2] Orin S. Kerr is among the most prolific of these academics, and has recently published a number of articles on related topics. *See, e.g.*, Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 280 (2005) (noting that courts have just begun to interpret the Fourth Amendment differently in computer cases); *see also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 533 n.2 (2005) (collecting cases demonstrating courts' contradictory holdings relating to computer searches).

[3] *See*, *e.g.*, Kerr, *Searches and Seizures*, *supra* note 2, at 533-34.

II. THE DEVELOPMENT OF FOURTH AMENDMENT JURISPRUDENCE

In enacting the Fourth Amendment, former colonists were reacting to the outrages and abuses they had experienced under the British in the form of general warrants and writs of assistance. General warrants permitted searches and seizures without requiring individualized suspicion or describing the persons or items to be seized.[4] Such warrants were frequently issued to suppress political dissent both in England and in the American colonies; they authorized searches and seizures of all "trunks, studies, cabinets, and other repositories of papers" for evidence of seditious libel.[5] As Crown officials issued the warrants ex parte and as they had the effect of immunizing the officers who executed them against civil trespass suits,[6] general warrants were especially threatening to the colonists. The 1763 English case *Wilkes v. Wood*,[7] perhaps the most famous case in late eighteenth century America, "was the paradigm search and seizure case for Americans"[8] and likely influenced the drafting of the Fourth Amendment.[9] In that case, Secretary of State Lord Halifax attempted to enforce the seditious libel laws against John Wilkes, a critic of King George III and an outspoken member of the House of Commons, by issuing a general warrant against him.[10] Wilkes sued, the general warrant was declared null and void, and a civil jury awarded Wilkes £4000 in punitive damages.[11] Reacting in part to this famous case, the Framers imposed strict limits on the scope of warrants.[12]

Writs of assistance—specialized forms of general warrants—authorized British customs officers to enter houses and shops without

---

[4] ANDREW E. TASLITZ, RECONSTRUCTING THE FOURTH AMENDMENT: A HISTORY OF SEARCH AND SEIZURE, 1789-1868, 17 (2006).

[5] NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 31 (1937).

[6] Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 771-72 (1994).

[7] 19 Howell's State Trials 1153 (C.P. 1763), 98 Eng. Rep. 489.

[8] Amar, s*upra* note 6, at 772 (emphasis omitted).

[9] AKHIL REED AMAR, THE BILL OF RIGHTS: CREATION AND RECONSTRUCTION 65-66 (1998).

[10] *Id.* at 67; Amar, *supra* note 6, at 772; Akhil Reed Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, 30 SUFFOLK U. L. REV. 53, 65 (1996).

[11] Amar, *supra* note 6, at 781; Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, *supra* note 10, at 65.

[12] AMAR, *supra* note 9, at 73.

probable cause or individualized suspicion in search of untaxed goods such as tea and sugar. The writs additionally authorized officials to commandeer peace officers or citizens to assist with the execution of the warrant.[13] While writs of assistance did not immunize officials who failed to discover contraband in the same way general warrants did,[14] enforcement of the writs still generated resentment among the colonists. This eventually erupted into violent opposition in the form of the Stamp Act riots of 1761.[15]

The Framers of the Bill of Rights designed the Fourth Amendment to assuage fears that the new American government would have similar powers.[16] The Amendment prohibited general warrants by mandating a demonstration of probable cause and by requiring particularity—the limitation that the warrant "particularly describ[e] the place to be searched, and the persons or things to be seized."[17] The Amendment additionally required that every search and seizure be "reasonable."[18]

With the Supreme Court's interpretative guidance, most notably since the Warren Court era, the Fourth Amendment has offered substantive protection against unreasonable governmental searches and seizures and general warrants. The Court's first major step in making the Fourth Amendment's protections broadly felt was to apply them to the states through the incorporation doctrine in *Wolf v. Colorado*.[19] Then, in *Mapp v. Ohio*, the Warren Court applied the Fourth Amendment's existing enforcement mechanism, the exclusionary rule, to the states as well.[20] Around this time the Court also shifted its understanding of the boundaries of the Fourth Amendment's protections. Previously, the Fourth Amendment had only extended its protection to physical trespass, but in *Katz v. United States* the Court declared that

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.

---

[13] Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, *supra* note 10, at 77-78.

[14] *Id.* at 79-80.

[15] TASLITZ, *supra* note 4, at 26.

[16] LASSON, *supra* note 5, at 99-105.

[17] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, 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.").

[18] *Id*.

[19] 338 U.S. 25 (1949).

[20] 367 U.S. 643 (1961).

> But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[21]

In *Katz*, the Court held that electronic surveillance of a phone conversation made in a closed telephone booth required a warrant. With *Katz*, the Court adopted an approach that considered whether a person "exhibited an actual (subjective) expectation of privacy" and whether that expectation is "one that society is prepared to recognize as 'reasonable'" in order to determine the applicability of the Amendment.[22] This extended the protections of the Fourth Amendment beyond instances involving trespasses to physical boundaries, and indicated a willingness of the Court to adapt its application of the Constitution to the "mischief" born of "[t]he progress of science."[23]

The Court also developed various exceptions to and elaborations on these Fourth Amendment protections. The two that have become especially relevant to computer searches are the plain view doctrine and the closed container rule. The plain view doctrine, an exception to the warrant requirement, permits officers to seize items not described with particularity in a warrant if the officer is lawfully in the location where the evidence is seized, the object itself is in plain view, and its incriminating nature is "immediately apparent."[24] Thus it applies broadly, justifying seizures even where there is no underlying warrant or search. The closed container rule cuts in the other direction. Courts limit the scope of a search, preventing it from becoming impermissibly overbroad, by permitting a search only of those closed containers that could reasonably hold items described in the warrant.[25] Courts have struggled over how to apply both rules to computer

---

[21] 389 U.S. 347, 351-52 (1967) (citations omitted).

[22] *Id.* at 360-61 (Harlan, J., concurring); *see also* Daniel J. Solove, *The Coexistence of Privacy and Security: Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 749-51 (2005) (listing the extension of the Fourth Amendment's jurisdictional reach, the application of the exclusionary rule to the states, and the expansion of the Amendment's applicability beyond physical trespass as the factors that effectuated the Fourth Amendment's rise to prominence in the regulation of criminal investigations).

[23] Olmstead v. United States, 277 U.S. 438, 473-74 (1928) (Brandeis, J., dissenting).

[24] Horton v. California, 496 U.S. 128, 136-37 (1990).

[25] United States v. Ross, 456 U.S. 798, 822-24 (1982).

searches, and have come to widely varying answers, leading to similarly divergent results.[26]

III. GENERAL SEARCHES: THE PROBLEM WITH DIGITAL INVESTIGATIONS

Computers present a special problem to Fourth Amendment jurisprudence: courts are unsure how to conceptualize them in relation to existing Fourth Amendment rules. In the context of digital evidence collection, seemingly intuitive answers to these questions "often lead to astonishing results" that "permit extraordinarily invasive government powers to go unregulated in some contexts."[27] Some courts have struggled to analogize computers to closed containers. Under this approach, the physical computer is a container,[28] and all electronic data stored therein are fairly searchable if agents have an otherwise valid warrant to search for any single document that might reasonably be stored electronically. When an investigator accesses the computer, she is opening a container, and exposing its contents to plain view. Other courts have instead viewed individual electronic files as closed containers, theorizing that because agents must open each file to search its contents, a search of file names in a computer directory does not place the files' contents in plain view.[29] Under this theory, only the name of the file itself is in plain view when an investigator begins a computer search.

The scope of warrants authorizing computer searches has engendered similarly contested analogies. Both defendants and the government have invoked comparisons of computers to file cabinets in challenging or defending against an overbroad search or seizure.[30] Under traditional Fourth Amendment jurisprudence, courts have authorized the search, and

---

[26] *Compare* People v. Gall, 30 P.3d 145,153-54 (Colo. 2001) (equating computers to containers and permitting search of them when "writings" were among other items enumerated in a search warrant) *with* United States v. Walser, 275 F.3d 981 (10th Cir. 2001) (rejecting analogy comparing computer equipment to storage containers for physical documents or objects, such as file cabinets and dressers, because "computers that are able to hold the equivalent of a library's worth of information[] go beyond the established categories of constitutional doctrine").

[27] Kerr, *supra* note 2, at 280.

[28] United States v. Runyan, 275 F.3d 449, 464 (5th Cir. 2001).

[29] United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999).

[30] *Id.* at 1274-75 (rejecting government's comparison of a computer to a file cabinet, which the government argued would have made a search of the contents of the entire computer permissible); *see also In re* Subpoena Duces Tecum Dated November 15, 1993, 846 F. Supp. 11 (S.D.N.Y. 1994) (quashing a subpoena for over-breadth when it demanded a corporation provide the investigating grand jury with the central processing unit of computers used by various officers and employees of the corporation).

sometimes the removal, of entire file cabinets during searches, though "wholesale removal" is generally not condoned.[31] The government has used this jurisprudence to argue that agents have the authority to search the entire contents of a computer, or to seize computers and other electronic storage equipment for later off-site searches.[32] Others have used the analogy to limit the reach of the government, arguing that the intermingled documents doctrine necessitates the use of scope-limiting search protocols. This approach acknowledges the practical reality that there will be some instances where it is infeasible for law enforcement agents to search for documents responsive to a valid warrant at the site of the search. In these cases, where responsive documents are so "intermingled" with documents that otherwise could not validly be seized, officials may be permitted to remove all the documents for a later search off-site.[33] Although the seizures in these cases are overbroad, courts will permit them based on concerns of practicality.[34] However, courts may also impose limits on the scope of the searches.

For example, in *United States v. Tamura*, the leading intermingled documents case, the court recognized that "the wholesale seizure of documents for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as 'the kind of investigatory dragnet that the Fourth Amendment was designed to prevent.'"[35] The *Tamura* court relied in part on language in *Andresen v. Maryland* 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."[36] This is because in searches of papers, "it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."[37]

---

[31] *See, e.g.*, United States v. Shilling, 826 F.2d 1365, 1369-70 (4th Cir. 1987).

[32] *Carey*, 172 F.3d at 1272.

[33] United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982); *see also Shilling*, 826 F.2d at 1369-70. The leading treatise on criminal procedure and the American Law Institute's Model Code also endorse this procedure. *See* 1 WAYNE R. LAFAVE, SEARCH & SEIZURE § 2 (2d ed. 1987 & 1994 Supp.); AMERICAN LAW INSTITUTE, A MODEL CODE OF PRE-ARRAIGNMENT PROCEDURE § 220.5 (1975).

[34] *Shilling*, 826 F.2d at 1369-70.

[35] *Tamura*, 694 F.2d at 595 (quoting United States v. Abrams, 615 F.2d 541, 543 (1st Cir. 1980)).

[36] 427 U.S. 463, 482 n. 11 (1976).

[37] *Id*.

In interpreting the Fourth Amendment, courts attempt to maintain a balance between the protection of individual citizens' privacy and the necessity of the government to discover evidence and prosecute crimes.[38] The large scale seizures necessitated by the practical realities of intermingled documents threaten to upset this balance. To address this problem, the *Tamura* court developed a procedure limiting the scope of searches where government agents have already taken possession of the documents. The court suggested that agents who seal and hold the documents pending the approval of a magistrate for a further search will likely avoid Fourth Amendment problems.[39] If the magistrate determines that the seized documents "'constitute books, diaries, or other documents containing matter not specified in the warrant'" she will "'specif[y] such . . . conditions and limitations on the further search . . . as may be appropriate to prevent unnecessary or unreasonable invasion[s] of privacy'" or order the documents returned.[40]

Originally, the intermingled documents doctrine remained fairly limited in application. The *Tamura* court itself envisioned that situations necessitating the procedure would be "comparatively rare,"[41] and courts tended to limit its applicability to a few cases involving searches of thousands of documents.[42] However, the heightened capacity for storing intermingled documents presented by computers, combined with the omnipresence of computers in contemporary life, suddenly gave this doctrine a new and different significance.

No longer merely word processors or data aggregation tools, computers now function as diaries, photo albums, stereos, telephones, desktops, file cabinets, waste paper baskets, and televisions. Computers have storage capacities greater than ever before: today, most basic personal computers come with at least eighty gigabytes of storage,[43] the

---

[38] *See* New Jersey v. T.L.O., 469 U.S. 325, 337 (1985) ("On one side of the balance [of the Fourth Amendment's reasonableness requirement] are arrayed the individual's legitimate expectations of privacy and personal security; on the other, the government's need for effective methods to deal with breaches of public order.").

[39] *Tamura*, 694 F.2d at 595-96.

[40] *Id.* at 596 n.3.

[41] *Id.* at 595.

[42] *See, e.g.*, *id.* (seizing eleven boxes, thirty-four file drawers of documents, and seventeen drawers of cancelled checks following search of an office for evidence of bribery, mail and wire fraud, conspiracy, racketeering, and Travel Act violations); United States v. Shilling, 826 F.2d 1365, 1369 (4th Cir. 1987) (seizing "entire file cabinets" following search of a residence for evidence of income tax violations).

[43] PC World, *How To Buy a Desktop PC*, Sept. 12, 2007, http://www.pcworld.com/article/id,125649-page,3-c,desktops/article.html#.

equivalent of forty million pages of text or eighty thousand books.[44] In addition to storing the documents and files users consciously save, computers also typically record "metadata"—information about the creation and modification of documents—as well as data deleted by the user, which investigators may be able to recover fully or partially.[45] Computers also store information about the websites a user has visited on the Internet.[46] With sixty-six percent of all homes in the United States containing computers,[47] and their massive ability to retain information for and about their users, courts have become increasingly concerned about balancing privacy interests against the government's need to search electronic storage devices.[48]

In a groundbreaking article, Raphael Winick recognized the rapidly expanding threat of generalized warrants that computer searches presented and argued that courts should apply *Tamura*'s procedure for intermingled paper documents to computer searches.[49] He realized that the danger the *Tamura* court saw in relation to file cabinets storing hundreds or thousands of documents becomes that much greater when considering computers with storage capacities of millions of pages of text. In response, Winick suggested expanding on *Tamura* by recommending that after seizing a computer, officers "should be required to specify which types of files are sought."[50] Law enforcement agents can, he suggested, outline the methods they will use to sift through the electronic data, and present them for approval by a magistrate. Use of key word searches,

---

[44] WiseGeek, *How Much Text Is in a Kilobyte of Megabyte?*, http://www.wisegeek.com/how-much-text-is-in-a-kilobyte-or-megabyte.htm (last visited Nov. 8, 2007).

[45] *See* Thomas K. Clancy, *The Search and Seizure of Computers and Electronic Evidence: The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 269-70 (2005) (noting that "deleted" documents may not be erased from a computer's hard drive until the drive is reformatted, and that even then investigators may still be able to recover documents or portions of documents); Kenneth J. Withers, *Electronically Stored Information: The 2006 Amendments to the Federal Rules of Civil Procedure*, 4 NW. J. TECH. & INTELL. PROP. 171, 174 (2006).

[46] People v. Gall, 30 P.3d 145, 162 (Colo. 2001) (Martinez, J., dissenting).

[47] U.S. Census Bureau, *supra* note 1, at 1-2.

[48] *See infra* note 52.

[49] Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 105 (1994).

[50] *Id.* at 108.

directory and file lists, and file types may aid officers in formulating their search protocols.[51]

As computer ownership and use increased, the heightened threat of overbroad searches began to register with the courts.[52] They started responding to these concerns by applying rules designed for physical searches to digital storage devices, many of them adopting the approach advocated by Winick. The Tenth Circuit became the first court to recommend this procedure in *Carey v. United States*.[53]

In *Carey*, the court expressed its concern that due to the ubiquity and immense storage capacity of computers, digital searches require a "special approach"[54] to avoid the dangers of becoming generalized.[55] The court considered whether a warrant authorizing a search for narcotics imposed any limit on the computer files agents could open. The detective involved in the *Carey* search began his examination of the defendant's computer by conducting key word searches of text files, as he looked for evidence relating to suspected drug crimes.[56] When this method failed to uncover evidence, he looked through the computer's file directories, where he discovered a JPG file. Upon opening it, he immediately saw that it contained an image of child pornography. The detective then downloaded over two hundred more JPG files, opening many of them in order to verify

---

[51] *Id.* at 107-08.

[52] *See, e.g.*, *In re* Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993, 846 F. Supp. 11, 12 (S.D.N.Y. 1994) (quashing a subpoena for any computer used by specified officers and employees of the subpoenaed corporation for being "overly broad"); *see also* United States v. Adjani, 452 F.3d 1140, 1152 (9th Cir. 2006) (acknowledging that "[i]n this era of rapid technological change" "[t]he contours of . . . protections in the context of computer searches pose difficult questions"); 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."); People v. Gall, 30 P.3d 145, 156 (Colo. 2001) (Martinez, J., dissenting) (noting that "because computers are different from writings, both in degree and in kind, . . . [b]oth the seizure of a computer and the search of a computer's data are separate and serious intrusions of individual privacy" requiring special protections).

[53] 172 F.3d 1268 (10th Cir. 1999).

[54] *Id.* at 1275 n.7.

[55] Other courts have echoed the call for a "special approach" or have characterized computer searches as "unique." *See* United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000); United States v. Barbuto, 2001 U.S. Dist. LEXIS 25868, No. 2:00CR197K, at *10 (D. Utah Apr. 12, 2001); *see also Gall*, 30 P.3d at 161 (Martinez, J., dissenting) (calling for a "specialized approach" due to the differences between computers and "writings and containers of writings").

[56] *Carey*, 172 F.3d 1268, 1271 (10th Cir. 1999).

that they contained similar images. Only then did he return to his search for evidence of drug transactions.[57]

The defendant moved to suppress the images of child pornography, arguing that because the warrant only permitted the officers to search for computer files containing "'names, telephone numbers, ledger receipts, addresses, and other documentary evidence relating to the sale and distribution of controlled substances,'" the search of his computer for child pornography transformed the warrant into a general warrant, and resulted in an illegal general search.[58] The government responded by comparing a computer search to the search of a file cabinet, arguing that just as if it had found the images in a valid search of a file cabinet for paper documents, the images fell under the plain view exception.[59] The *Carey* court rejected this argument, instead imposing a subjective intent test. The court held that every image except the first should be suppressed. This first image the detective had discovered inadvertently, but the other images were the product of an unauthorized search for illegal pornography; the detective had "temporarily abandoned" his search for evidence of drug trafficking.[60] Instead, he should have obtained a second warrant authorizing his search for the other images.[61]

The *Carey* court continued by declaring that reliance "on analogies to closed containers or file cabinets may lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.'"[62] Instead, it recommended that courts acknowledge that computers contain intermingled documents and adopt the *Tamura* court's procedure, as applied to computers by Winick[63] (the "*Carey-Tamura*" approach). It was this application of the intermingled documents doctrine that the *Carey* court described as the required "special approach."[64]

The Tenth Circuit clarified this meaning in *United States v. Campos*.[65] In *Campos*, law enforcement agents obtained a warrant to search the

---

[57] *Id.*

[58] *Id.* at 1270, 1271-72.

[59] *Id.* at 1272.

[60] *Id.* at 1273.

[61] *Id.*

[62] *Id.* at 1275.

[63] *Id.*

[64] *Id.* at 1275 n.7.

[65] 221 F.3d 1143, 1148 (10th Cir. 2000).

defendant's computer for images of child pornography after they received information from a man alleging that the defendant had sent him two images of child pornography via email.[66] The agents obtained a warrant to search the defendant's computer for "items relating to child pornography,"[67] and recovered a total of eight images, including the two originally provided by their informant.[68] The defendant moved to suppress the additional six images, arguing that the search was overly broad and should have been restricted to just the original two images. The court held that, unlike in *Carey*, the officers' search here had remained properly within the scope of the warrant. However, the *Campos* court added the same caveat as did the court in *Carey*, that a "special approach" necessitating an "intermediate step of sorting various types of documents" may be required when computers contain intermingled documents.[69] The *Campos* and *Carey* opinions make clear that, to the Tenth Circuit at least, a "special approach"—meaning a file sorting requirement—may be necessary to protect against general warrants.[70]

Other courts have developed different rules to address the unique dangers to privacy presented by digital searches. Some courts have interpreted the particularity requirement to require a description of the evidence sought rather than the computer hardware that stores that evidence.[71] Alternatively, courts have required that the warrant specify

---

[66] *Id.* at 1145.

[67] *Id.* at 1147.

[68] *Id.* at 1146.

[69] *Id*.

[70] Another Tenth Circuit case, *United States v. Walser*, also supports this view. 275 F.3d 981 (10th Cir. 2001). In *Walser*, the court held that officers had properly opened an AVI file that contained a child pornography video, even though according to the warrant the officers were authorized only to search for evidence of drug possession and transactions. The court explained that the agent had seized the defendant's computer and searched it using a "specific methodology" during the course of which he happened to open the AVI file. *Id.* at 984. At that point, the officers sought a warrant specifically authorizing a search for child pornography. *Id.* at 985. The court acknowledged that "key differences" apply to searches of computers, as they are "able to hold the equivalent of a library's worth of information." *Id.* at 986. In computer searches, officers are more likely to encounter intermingled documents, and thus a greater risk of invasion of privacy exists. Here, however, the court found that the agent conducting the search had met *Carey*'s requirements by using a "clear search methodology," not a wholesale "rummaging." *Id.* at 987.

[71] *See* Ark. Chronicle v. Easley, 321 F. Supp. 2d 776, 793-94 (E.D. Va. 2004) (holding that a warrant authorizing the search and seizure of "virtually every piece of computer equipment, computer file or document" in a home "essentially amounted to a general warrant giving police the authority to rummage through every single computer file and document with no limitations").

"the purpose for which the computers were seized"[72] in order to impose limits on the search. A district court has developed an approach that treats folder labels, but not folder contents, as being in plain view, limiting the folders an investigator may validly search to those with either ambiguous or clearly responsive names.[73] A New York state court took a similar approach, stating that police did not have the right pursuant to their warrant to open a digital folder based on the folder's label, when that label clearly indicated the folder contained data that was unresponsive to the warrant.[74] Other courts have required investigators to use more technologically advanced search methods at their disposal when there was some indication that those methods would be sufficient to capture the needed evidence.[75] Because, however, the *Carey-Tamura* approach has been one of the most widely cited and criticized of the judicial innovations, I will focus primarily on that rule in the discussion below.

IV. AN ELUSIVE SOLUTION

Like courts, legal scholars have offered proposals for how to apply Fourth Amendment protections to digital sources. Some advocate their own "special approach"[76] while others deny that their solutions are "special" at all, but rather mere applications of traditional Fourth Amendment rules to the digital context.[77] Regardless of how they are framed, the commentators share both a concern that digital searches conducted pursuant to warrants contain a heightened risk of governmental

---

[72] *See* United States v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998).

[73] *See* United States v. Stierhoff, CR No. 06-042-ML, 2007 U.S. Dist. LEXIS 18846, at *73-74 (D.R.I. Mar. 13, 2007).

[74] People v. Carratu, 755 N.Y.S.2d 800, 808 (N.Y. Sup. Ct. 2003) (suppressing evidence discovered after investigators opened a digital folder when its name "clearly indicated that it likely contained false identification documents rather than documents or records" within the scope of the warrant).

[75] *In re* Grand Jury Supoena Duces Tecum Dated November 15, 1993, 846 F. Supp. 11, 13 (S.D.N.Y. 1994) (quashing a subpoena for being overly broad when the government "acknowledged that a 'key word' search of the information stored on the devices would reveal 'which of the documents are likely to be relevant to the grand jury's investigation'"); *see also* People v. Gall, 30 P.3d 145, 166 (Colo. 2001) (Martinez, J., dissenting) ("[S]earches may be limited to avoid searching files not included in the warrant by 'observing file types and titles listed in the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory.'").

[76] Kerr, *Digital Evidence and the New Criminal Procedure*, *supra* note 2, at 280.

[77] Clancy, *supra* note 45, at 195; Daniel J.S. Ziff, *Note, Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841, 842 (2005).

intrusion and a belief that none of the judicial rules applied thus far are satisfactory. This dissatisfaction has prompted each to offer his own proposal. Unfortunately, as of now no single proposal has adequately solved the problem posed by digital searches. The inability of both courts and commentators to develop a generally applicable rule demonstrates the complexity of the problem and its resistance to any one solution, at least with our current state of technology. However, the flaws exhibited by the proposed rules demonstrate that it is important to explore the issues presented by digital searches more completely before rushing to constitutionalize or enact any such rule. These flaws also indicate that a single, ideal rule is likely not forthcoming from courts, Congress, or legal academics. Instead, the lower courts should continue to innovate, developing new rules that may not be generalizable to all contexts, but may take the increased dangers presented by digital searches into account in contextually appropriate ways.

The *Carey-Tamura* method, one of the earliest and most frequently applied by the courts, has received the most attention from commentators who have voiced dissatisfaction with existing approaches. While some courts continue to cite *Carey* and advocate its approach,[78] commentators have almost uniformly criticized it. Despite these criticisms, however, the *Carey-Tamura* approach could still provide a helpful tool in reducing the threat of generalized searches in some contexts.[79]

There are three major criticisms of the *Carey-Tamura* rule, each of which is valid in many, but not all, factual contexts. The first, levied by Professor Orin S. Kerr, has focused on the method's ex ante restriction requirement.[80] 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."[81] 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. An analyst will

---

[78] *See, e.g.*, United States v. Comprehensive Drug Testing, Inc., 473 F.3d 915, 965 n.11 (9th Cir. 2006) (Thomas, J., dissenting); United States v. Hill, 459 F.3d 966, 978 n.14 (9th Cir. 2006); United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001); United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000); *In re* Search of 3817 W. West End, First Floor Chi., Ill. 60621, 321 F. Supp. 2d 953, 961 (N.D. Ill. 2004); People v. Gall, 30 P.3d 145, 161 (Colo. 2001) (Martinez, J., dissenting).

[79] Similarly, while not discussed here, other court-developed rules that are not workable in all cases may be able to provide important protections in some factual contexts. *See, e.g.*, *In re* Grand Jury Supoena Duces Tecum Dated Nov. 15, 1993, 846 F. Supp. 11, 13 (S.D.N.Y. 1994) (noting that the government had acknowledged that use of a key word search would have been sufficient to locate documents relevant to the investigation).

[80] Kerr, *Searches and Seizures in a Digital World*, *supra* note 2, at 575-76.

[81] *Id.* at 575.

therefore not know which forensic tool is best suited to her search until she begins her examination of the files. She will have a difficult time deciding on a protocol ex ante, and the magistrate to whom she applies for a warrant will have even less of an idea about how to evaluate her recommendation.[82]

A second practical objection to the *Carey-Tamura* method derives from the same phenomenon that is driving increasing concerns about the general nature of computer searches: the rapidly growing storage capacities of computers and other electronic devices.[83] When Raphael Winick first proposed applying *Tamura*'s intermingled document procedure to computers, a typical home computer could store the equivalent of about 100,000 typewritten pages.[84] Hard drives in typical home computers sold today are over 800 times larger, and can contain the equivalent of forty million typewritten pages.[85] When even average-sized hard drives hold such large numbers of documents, having a magistrate review file directories becomes highly impractical.

A third common criticism of the *Carey-Tamura* screening mechanism is that it assumes the file names the magistrate reviews accurately reflect the contents of the files. The problem here is that criminals with an incentive to hide evidence are unlikely to name files in ways that lead investigators directly to them.[86] Not only can they give files innocuous sounding titles (for example "Johnny's Science Fair Project" lacks the malevolent ring of "SexyTeenPics"), but suspects with something to hide can also easily change the extensions under which files are saved. Thus, someone attempting to disguise a spreadsheet detailing ill-gotten profits might label it with the extension .jpg, indicating that it is an image file instead. Conversely, someone trying to disguise images of child pornography could label his digital contraband with .doc extensions.[87]

While there are valid objections to the specific special approaches that have been offered by the courts, as most clearly illustrated by the *Carey-Tamura* approach, valid critiques may also be made of the proposals offered by academics. Although each of the commentators has proposed fixes that acknowledge the potential dangers presented by digital evidence searches,[88] none of their rules offers a universal solution. One proposal,

---

[82] *Id.* at 575-76.

[83] *See* Ziff, *supra* note 77, at 860.

[84] Winick, *supra* note 49, at 81.

[85] *See* WiseGeek, *supra* note 44.

[86] *See, e.g.*, Clancy, *supra* note 45, at 207-08.

[87] *See id.*

advocated by Thomas K. Clancy, would treat electronic storage devices just like other containers.[89] This approach flows naturally from those who argue that a "special approach"—i.e. the application of unique procedures to computers or electronic documents—is unnecessary. But because Clancy acknowledges the dangers of unlimited searches of computers, he has proposed focusing instead on "the sufficiency of the allegations of criminal conduct or the description of the objects sought"[90] as a means of protecting citizens from excessive governmental intrusion. However, it is unclear how this will protect people from general searches in practice when investigators will still be forced to open each computer file to determine whether or not it is responsive to the warrant.

It is possible, of course, that by suggesting a less effective solution, Clancy is merely contending that the danger is not sufficient enough to warrant stronger safeguards. He may believe that the weak protections he offers will maintain the proper balance between privacy rights and governmental need. Certainly this is consistent with advocating the container analogy: computers contain evidence intermingled with other materials just as diaries, file cabinets, desk drawers, and calendars do. Despite the heightened risk of intermingling that electronic storage of documents may present, computers should not merit special rules.[91]

It seems too soon to reach such a definitive conclusion. Currently, and as Clancy himself has noted, "searches of computers for evidence of child pornography and other sexual exploitation of children make up a shockingly large percentage of the decided cases."[92] While these cases are certainly the most common, they are far from the only type of digital investigations. Until more fact patterns present themselves, these cases will continue to be the most salient, and the ones decision makers will likely have in mind when formulating rules. Unfortunately, the particularly distasteful nature of the crime may unconsciously influence decision makers (as it may have influenced Clancy) to believe that stronger protections against general computer searches are unnecessary. Of course, this is only speculation. However, the fact that the vast majority of cases have involved similar fact patterns indicates that decision makers have yet to see the full contours of the computer search problem, and the full range of threats to individual rights they potentially represent. This

---

[88] *See id.* at 199 ("Accepting this view does not mean that wholesale searches of data on computers are permitted."); Ziff, *supra* note 77, at 869 (noting that his proposal "responds to concerns, shared by Professor Kerr and [the *Carey* court], with the grand scale of computer searches").

[89] Clancy, *supra* note 45, at 217-18.

[90] *Id.* at 200.

[91] *Id.* at 199, 217-18.

[92] *Id.* at 200.

limited context indicates that courts or legislatures should hold off on selecting one particular method of regulating digital searches.

A second proposal involves applying existing scope limits to computers. An officer authorized to look for incriminating documents would have the authority to open and inspect all digital files, including those innocuously named, in order to determine whether they are among those documents authorized to be seized by the warrant. This would be permissible because in the case of document searches "'it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.'"[93] The officers' authority to inspect the documents would, however, "extend[] only so far as necessary to determine if a given document is within the scope of the warrant."[94] Under this proposal, then, computer owners would be protected from a general search because investigators would only have the authority to examine files cursorily—they would be limited to making a threshold determination about whether the document was covered by the warrant or not—but their authority to search would not extend to scrutinizing the document for evidence of other crimes.[95]

This proposal provides little real protection. First, it relies on officers to police themselves. While it seems reasonable to think that in most cases practical limitations alone would prevent officers from reading through every word of every document to search for evidence of other crimes, in the event that they did uncover evidence of a second crime, courts and citizens would be forced to rely on only the officers' word that they did so while conducting a cursory search for evidence authorized by the warrant. Unlike many search situations, where a court is forced to weigh the credibility of an officer's statement against that of a defendant or a witness, most computer searches take place far from the watchful eyes of the computer owner. Officers seize the computer first, and bring it back to a forensic laboratory to be searched at the government's leisure.[96] Once there, the government can create a bitstream image—an exact copy of the hard drive—and retain it "to mine it for clues without limit."[97] Zealous investigators motivated by the best of intentions—protecting current or future victims of crime—may find it morally conscionable to go on a fishing expedition for evidence of crimes about which they may have a

---

[93] Ziff, *supra* note 77, at 862.

[94] *Id.*

[95] *See id.* at 861-65.

[96] Kerr, *Digital Evidence and the New Criminal Procedure*, *supra* note 2, at 288.

[97] *Id.* at 300.

suspicion, but not probable cause, covering up their activities with white lies in court.[98] Because the court will only have the officer's word, even in the cases where an officer noticed clear evidence of a secondary crime merely by opening a file, this reliance on the government's say-so will serve only to erode the trust between law enforcement and the public.

Second, and more importantly, this proposed solution offers no protection from general searches where the evidence sought is stored in the form of text documents rather than images. A cursory search acts as a meaningful limiting device only when the evidentiary value of a document is apparent at first glance. This will be true for many, but not all, computer searches. Suspected transmitters of child pornography, for example, might receive some protection from general warrants under this theory. As investigators will be opening files looking for illegal images, they should quickly discard any text or data files as being non-responsive to the warrant.[99] However, this technique will not provide any protection from a general search to those accused of crimes where the evidentiary value of a document is not immediately apparent. An investigator authorized to search a computer for evidence relating to tax evasion, for example, may have to scrutinize each and every spreadsheet and document to determine whether it is responsive.

A third proposal, put forth by Orin Kerr and inspired by his concerns about the "difficulties [that] arise when [Fourth Amendment] doctrine is applied to the facts of computer crime investigations,"[100] would "reject the plain view rule in the context of digital evidence searches."[101] Eliminating this rule would render inadmissible any digital evidence discovered beyond that authorized by the warrant. According to Kerr, such a rule could be generated either by the courts or by Congress,[102] but would likely need to at least be supplemented with federal privacy statutes.[103]

---

[98] *See* Christopher Slobogin, *Testilying: Police Perjury and What to Do About It*, 67 U. COLO. L. REV. 1037, 1041 (1996) ("[E]xisting literature demonstrates a widespread belief that testilying is a frequent occurrence."); *cf.* Sarah Barlow, *Patterns of Arrest for Misdemeanor Narcotics Possession: Manhattan Police Practices 1960-62*, 4 CRIM. L. BULL. 549, 549-50 (1968) (examining data demonstrating that the incidence of testimony by police that arrestees dropped drugs as the police discovered them increased after the application of the exclusionary rule to the states, indicating that "the police are lying about circumstances of arrests" in order to avoid the suppression of evidence).

[99] Conversely, this technique may offer little protection from general searches to *unsuspected* child pornographers. When investigators have probable cause to search the files of those suspected of other crimes, the immediately incriminating nature of images of child pornography will mean that these files will likely survive a challenge to suppress.

[100] Kerr, *Digital Evidence and the New Criminal Procedure*, *supra* note 2, at 281.

[101] *Id.* at 314; Kerr, *Searches and Seizures in a Digital World*, *supra* note 2, at 577.

[102] *See* Kerr, *Digital Evidence and the New Criminal Procedure*, *supra* note 2, at 314.

Practically, this may be the best means for limiting the scope of digital searches, as current technology has not, to date, presented investigators with a tool allowing them both to conduct a comprehensive search of digital files for authorized items while screening out documents not described in a warrant. This proposal would, however, offer far greater protection to digital files than Fourth Amendment doctrine provides to any category of physical evidence. While Kerr has argued that such a rule might still "best balance the competing needs of privacy and law enforcement in light of developments in computer technology," even he has concluded that eliminating the plain view exception is "too severe," at least at present.[104]

V. THE CASE FOR THE COURTS

Aside from the elimination of the plain view doctrine as applied to computers, Kerr has more generally advocated for legislatively enacted rules to address issues of criminal procedure presented by new technology, rather than reform initiated by the courts.[105] Kerr argues that legislatures possess a significant institutional advantage in creating rules governing law enforcement investigations using new technologies, at least as long as these technologies are rapidly changing.[106] According to Kerr, legislatures are more institutionally competent because they can create rules ex ante rather than ex post, have greater flexibility, and are better situated to gain a comprehensive understanding of the technologies at issue.[107] While

---

[103] Kerr, *Searches and Seizures in a Digital World*, *supra* note 2, at 583.

[104] *Id.*

[105] Orin S. Kerr, *The Search and Seizure of Computers and Electronic Evidence: Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 88 (2005). While Kerr has proposed several specific statutory warrant rules that chiefly clarify the translation from the language of physical investigations to that of the digital, none of these proposed legislative rules addresses exactly how digital searches of data storage devices can be narrowed to avoid authorizing general searches. *Id.* at 127-34. Instead, these rules acknowledge the realities of what he has described as the two-step search process for digital evidence—the process by which investigators search a site for physical evidence, and later conduct a digital search off-site of any hardware they initially seized. *Id.* at 86. For example, Kerr proposes that statutory rules should: (1) require the police both to describe the type of physical evidence they plan to seize and then the type of evidence they will search for in the subsequent electronic search; (2) recognize that a Fourth Amendment search still occurs even when the physical object being searched is a bitstream copy of the seized data; and (3) provide guidance on when each part of the two step search process should be executed, and when seized hardware must be returned. *Id.* at 127-34; *see also* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 858-60 (2004).

[106] Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, *supra* note 105, at 805.

each of Kerr's arguments might apply to the creation of rules governing new technologies,[108] his thesis fails to hold in the context of digital searches. At least in this context, until a fuller picture of the factual circumstances in which these searches arise emerges and the implications that they have for individual rights becomes clearer, lower courts are better positioned to continue innovating with the application of Fourth Amendment rules.

This may seem counterintuitive because legislatures enact generally applicable rules prospectively, rather than waiting to resolve issues as they arise in the form of cases and controversies, as courts do. Judicially imposed rules create an undesirable lag between the appearance of new technologies and the rules that apply to them. This may result in courts promulgating "unsettled and then outdated rules."[109] Alternatively, legislatures can proactively provide law enforcement agents with guidance on new technological issues, addressing potential legal challenges before they arise in court.[110]

Clearly, as indicated by the cases discussed above, the time has already passed for Congress to provide the courts with ex ante rules for narrowing searches. These cases have already arrived and been adjudicated before state and federal courts, and those courts were left to make decisions ex post, as the specific circumstances arose. Additionally, even Kerr's premise—that legislatures could have enacted laws to provide guidance up front—may not apply here. Unlike other technological concerns, such as the privacy status of e-mail,[111] the privacy issues raised by searches of home computers were likely not immediately apparent to either Congress or the courts when magistrates first issued warrants involving digital evidence. Specific cases and controversies, as well as further technological change in the form of increased storage capacity and functionality, were required to call attention to these problems. As these cases have trickled up to the courts, judges and academics alike have recognized the possibility that such warrants could upset the careful balance the Fourth Amendment has traditionally struck between the concerns of law enforcement and privacy. However, the attention has yet to reach the level of public awareness and concern that it often takes to

---

[107] *Id.* at 868, 871, 875.

[108] *But see* Solove, *supra* note 22, at 748 (rebutting Professor Kerr's arguments for the institutional competence of legislatures over courts in developing Fourth Amendment rules for new technologies).

[109] Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, *supra* note 105, at 868.

[110] *Id.* at 870.

[111] *Id.*

initiate legislative attention.[112] In such cases, courts cannot and should not wait for legislatures to act.

Far from being problematic, courts acting ex post may hold the comparative institutional advantage in this context. When Fourth Amendment concerns are not immediately apparent, an interstitial judicial decision-making approach is preferable. One cannot assume that once the issue has finally come to the attention of the courts that the full contours of the problem will be visible. Only the examination of many different cases will illuminate the full depth and breadth of the newly discovered Fourth Amendment concern. Additionally, in the case of digital searches, not only were the serious privacy implications not immediately apparent, but no easy solution to them has been forthcoming either, as the discussion above should have made clear.

Kerr also argues that legislatures' flexibility gives them another advantage over courts. Whereas legislatures are free to experiment with rules and can amend them as needed, courts are bound by *stare decisis*.[113] However, *stare decisis* is an obligation that may be "released when competing public policy beckons persuasively" due to "changed conditions[,] . . . increased knowledge," or the realization that "the rule has become unsound in the circumstances of modern life."[114] Indeed, with respect to the Fourth Amendment, the courts' rules have exhibited a high degree of flexibility: exceptions "such as *Terry* stops, exigent circumstances, and 'special needs' in schools and workplaces" "allow the courts to accommodate a wide range of government investigative activity within the protective framework of the Fourth Amendment" while still balancing privacy interests.[115] And courts have been equally flexible and creative in coming up with unique requirements in order to narrow the scope of future digital searches. Reviewing courts have recommended[116]

---

[112] *Id.*; *see also* BENJAMIN N. CARDOZO, THE NATURE OF THE JUDICIAL PROCESS 144 (1921) ("All history demonstrates that legislation intervenes only when a definite abuse has disclosed itself, through the excess of which public feeling has finally been aroused."); M. Stuart Madden, *The Vital Common Law: Its Role in a Statutory Age*, 18 U. ARK. LITTLE ROCK L. REV. 555, 566 (1996) ("A statutory answer is not normally sought until a problem has erupted in the public consciousness, when a social dilemma has achieved such a level of gravity and tenacity that 'social convention' demands 'community voting.'").

[113] Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, *supra* note 105, at 871.

[114] Madden, *supra* note 112, at 590 (quoting Boblitz v. Boblitz, 462 A.2d 506, 526 (Md. 1983)); *see also* OLIVER WENDELL HOLMES, COLLECTED LEGAL PAPERS 187 (1921) ("It is revolting to have no better reason for a rule of law than that so it was laid down in the time of Henry IV.").

[115] Solove, *supra* note 22, at 762.

and authorized[117] magistrates' imposition of ex ante search protocols; they have required the limitation of searches by examining lists of file names[118] or key word searches;[119] they have treated computers simply as closed containers;[120] and they have imposed subjective intent tests.[121]

This spectrum of responses may come from the fact that courts are forced to make ex post decisions: when presented with a new set of facts, courts are able to develop or grow the law by applying traditional Fourth Amendment rules to the new context. "[F]requent encounters with a general problem, presented in various contexts that an endless variety of fact patterns provides" allow courts to formulate and test new rules.[122] Additionally, *stare decisis* acts as less of a binding norm when courts are suddenly presented with entirely new factual contexts[123]—including those generated by technological change. In fact, courts may be doing a *better* job at providing flexibility in decision-making than legislatures when it comes to technological issues. Professor Daniel J. Solove notes, for example, that Congress has failed to enact legislation that keeps pace with technological developments, and has neglected to update existing statutes.[124] While Solove's response focuses on electronic surveillance law, the same can certainly be said for privacy concerns relating to overly broad computer searches.

It is true that with this type of judicial innovation through common law decision-making the clarity of the law suffers. However, as Solove asserts, the values of "flexibility and clarity are often in conflict" and are "endemic to all rules, whether legislative or judicial."[125] With

---

[116] *See, e.g.*, United States v. Carey, 172 F.3d 1268, 1275-76 (10th Cir. 1999); People v. Gall, 30 P.3d 145, 162-65 (Colo. 2001) (Martinez, J., dissenting).

[117] *See, e.g.*, *In re* Search of 3817 W. West End, First Floor Chi., Ill. 60621, 321 F. Supp. 2d 953, 959 (N.D. Ill. 2004).

[118] *See, e.g.*, People v. Carratu, 755 N.Y.S.2d 800, 807-09 (N.Y. Sup. Ct. 2003).

[119] *See, e.g.*, *In re* Grand Jury Subpoena Duces Tecum Dated November 15, 1993, 846 F. Supp. 11, 13 (S.D.N.Y. 1994).

[120] *See, e.g.*, *Gall*, 30 P.3d at 153; United States v. Al-Marri, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002).

[121] *See, e.g.*, *Carey*, 172 F.3d at 1273.

[122] Cornelius J. Peck, *The Role of Courts and Legislatures in the Reform of Tort Law*, 48 MINN. L. REV. 265, 297 (1963).

[123] *See* Planned Parenthood v. Casey, 505 U.S. 833, 854-55 (1992) (explaining that the doctrine of *stare decisis* does not function as an "inexorable command" when the "facts have so changed, or come to be seen so differently, as to have robbed the old rule of significant application or justification"); *see also supra* text accompanying note 114.

[124] Solove, *supra* note 22, at 769.

technological change, as Kerr suggests, flexibility becomes more important so that rules can change in response to technological advances.[126] Lack of clarity therefore becomes a practical reality of both judicial and legislative rulemaking, and a rational tradeoff.

Finally, Kerr argues that the legislative branch has greater institutional competence for generating Fourth Amendment privacy rules relating to new technology due to the legislature's ability to gather a comprehensive understanding of the facts. While reviewing courts are generally limited in their fact gathering to written briefs and oral arguments, legislative rules can be the product of hearings with testimony and comments from experts, advocacy groups, civil liberties groups, and the Department of Justice. Additionally, the entire process tends to be open to public scrutiny, which can also influence the end results.[127] The breadth and types of sources provide the legislature with a clearer understanding of how the technology actually works, the argument goes.

However, Solove has argued that "there is no reason . . . to assume that the average legislator can better understand technology than the average judge."[128] Furthermore, "in many cases, the technologies at issue are not particularly complex."[129] Solove asks, "[d]o we really need two years and thousands of pages of detailed information to understand how e-mail works?"[130] The same question can be asked about naming and opening files on a home computer—the major technological understanding required to think about digital searches. Any further necessary information can efficiently be gathered by a quick Westlaw search for Kerr's own law review articles, which summarize the technology involved at a level even a Luddite in robes can understand. At least with regard to conceptualizing the problems involved in limiting the scope of digital searches, the most important skill is a judicial one: analogizing computer searches to searches of physical documents or objects, and applying Fourth Amendment rules in a way that is consistent with that comparison.

The courts, then, rather than the legislature, are the best institution for reestablishing an acceptable balance between individual privacy and the needs of law enforcement when technology is in flux, at least for the particular problem presented by computer searches.[131] Courts have played

---

[125] *Id.* at 767-68.

[126] Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, *supra* note 105, at 871.

[127] *Id.* at 875, 881.

[128] Solove, *supra* note 22, at 771.

[129] *Id.*

[130] *Id.*

this role before with success, adapting the Fourth Amendment to provide individual protections even in the face of new technologies. Justice Brandeis recognized that courts can and should play this role in his dissent in *Olmstead*, when he wrote, "[c]lauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world. . . . Time works changes, [and] brings into existence new conditions and purposes."[132] Thus, he concluded, "'in the application of a constitution, our contemplation cannot be only of what has been but of what may be.'"[133] The Supreme Court later demonstrated its capacity to adapt constitutional rules to technological changes in *Katz*, when the Court overruled *Olmstead*. There, the Court rejected the "narrow" and static view of the Fourth Amendment on which *Olmstead* had rested, holding that a warrant was required to eavesdrop electronically on telephone calls made from a public phone booth.[134]

The role of the courts is even more vital in the context of computer searches. Many courts and commentators have expressed concern over the lack of a limiting device for computer searches.[135] Without a means of limiting the scope of searches, otherwise valid warrants have the potential to become overbroad, authorizing generalized searches. While there is not yet a judicial consensus that recognizes the privacy dangers inherent in computer searches, as computers' storage capacities grow and they become ever more present in our daily lives, this concern is increasing. At the same time, neither the courts nor the commentators have offered a silver bullet solution in the form of a generally applicable rule. Each proposal offers certain advantages, but also suffers from very real flaws. Each also contains its own inherent conception of the proper balance between law enforcement needs and privacy concerns. As the technology continues to change and the courts and the citizens they protect continue to develop an intuitive sense of a proper balance, common law innovation to

---

[131] According to Professor Melvin Eisenberg, common law judges may legitimately play a "leadership role" by identifying the community's norms when they are changing or in flux. MELVIN ARON EISENBERG, THE RATIONALITY OF THE COMMON LAW: THE NATURE OF THE COMMON LAW 19 (1988).

[132] Olmstead v. United States, 277 U.S. 438, 472-73 (1928) (Brandeis, J., dissenting).

[133] *Id.* at 474.

[134] Katz v. United States, 389 U.S. 347, 353 (1967). Of course, the rule in *Katz* has ironically increased police power in some areas, as it has led courts to conclude that particular police actions do not constitute "searches" in the first place. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 40-41 (1988) (holding that the examination by police of a sealed, opaque garbage bag left on the side of a public street was not a "search" within the meaning of the Fourth Amendment—and therefore not entitled to Fourth Amendment protections—because a person has no reasonable expectation of privacy in discarded items).

[135] *See supra* note 52.

discover rules that strike that balance is necessary.[136] Courts, rather than the legislature, are best suited to find this balance.

For example, despite the criticisms of it, the *Carey-Tamura* approach would have been an appropriate tool to use in the context presented by *United States v. Comprehensive Drug Testing*.[137] That case arose from a federal investigation into the Bay Area Lab Cooperative (BALCO) on the suspicion that it was distributing illegal steroids to professional baseball players. In the course of its investigation, the government obtained warrants to search two different laboratories that had tested urine samples of Major League Baseball players.[138] However, the warrant authorized the seizure of drug test records for only ten named players whose connections to BALCO had previously been established.[139] The warrant authorized the search of computer equipment for this information as well as the seizure of the data or the hardware itself. When investigators arrived at Comprehensive Drug Testing, Inc. (CDT), one of the labs, they discovered that the information covered in the warrant existed in three different places: a list containing information about the ten named players, a master list of the drug test results for all Major League Baseball players, and an electronic directory. That directory, referred to as the "Tracey directory," contained over 2900 files including "medical test results for hundreds of other baseball players and athletes engaged in professional sports."[140] Investigators seized all three items and then used the seized files to obtain subsequent search warrants for all baseball players who had positive test results.[141]

While the majority in *Comprehensive Drug Testing* determined that investigators lawfully seized the entire Tracey directory because it contained information intermingled with evidence covered in the warrant,[142] the dissent argued that the *Carey-Tamura* procedure would

---

[136] While this Note focuses on the role reviewing courts play in developing a new common law limiting the scope of electronic searches, magistrate judges also have an important role to play ex ante, by imposing limitations on the scope of digital searches when they issue warrants. *See, e.g.*, *In re* Search of 3817 W. West End, First Floor Chi., Ill. 60621, 321 F. Supp, 953, 957 (N.D. Ill. 2004) (upholding the authority of a magistrate judge to require the government to provide an ex ante search protocol limiting the scope of computer searches).

[137] 473 F.3d 915 (9th Cir. 2006).

[138] *Id.* at 919-20.

[139] *Id.* at 921.

[140] *Id.* at 946-47 (Thomas, J., dissenting).

[141] *Id.* at 949.

[142] *Id.* at 934-35.

have been the appropriate means of limiting the examination of personal medical information outside the scope of the warrant.[143] The dissent asserted that the court should have imposed a rule requiring the agents to present the data to a "'neutral and detached'" magistrate" for review.[144] In the *Comprehensive Drug Testing* context, this approach seems correct. Here, the information responsive to the warrant was contained in a single electronic directory (as well as in two paper documents). The specific information authorized by the warrant might have been separated out from the unresponsive, private medical information with the simple expedient of a key word search or the screening of files by a magistrate. Because the warrant itself covered only a narrow set of data, and because the agents found this data almost immediately while still at the CDT lab,[145] seizing vast quantities of unresponsive data was unnecessary. Unlike in many of the digital search cases, agents had no need to open files one by one to locate the evidence covered in the warrant. Based on these circumstances, the objections to the *Carey-Tamura* approach outlined above do not apply. Here, the amount of information was not so overwhelming as to make examination by a magistrate impractical or impossible. Nor was there any question that the file type or name of the directory was disguised: the investigators found exactly what they were looking for while on-site at the lab, without significant delay.[146] Finally, with the search of a single directory, there was no difficulty imposed by creating a search protocol ex ante. The magistrate could have culled the responsive data from the unresponsive without technological know-how; there was no need for agents to present a magistrate with a step-by-step search plan upfront.

---

[143] *Id.* at 952 (Thomas, J., dissenting).

[144] *Id.* at 965 (Thomas, J., dissenting).

[145] *Id.* at 922-23 (majority opinion).

[146] Although the government may have been concerned that electronic files are *in general* more susceptible to being deleted or disguised, that concern did not appear to come into play in this specific case. While the government justified removing electronic data and computer equipment from CDT by averring in the affidavit accompanying its application for a warrant that "'[c]omputer users can attempt to conceal data within computer equipment and storage devices through a number of methods'" and "'[c]omputer hardware and storage devices may contain 'booby traps' that destroy or alter data,'" the government had no "evidence or reason to believe that CDT had engaged in . . . boobytrapping computers, or any type of data destruction or alteration." *Id.* at 960-961 (Thomas, J., dissenting). In fact, the government "had accepted in writing CDT's assurances 'that CDT will maintain and preserve all materials called for by the first subpoena as well as any materials called for by the new subpoena' and that 'CDT would not destroy or alter any of the materials called for by either of the subpoenas.'" Despite the general concerns outlined in the government's affidavit, "there was no suggestion that CDT was attempting to mislead the government in any respect." *Id.* at 961 (Thomas, J., dissenting).

It is true that circumstances where the *Carey-Tamura* approach would be useful may not be the norm. But as long as the threat of general digital searches is present, and a universal tool for addressing that threat is not, the common-law development of useful rules and a context-dependent selection of the appropriate one may be the best means of protecting the Fourth Amendment's traditional balance of privacy against governmental intrusion. It is also true that the lack of a universal rule creates uncertainty and makes the limits on government power unclear.[147] However, an interstitial rulemaking approach by the lower courts is useful where a problem with no easy solution has been identified. The courts can explore the contours of the problem—adjudicating cases like *Comprehensive Drug Testing* where the *Carey-Tamura* approach might make more sense, along with others, where the commonly raised objections to that approach have more traction. Additionally, they can innovate, creating new rules when entirely new factual or technological contexts arise.

While the uncertainty this approach generates will pose problems for law enforcement, it will provide incentives that do not now exist for law enforcement agents to pause before they search and seize indiscriminately.[148] Law enforcement agents are already functioning in a world of digital searches without clearly defined rules. Neither the courts nor Congress has provided clear rules for conducting computer searches. The Department of Justice has published a handbook that outlines the basic procedures and issues agents and prosecutors should consider when planning an electronic search, but these take the form of suggestions for how to approach searches of computer equipment and data generally—such as how to draft the warrant and accompanying affidavit—rather than rules.[149] Instead, law enforcement agents are left with little or no incentive

---

[147] Kerr, *The Search and Seizure of Computers and Electronic Evidence: Search Warrants in an Era of Digital Evidence*, *supra* note 105, at 861-62.

[148] Moreover, once reviewing courts begin to develop a set of rules governing electronic searches, magistrate judges will increasingly be able to impose scope-limiting search strategies ex ante, providing additional clarity for investigators.

[149] U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2002), *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf. For example, the handbook explains the differences between warrants to seize hardware and warrants to seize electronic information, and discusses when and why agents might opt for one rather than the other. *Id.* at 61-65. The publication also advises agents to explain their search strategy and the techniques they plan to use to separate incriminating documents from commingled documents whenever possible to avoid allegations that the government is using a warrant to justify a general search. *Id.* at 73-74. While the handbook cautions agents to "be particularly careful when seeking authority to seize a broad class of information," it does not provide specific rules or guidelines for agents to use to narrow their electronic searches. Instead, it provides practical advice designed to assist agents in

to limit themselves to searching for evidence described in the warrant. In *Comprehensive Drug Testing*, for example, the government agents could have limited themselves to the information covered by the warrant. Instead, they both seized and examined the entire Tracey directory for positive test results from other baseball players, and then used that evidence to support new warrants. If courts made it clear to investigators that the *Carey*-*Tamura* procedure was a tool they should use when reasonable, the agents might have considered whether abiding by such a procedure would have successfully provided them with all the information they were authorized to obtain, without a concurrent risk of suppression. Where the courts have been willing to suppress evidence, investigators have proceeded more cautiously, for example, by going back to obtain a second warrant in the event they inadvertently uncover incriminating evidence outside the scope of the original warrant.[150] Furthermore, the absence of a clear rule has not impeded investigators in the execution of their original searches. The suppression battle in digital search cases has generally been waged over evidence outside the scope of the original warrant; and where the courts have focused on the originally sought-after evidence,[151] they have been reluctant to suppress that evidence, even when acknowledging flaws in the warrants.[152] Thus, the lack of clear rules does not impede the admission of the originally sought evidence.

Public choice theory also supports a judicial approach to the protection of Fourth Amendment rights in this context. Public choice theorists have observed that legislative actions are frequently influenced by the efforts of interest groups to lobby the legislature to enact laws that benefit them at the expense of the general public. While the laws might harm more people than they help, the harms they produce are slight compared to the significant benefits they provide to particular interests. Well-organized interest groups therefore have strong incentives to lobby for these changes, while the more diffuse general population has weak incentives to oppose them, and faces substantial barriers in the form of higher transaction

---

drafting and executing warrants while avoiding legal pitfalls specific to electronic searches and seizures. *Id.* at 62.

[150] *See, e.g.*, United States v. Walser, 275 F.3d 981, 985 (10th Cir. 2001).

[151] *See, e.g.*, *id.* at 986-87 (focusing bulk of discussion on the defendant's motion to suppress child pornography evidence obtained during a search for records of drug transactions); United States v. Gray, 78 F. Supp. 2d 524, 528 (E.D. Va. 1999) (discussing propriety of seizure of pornographic images of minors during search for evidence of hacking).

[152] *See, e.g.*, United States v. Hill, 459 F.3d 966, 976-77 (9th Cir. 2006) (affirming the district court's denial of the defendant's motion to suppress evidence, despite the fact that the warrant was overbroad); United States v. Hunter, 13 F. Supp. 2d 574, 585 (D. Vt. 1998) (holding that suppression of evidence was not warranted, even when the section of the warrant pertaining to the digital evidence was "impermissibly overbroad").

costs.[153] The judiciary, by contrast, makes its decisions independent of interest groups' influence.[154] Though generally recognized, this distinction between the courts and the legislature is more pronounced in the realm of criminal procedure, and specifically digital evidence searches.[155] With a statutorily diminished voice in legislative affairs, criminals are at a greater danger than most for being victims of democratic failings.

As Donald Dripps has argued, "legislatures systematically undervalue the rights of the accused."[156] This occurs because a majority of the voting public identifies more with crime victims than with criminals. The interests of voters will therefore align with law enforcement, and result in the enactment of greater investigative powers or lesser privacy protections. In the context of computer searches, then, voters will be less likely to identify with those whose computers are searched, and will tend to support rules permitting broader searches. While this trend in criminal procedure may be somewhat mitigated due to the advocacy efforts of technology-oriented interest groups such as internet service providers, their work may ultimately have little effect. Instead, this trend of undervaluing the rights of the accused in criminal procedure may actually become exacerbated when one considers that most computer search cases have arisen in the context of child pornography.[157] Voters are even more likely to support measures that result in the prosecution of child pornographers at great cost to individual rights. Child pornographers are likely the most vilified and marginalized criminals, and consequently, make easy targets for legislators hoping to win votes. Courts, then, will be the institution most likely to generate balanced rules.

---

[153] *See generally* Robert D. Tollison, *Symposium on the Theory of Public Choice*, 74 VA. L. REV. 339 (1988).

[154] *See generally* William M. Landes & Richard A. Posner, *The Independent Judiciary in an Interest Group Perspective*, 18 J.L. & ECON. 875 (1975).

[155] *But see* Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, *supra* note 105, at 884-87 (arguing that public choice insights "have only limited force in the context of criminal procedure rules" because law enforcement interests generally align with the public, as both groups generally advocate for greater enforcement of substantive criminal laws).

[156] Donald A. Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice; Or Why Don't Legislatures Give a Damn About the Rights of the Accused?*, 44 SYRACUSE L. REV. 1079, 1100 (1993).

[157] Clancy, *supra* note 45, at 200; *see also* Ziff, *supra* note 77, at 842.

VI. CONCLUSION

As we increasingly rely on the conveniences of digital technology, courts are ever more frequently confronted with the complex constitutional questions these technologies raise. As many courts have recognized, the application of traditional Fourth Amendment rules to new technology—at least in the context of digital evidence searches—has the potential of eroding the time-honored protections of search warrants. Unless the procedures for executing digital searches evolve to take the differences associated with digital investigations into account, warrants authorizing searches and seizures of digital evidence may become no more of a check on governmental authority than the general warrants the American colonists reviled.

Unfortunately, a satisfactory and universal method of modifying digital search procedures to avoid this outcome does not yet exist. Although courts and scholars have proposed various means of adapting traditional Fourth Amendment rules to digital searches, currently none of the proposals offer a workable, generally applicable rule with sufficient protections. Eventually, such a rule may become a reality. Still, this interim period provides an important opportunity. As the technology continues to change, the factual contexts in which these issues arise will expand and diversify. An exploration of these diverse contexts will provide a better sense of the proper balance between individual privacy and governmental necessity that any rule applying the Fourth Amendment's protections should seek to provide. But until the full contours of the issues presented by digital searches become apparent, courts can and should continue their work, using common law innovation to apply traditional rules in new ways that provide sufficient Fourth Amendment protections to digital technology users. Until a "perfect" solution can be found, these judicially developed rules offer the best protections against the erosion of Fourth Amendment rights in the digital world.