Search Protocols: Establishing the Protections Mandated by the Fourth Amendment Against Unreasonable Searches and Seizures in the World of Electronic Evidence

Derek Haynes*

TABLE OF CONTENTS

* J.D. Candidate, University of the Pacific, McGeorge School of Law, 2009; B.S., Criminal Justice, California State University, Sacramento, 2005. I would like to thank my parents, Sandy LaMendola and Jerry Haynes, as well as Michael Vermillion and Janna Zapara for encouraging me to pursue my goals and offering their unwavering love, patience, and support throughout this process.

I. INTRODUCTION

"'What happened to the Fourth Amendment? Was it repealed somehow?'"[1] Although the Amendment itself has not been repealed, recent decisions by the lower courts have essentially eliminated the protections it was intended to provide to our constitutional right to privacy. Specifically, the problems lie in the application of the Fourth Amendment to electronic evidence. As computers have become a more vital component in our everyday lives,[2] they have developed into an increasingly important source of evidence for investigators.[3] As a result, courts have the unenviable task of applying century-old doctrines to modern-day technology in an attempt to determine the constitutionality of the methods used by law enforcement to extract that information. Unfortunately, by applying the traditional doctrines—which developed in the context of tangible physical evidence—rather than developing new rules to resolve the novel issues associated with electronic evidence, our constitutional right to privacy has all-but been eliminated. The results are alarming.

For example, courts have held that officers have the unbridled authority to open and examine every personal item contained on a suspect's home computer and bring charges based on the information found, even if the officers lacked the initial probable cause to search through all of those items.[4] Even more alarming is a recent decision by the Ninth Circuit. There, the court held that when a warrant is issued authorizing an officer to search the medical records of a single patient, that officer may also, absent individualized suspicion, open and examine the *confidential* medical records for every other patient contained on that same computer.[5] Therefore, every medical patient unlucky enough to visit the same hospital as a person suspected of a crime loses his or her right to privacy.

By relying on these traditional doctrines and granting officers this unprecedented authority, courts are ignoring the very purpose of the Fourth Amendment: to prevent officers from conducting unreasonable exploratory searches.[6] Thankfully, the results have not gone unnoticed. Chief Judge Walter

---

1. United States v. Comprehensive Drug Testing, Inc., 473 F.3d 915, 944 (9th Cir. 2006) (Thomas, J., dissenting) (quoting "[o]ne of the three extremely able district court judges who rejected the governments argument").

2. *See* ERIC NEWBURGER, U.S. CENSUS BUREAU, HOME COMPUTERS AND INTERNET USE IN THE UNITED STATES: AUGUST 2000, at 1-2 (2001), *available at* http://www.census.gov/prod/2001pubs/p23-207.pdf (on file with the *McGeorge Law Review*) (noting that the number of people using a computer and internet at home nearly doubled from 1998 to 2000).

3. G. Robert McLain Jr., United States v. Hill*: A New Rule, But No Clarity for the Rules Governing Computer Searches and Seizures*, 14 GEO. MASON L. REV. 1071, 1071-72 (2007) (discussing how in some instances computers have changed the nature of crimes like child pornography and in other cases the computer has taken the place of pen and paper as a repository for evidence of criminal activity).

4. United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999).

5. *Comprehensive Drug Testing*, 473 F.3d at 944 (Thomas, J., dissenting).

6. *See, e.g.*, Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("By limiting the authorization to search to

Cox of the United States Court of Appeals for the Armed Forces made his plea for a new approach:

> New technologies create interesting challenges to long established legal concepts. Thus, just as when the telephone gained nationwide use and acceptance, when automobiles became the established mode of transportation, and when cellular telephones came into widespread use, now personal computers, hooked up to large networks, are so widely used that the scope of the Fourth Amendment core concepts of "privacy" as applied to them must be reexamined.[7]

Courts have been slow to recognize the need for reform and now the Advisory Committee for the Federal Rules of Criminal Procedure should step in to protect our constitutional right to privacy and bring clarity to this splintered area of constitutional law. Specifically, the Advisory Committee should propose an amendment to the Federal Rules of Criminal Procedure that would make search protocols[8] mandatory in every application for a warrant involving electronic evidence. In the search protocol, officers should be required to provide a detailed description of the evidence they hope to uncover and the methods they will use to search through and target that information. Then, before the warrant is issued, the court should be required to make an independent determination regarding the reasonableness of the officers' proposed conduct and ensure that a proper balance is struck between the individual's right to privacy and the government's interests in effective law enforcement.

This Comment is broken into four parts. Part II starts by exploring the traditional rules governing search and seizure and how the courts have applied these rules to electronic evidence. Part III illustrates why, in the context of electronic evidence, the traditional rules fail to provide sufficient protections against unreasonable searches and seizures. Part IV discusses some of the attempts made by lower courts to correct this problem and why the rules they developed are inadequate. Finally, Part V proposes a solution to the problem.

II. THE CURRENT APPROACH

A. Traditional Doctrines Governing Search and Seizure

The Fourth Amendment guarantees the right of all citizens to be free from "unreasonable" searches and seizures.[9] Courts determine whether a search or seizure

---

the specific areas and things for which there is probable cause to search[,] . . . [it] ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.").

7. United States v. Maxwell, 45 M.J. 406, 410 (C.A.A.F. 1996).

8. A search protocol describes, with specificity, the evidence the officers will seize and the methods they will use to search for that evidence without unnecessarily opening and examining irrelevant information.

9. U.S. CONST. amend. IV.

is reasonable on a case-by-case basis by balancing the government's interest in effective law enforcement against the severity of the intrusion on the individual's Fourth Amendment right to privacy.[10] As a result, the reasonableness of police conduct will vary depending on the government's need and the severity of the intrusion involved.[11]

To balance these interests appropriately and protect against unreasonable searches and seizures, officers must comply with a series of procedural requirements. The first of these procedures is the warrant requirement. Subject to a few narrow exceptions, officers must obtain a valid warrant before conducting a search or seizure.[12] For a warrant to be valid it must be: (1) issued by a neutral and disinterested magistrate;[13] (2) supported by probable cause to believe that the evidence sought will aid in the apprehension or conviction for a particular offense;[14] and (3) describe, with particularity, the places to be searched and the items to be seized.[15]

In addition to obtaining a valid warrant, the Fourth Amendment also mandates that officers act reasonably throughout the execution of that warrant.[16] If the officers act unreasonably, courts will generally suppress the evidence the officers seized.[17] Specifically, for the search to be reasonable, officers must limit the scope of their search to the areas where the items they are looking for may

---

10. *See* New Jersey v. T.L.O, 469 U.S. 325, 337-42 (1985) ("On one side of the balance 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.").

11. *Id.*

12. *See* Katz v. United States, 389 U.S. 347, 357 (1967) (noting that, absent a few exceptions, searches done without prior judicial approval are per se unreasonable even if there was probable cause to support the belief that evidence of a crime would be found).

13. Johnson v. United States, 333 U.S. 10, 14-15 (1948) (stating that it is the job of "the neutral and detached magistrate" to determine whether there is sufficient evidence to warrant an intrusion into a person's privacy because granting that authority to a neutral individual rather than the interested officer helps establish the proper balance between the interest of law enforcement and those of the individual).

14. Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.").

15. *Id.*; *see also* Marron v. United States, 275 U.S. 192, 196 (1927) (requiring the description of the items to be detailed enough that "nothing is left to the discretion of the officer executing the warrant"); United States v. Stefonek, 179 F.3d 1030, 1033 (7th Cir. 1999) (stating that the rationale behind requiring a particularized description is to protect against an overly-intrusive invasion of an individual's privacy that is beyond what is necessary to achieve a valid law enforcement purpose).

16. *See, e.g.*, United States v. Ross, 456 U.S. 798, 820-21 (1982) (noting that a lawful search under the Fourth Amendment extends just to the places where it would be reasonable to believe the items described in the warrant may be located).

17. *See, e.g.*, Mapp v. Ohio, 367 U.S. 643, 649 (1961) ("'The striking outcome of the Weeks case and those which followed it was the sweeping declaration that the Fourth Amendment, although not referring to or limiting the use of evidence in court, really forbade its introduction if obtained by government officers through a violation of the amendment.'" (quoting Olmstead v. United States, 277 U.S. 438, 462 (1928))).

reasonably be located.[18] Imposing that limitation protects the individual's right to privacy by preventing a general exploratory search through all of the individual's belongings, while still meeting the needs of law enforcement by allowing the officers to target the lawful object of their search. As a result, the mandatory Fourth Amendment balance is struck.

B. Applying Traditional Doctrines to Electronic Evidence

While limiting the scope of a search to the areas where the items listed in the warrant may reasonably be located may protect against overly intrusive police conduct in the context of physical evidence,[19] applying that "limitation" to electronic evidence invites, rather than prevents, a general exploratory search.[20]

For example, in *United States v. Walser*, the magistrate issued a warrant authorizing the officers to search a suspect's computer for any information linking him to suspected drug activity.[21] During the initial search, one of the officers came across a file containing a thumbnailed[22] picture of what he suspected was illegal sexual activity.[23] Even though the warrant only authorized the officer to search for information pertaining to illegal drug-activity, he decided to open the picture anyway.[24] At trial, the defendant filed a motion to suppress, arguing that the officer violated his Fourth Amendment rights by opening a file that fell beyond the scope of the warrant.[25] In denying the motion, the court explained that relevant electronic information can potentially be anywhere on a computer and therefore officers must have the authority to open and examine every document.[26] As a result, the court essentially gave officers the authority to conduct general exploratory searches of every personal item contained on personal home computers, even if they lack the requisite probable cause for each individual item.

---

18. *See, e.g.*, *Garrison*, 480 U.S. at 84 (explaining that a warrant establishing probable cause that a stolen lawnmower may be found in the garage would not authorize a search of the upstairs bedroom); People v. Harmon, 413 N.E.2d 467, 470 (Ill. App. Ct. 1980) (noting that the appellate court overturned the defendant's conviction for stealing a CB radio because the officers went beyond the scope of the warrant and violated the Fourth Amendment when they searched inside the back of the defendant's television despite the warrant's limitation that the officers only look where it is reasonable to conclude that railroad jacks, forks, and switch brooms would be located).

19. *Ross*, 456 U.S. at 820-21.

20. *See* Rosa v. Commonwealth of Virginia, 628 S.E.2d 92, 98-102 (Va. Ct. App. 2006) (noting that the scope "of a search extends to every place where the object of the search may reasonably be found" and that an officer may open up every file in a computer to determine its relevance).

21. United States v. Walser, 275 F.3d 981, 983 (10th Cir. 2001).

22. *See* Kristin Richards, Comment, *Evolution in Slow Motion: Opting into a Digital World*, 29 HASTINGS COMM. & ENT. L.J. 447, 453 (2007) (describing a thumbnail as a small item that when clicked, will link to the larger, visible version of the picture).

23. *Walser*, 275 F.3d at 984-85.

24. *Id.* at 985.

25. *Id.* at 986-87.

26. *Id.*

United States v. Gray is another example of the inadequacy of traditional doctrines when applied to electronic evidence. In *Gray*, the court issued a warrant authorizing an officer to search for evidence implicating Gray in a computer-hacking scheme involving text-based government documents.[27] However, rather than limiting the examination to text files,[28] the officer took it upon himself to open a picture file that was entirely unrelated to the hacking-scheme.[29] Relying on the information contained in that picture, the officer then applied for, and received, an additional warrant to search through the rest of Gray's belongings.[30] At trial, the court denied Gray's motion to suppress the pictures, explaining that an electronic document could potentially be housed anywhere and therefore officers have the authority to open and examine every file contained on a computer.[31]

C. *Insufficient Limitation*

As both *Walser* and *Gray* indicate, a digital document, unlike a physical item, can be stored anywhere on a computer, regardless of its size. While it would be unreasonable for an officer to open up a shoebox while looking for a stolen stereo, a digital document can potentially be stored anywhere inside the library-sized storage capacity of a computer. Thus, while a proper balance between effective law enforcement and privacy may be achieved by limiting the scope of a search to areas where physical items may reasonably be located, applying that same rule to electronic evidence permits a search of every personal item contained on a computer. As a result, when courts apply the traditional doctrines governing searches and seizures of tangible physical documents to electronic evidence, the public's privacy interests go unprotected because the officers may conduct a general exploratory search.

III. TRADITIONAL DOCTRINES FAIL TO ESTABLISH THE BALANCE MANDATED BY THE FOURTH AMENDMENT

The Fourth Amendment to the United States Constitution provides:

> 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

27. United States v. Gray, 78 F. Supp. 2d 524, 526 (E.D. Va. 1999).
28. *Id.*
29. *Id.*
30. *Id.* at 528.
31. *Id.*

> or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[32]

The Supreme Court has held that reasonableness under the Fourth Amendment is based on a sliding scale, balancing the need for effective law enforcement against the severity of the intrusion on an individual's right to privacy.[33] Accordingly, as privacy interests increase, the intrusiveness of the search should correspondingly decrease.[34] However, under the current approach employed by the courts, that balance is lost.

A. Heightened Privacy Interests in Electronic Evidence

The privacy interests involved with electronic evidence far exceed those associated with traditional searches for tangible physical items. First, consider that the storage capacity of an average desktop computer is 109 gigabytes, the equivalent of a library full of academic journals.[35] Next, think about the role that computers play in our lives and the variety of information they contain. While at the outset computers were nothing more than a replacement for the common typewriter, today they have become "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more."[36] With the massive storage capacity and the variety of information stored on modern-day computers, our interests in keeping that information secure have never been greater. With just a few clicks, an intruder can access all of one's financial information, personal contacts, and deepest thoughts.

Unfortunately, not only do the unique characteristics of computers increase the need to protect computers against unlawful intrusion, these unique characteristics actually make it more likely that an unlawful intrusion will occur.[37] For example, compare a search of a home for physical evidence to one involving electronic information. First, before searching a home for physical evidence, officers must organize into a team and receive special training for the operation.[38] After training for the operation, the entire team of officers must go to the location specified in the affidavit to execute the warrant,[39] then, as dictated by

---

32. U.S. CONST. amend. IV.

33. New Jersey v. T.L.O., 469 U.S. 325, 337 (1985).

34. *See id.* (holding that a balance is supposed to be struck between the competing interests based on the specific circumstances surrounding the case).

35. Benjamin D. Silbert, Comment, *The 2006 Amendments to the Rules of Civil Procedure: Accessible and Inaccessible Electronic Information Storage Devices, Why Parties Should Store Electronic Information in Accessible Formats*, 13 Rich. J. L. & Tech. 14, 1 (2007).

36. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005).

37. *Id.*

38. *Id.*

39. *Id.*

standard procedures, all of the officers must stay on location until the search is complete.[40] As a result, while it is possible for officers to conduct a complete and comprehensive search of a home for physical evidence, the amount of planning, preparation, and manpower required for such an operation means that it rarely actually happens.[41]

Unlike the time-consuming and burdensome process of searching a home for physical evidence, it is much easier to search a computer for electronic evidence. The manpower is minimal; it only takes one analyst to perform a complete and comprehensive search. Additionally, since officers do not search the computer until it is back at the station, they have an extended amount of time to operate.[42] Because reasonableness, and thus the constitutionality of a search and seizure, is based on balancing the government's interest in law enforcement against the severity of the privacy intrusion in the particular case, courts must consider these unique characteristics of electronic evidence.[43] Unfortunately, courts have struggled with this task and, as a result, our right to privacy has suffered.

B. Meeting the Needs of Law Enforcement

Although modern technology increases the risk of overly intrusive police conduct, it may also provide the key to meeting the needs of law enforcement while still protecting our privacy interests.[44] Technology enables officers to seize relevant information while avoiding unnecessary privacy intrusions by directly targeting the legitimate objects of the search for which they have demonstrated probable cause.[45]

First, consider the process involved with searching a file cabinet for physical, hard-copy documents. A typical file cabinet, like a computer, will house both relevant and irrelevant documents. Unfortunately, the only way for an officer to determine whether a specific physical document is relevant to the case is by performing a cursory examination of each item.[46] As a result, officers have the authority to conduct these cursory inspections because it is the only way they can meet their needs of effective law enforcement.[47]

While the very nature of a file cabinet full of tangible physical documents requires an officer to perform a cursory inspection of each item, electronic

---

40. *Id.*

41. *Id.*

42. *Id.*

43. New Jersey v. T.L.O, 469 U.S. 325, 337-42 (1985).

44. *See In re* Search of 3817 W. West End, 321 F. Supp. 2d 953, 959 (N.D. Ill. 2004) ("[C]omputers also present the tools to refine searches in ways that cannot be done with hard copy files.").

45. *See id.* ("[C]omputer technology affords a variety of methods by which the government may tailor a search to target on the documents which evidence the alleged criminal activity.").

46. Andersen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

47. *Id.*

evidence is different. With the use of modern technology, officers have the opportunity to tailor their search in a way that prevents an unnecessary intrusion while still targeting the specific documents for which probable cause has been established.[48] Some of the methods for targeting these documents include: keyword searches, limitations on the specific software programs or file types, and even restricting the search based on the date a document was created or last opened.[49] While no single method will work in every case, the fact that these tools are available "demonstrates the ability of the government to be more targeted in its review of computer information than it can be when reviewing hard copy documents or file cabinets."[50] Given that courts consider the specific circumstances of an individual case when determining the reasonableness of the intrusion, authorities should mandate the use of the limitations made available through modern technology rather than relying on the traditional doctrines that allow for general exploratory searches.[51]

Given the heightened privacy interests associated with electronic evidence, the likelihood of an overly intrusive invasion, and the unnecessary use of cursory inspections, it is unreasonable under the Fourth Amendment for the courts to continue granting officers the authority to open and examine every piece of electronic information on a personal computer.

IV. RESPONDING TO THE INADEQUACIES OF TRADITIONAL DOCTRINES

A. Recognizing the Need for a Special Approach

Developing new rules tailored to the unique issues associated with electronic evidence is not a novel concept. In fact, the Supreme Court, Congress, prominent judges, lawyers, and law professors have all agreed that the procedures governing physical information are simply inadequate when applied to electronic information. As a result, the Advisory Committee on the Federal Rules of Civil Procedure amended the rules in December of 2006 to account for these insufficiencies.[52] While the new rules dealt with the pre-trial discovery of electronic information, the concerns that led to the amendments are the same as those presented in searches and seizures of electronic evidence in criminal investigations. Specifically, the Advisory Committee pointed to some important differences between electronic information and information stored in hard-copy documents,[53] including the potential volume of information contained on a

48. *In re Search*, 321 F. Supp. 2d at 959.

49. United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999).

50. *In re Search*, 321 F.Supp.2d at 959.

51. New Jersey v. T.L.O., 469 U.S. 325, 337-42 (1985).

52. *See generally* FED. R. CIV. P. 16, 26, 33, 34, 37, 45 (adopting new, specialized rules governing the pre-trial discovery procedures for electronic information).

53. *See* Memorandum from Advisory Committee on Federal Rules of Civil Procedure, to Committee on

computer,[54] the difficulty that arises when trying to locate relevant information,[55] and the potential burdens imposed on the aggrieved party if a person searches through all of the information contained on their computer.[56] As a result, the Advisory Committee amended the rules to reestablish the proper balance between the needs and interests of the parties involved.[57]

Although the amendments to the Federal Rules of Civil Procedure deal with electronic information in the context of civil pre-trial discovery,[58] the principle applies equally to criminal investigation: new procedures are necessary to deal with the unique problems associated with electronic information. It is time for the Committee on the Federal Rules of Criminal Procedure to extend the reasoning behind the amendments to the Federal Rules of Civil Procedure to the criminal context. Unfortunately, until the Committee amends the rules, the public's privacy interests will continue to suffer.

B. The First Step

Although insufficient in scope, some specialized procedures have developed in response to the inherent differences between digital and physical evidence.[59] For physical evidence, officers typically go to the location described in the warrant, search for the items listed, and then seize the relevant items found.[60] But, there is an additional step when the warrant involves electronic evidence.[61] After the officers establish probable cause for electronic evidence, the court issues a warrant authorizing the officers to search for and seize the computer containing the relevant electronic evidence.[62] At this point, the officers do not search through the computer to determine which documents are relevant to their case.[63] Instead, the officers wait until the computer is back at the station, and only

---

Rules of Practice and Procedure 18 (May 7, 2005), *available at* http://www.uscourts.gov/rules/Reports/CV5-2005.pdf [hereinafter *Advisory Committee Memo*] (on file with the *McGeorge Law Review*) (explaining that "electronically stored information has important differences from information recorded on paper," including the volume of information that people generally store on their computers).

54. *Id.*

55. *Id.* at 23.

56. *Id.* (explaining that electronic information is "often voluminous and dispersed, [and] can be burdensome to locate and review).

57. *See id.* at 34 (explaining that Rule 26(f) will help promote a balance between one party's interest in preserving electronic evidence that is relevant to his or her case and the opposing party's interest in being able to continue operations).

58. *See id.* at 1 (explaining that rules 16, 26, 33, 34, 37 and 45 address discovery of electronically stored information).

59. United States v. Hill, 322 F. Supp. 2d 1081, 1089-90 (C.D. Cal. 2005).

60. Amy Baron-Evans & Martin F. Murphy, *The Fourth Amendment in the Digital Age: Some Basics on Computer Searches*, 47 B. B. J. 10, 11 (2003).

61. Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 90 (2005).

62. *Id.*

63. *Id.*

then do they turn it on and begin the process of searching for relevant information.[64]

While some people argue that this procedure is overly intrusive because it allows the officers to seize the entire device rather than just the relevant information, courts have held that the intrusion is less severe than it would be if the officers searched the computer on-site.[65] These courts explain that a full and comprehensive search of a computer requires officers to "examine every one of what may be thousands of files on a disk[,] . . . [which] could take many hours or perhaps days."[66] This means that if officers search the computer on-site, rather than back at the station, they would inevitably intrude on the individual's personal space for the duration of the search. As a result, granting officers the authority to search the computers off-site reduces the privacy intrusion while still allowing officers to access the relevant information.[67] Although courts recognize that this specialized approach is a step in the right direction, this alone is not enough to reestablish the balance mandated by the Fourth Amendment.

C. Going Further

Some courts have recognized the need for an expanded set of procedures to govern electronic evidence,[68] but the rulings set forth by these courts have been insufficient and inconsistent.

1. The Tenth Circuit's Approach

In *Unites States v. Carey*, the Tenth Circuit set forth its own unique approach for searches of electronic evidence.[69] However, the court ignored the language of the Fourth Amendment and years of Supreme Court precedent by holding that the constitutionality of a search for electronic evidence depends on the subjective intent of the officer conducting the search.[70] In other words, as long as the officer does not intend to exceed the scope of the warrant, there is no violation of the Fourth Amendment. However, the language of the Fourth Amendment does not support a test based on the subjective intent of an officer.[71] In fact, the words

---

64. *Id.*

65. United States v. Hill, 322 F. Supp. 2d 1081, 1089-90 (C.D. Cal. 2005).

66. *Id.* at 1089.

67. *Id.* at 1089-90.

68. *See* United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (stating that courts have to look at the subjective intent of the officer when determining the constitutionality of Fourth Amendment intrusion).

69. *Id.*

70. *See id.* (stating that "until he opened the first JPG file, he stated he did not suspect he would find child pornography" and because "he inadvertently discovered the first image during the search for documents relating to drug activity, our holding is confined to the subsequent opening of numerous files the officer . . . expected, would contain images of child pornography").

71. Scott v. United States, 436 U.S. 128, 137 (1978).

specifically forbid "unreasonable" searches and seizures.[72] The Supreme Court has made it clear that reasonableness is based an objective standard.[73] The Court explained that a rule relying on the subjective intent of an officer to determine the reasonableness of a search and seizure would strip away the entire meaning of the Fourth Amendment.[74] In addition, a subjective standard would cause inconsistent rulings that depend entirely on the specific officer conducting the search. Therefore, the special approach established by the Tenth Circuit is in direct conflict with the Fourth Amendment and fails to establish the mandatory balance between privacy interests and effective law enforcement.

2. A District Court's Approach

The United States District Court for the Northern District of Illinois also recognized the need to adopt specialized rules for electronic evidence. While investigating a suspect for alleged tax fraud, officers applied for a warrant to search through *all* of the electronic information contained on the suspect's computer.[75] Recognizing the need to protect the heightened privacy interests inherent in electronic evidence,[76] the court granted the warrant to seize the computer but held that the officers could not search the data until they provided a search protocol defining the methods they were going to use to search through the information.[77]

While the court held that mandating the use of a search protocol was necessary under the Fourth Amendment,[78] it failed to consider the unnecessary burdens that result from granting the officers a warrant to seize the computer, yet denying them the opportunity to search the information until a later date. Not only does this delay the officers' investigation, but it also strips the aggrieved party of their property for an extended period of time without any confirmation that it does in fact contain relevant evidence. For example, in this case, the computer was seized on May 1st,[79] but the officers were unable to search the information (i.e., the suspect was without his property) until the search protocol was scheduled for review forty-eight days later.[80] Therefore, while the court protected the individual's privacy interests by preventing a general rummaging through of all of the electronic data by mandating a search protocol, the

72. U.S. CONST. amend. IV.

73. Terry v. Ohio, 392 U.S. 1, 21-22 (1968).

74. *Id.*

75. *In re* Search of 3817 W. West End, 321 F. Supp. 2d 953, 955 (N.D. Ill. 2004).

76. *Id.* at 958-59 (explaining that computers have an enormous storage capacity and the characteristics of computers increase the likelihood that documents will be intermingled).

77. *Id.* at 955-56.

78. *Id.*

79. *Id.* at 956.

80. *Id.* at 963.

implementation of the process resulted in unnecessary burdens for both the police department and the owner of the property.

3. The Ninth Circuit's Approach

One of the most alarming opinions concerning the applicability of the Fourth Amendment to electronic evidence is the recent decision by the Ninth Circuit in *United States v. Comprehensive Drug Testing, Inc*. The case arose out of the federal government's investigation of the Bay Area Lab Cooperative (Balco) for allegedly distributing illegal steroids to Major League Baseball (MLB) players.[81] During the investigation, officers discovered that the MLB had a drug-testing program that a company called Comprehensive Drug Testing (CDT) was responsible for administering.[82] Hoping to discover information relating to the pre-existing Balco investigation, the officers applied for, and were granted, a warrant to search CDT for the medical records of eleven specifically-named MLB players.[83] However, rather than limiting their search to just those eleven players, the officers seized, and eventually searched through, the electronic medical records of thousands of professional athletes and private individuals.[84] Arguing that the officers went beyond the scope of the warrant, the MLB Players' Association filed a motion demanding that the officers return the medical records for every person not named in the initial warrant.[85] The District Court of Nevada agreed and ordered the officers to return the documents.[86]

On appeal, the Ninth Circuit overruled the district court's decision, holding that the officers acted reasonably and that they therefore were not required to return any of the information.[87] In coming to that conclusion, the court relied on the dicta from *United States v. Tamura*, a case involving hard-copy documents.[88] According to *Tamura*, when presented with a stack of documents containing both relevant and irrelevant information, officers have two options: either wait for a judge's approval or develop their own set of procedures for searching through and seizing the documents.[89] Relying on *Tamura*, the Ninth Circuit held that it was reasonable for the officers to seize all of the medical records because they had a set of procedures in place to help them identify which information was relevant.[90]

---

81. United States v. Comprehensive Drug Testing, Inc., 473 F.3d 915, 919 (9th Cir. 2006).
82. *Id.* at 920.
83. *Id.* at 944 (Thomas, J., dissenting).
84. *Id.*
85. *Id.* at 923 (majority opinion).
86. *Id.* at 924.
87. *Id.* at 937.
88. *Id.* at 933.
89. United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir. 1982).
90. *Comprehensive Drug Testing*, 473 F.3d at 933.

After the court held that the officers acted reasonably in seizing all of the electronic medical records, it turned to the second issue: how to search through the information without violating the Fourth Amendment.[91] Relying again on the dicta from *Tamura*, the Ninth Circuit established a series of guidelines for officers to follow.[92] The court explained that officers may search through the information, without limitation, unless the aggrieved party asks the court to intervene and oversee the search.[93] If the party does request judicial supervision, and the court agrees that supervision is necessary, a neutral magistrate is appointed to oversee the search.[94]

The problems with this approach are twofold. First, while judicial supervision may help protect against unreasonable searches and seizures in theory, the strain it would place on the judiciary makes such an approach entirely impractical. Judges simply do not have the time to supervise every electronic search given the prevalence of computers[95] and the amount of time it takes to perform a comprehensive search.[96] Secondly, the court's explanation of how the process would work calls into question the entire basis for the ruling. Although the court spoke strongly about protecting privacy interests through judicial supervision,[97] it went on to make that requirement nothing more than a window-dressing for what would in effect authorize officers to perform general exploratory searches in violation of the Fourth Amendment. The court explained that even if the supervising magistrate determines that some of the documents seized by the officers fall beyond the scope of the warrant, the officers must only return those documents to the aggrieved party *temporarily* because "the government is always free to seek . . . [a] subsequent search warrant[] . . . to justify expansion of the investigation upon proper showing of any item's relevancy to suspected criminal behavior uncovered during review of the evidence initially seized."[98] In other words, even if the officers exceed the scope of the initial warrant by searching through evidence for which there was no probable cause, they can still use the information obtained during that unlawful search as the basis for a subsequent warrant.[99] This result is anything but "reasonable" under the Fourth Amendment, and it does nothing more than authorize general exploratory searches.

---

91. *Id.* at 938.

92. *Id.* at 938-39.

93. *Id.* at 939.

94. *Id.*

95. *See* NEWBURGER, *supra* note 2, at 2 (noting that the average number of people using computers and the internet doubled from 1998 to 2000 to include over sixty percent of society).

96. *See* United States v. Hill, 322 F. Supp. 2d 1081, 1089-90 (C.D. Cal. 2005) (stating that it could take hours or even days to conduct a comprehensive search).

97. *Comprehensive Drug Testing*, 473 F.3d at 939-40.

98. *Id.* at 940.

99. *Id.*

V. REESTABLISHING THE FOURTH AMENDMENT'S MANDATORY BALANCE

A. A Proposed Solution

Just as Chief Judge Walter Cox explained, as technology continues to advance, so too does the need to reexamine the applicability of the Fourth Amendment.[100] Unfortunately, the courts have been slow to recognize the need for reform. As a result, the Advisory Committee on the Federal Rules of Criminal Procedure should step in and provide some direction to this fractured area of Fourth Amendment law. Specifically, the Federal Rules of Criminal Procedure should be amended to make search protocols mandatory in every case involving electronic evidence.

While the specifics of the search protocol will vary depending on the case, they should all include the same basic components: (1) a detailed description of the electronic evidence sought by the officers and (2) the methods they will use to search for and seize that information. Then, before issuing a warrant, a court must make an independent determination that the protocol is narrow enough to protect against an unreasonable search and seizure. In assessing the sufficiency of the protocol provided by the officers, courts should rely on the same "particularity" requirement that governs a search and seizure of physical evidence.[101] Specifically, the officers must describe the evidence they hope to uncover with sufficient particularity such that "nothing is left to the discretion of the officer executing the warrant."[102] While there are a variety of different methods for searching through the information, no single method is appropriate for every case. Therefore, whether the search method is reasonable will depend on the circumstances of the given case.

1. Keyword Searches

One of the oldest and most familiar search methods is an automated search using keywords. Keyword searches are a particularly useful method when the inquiry focuses on specific documents and the language used is relatively predictable.[103] "For example, keyword searches work well to find documents that mention a specific individual or date, regardless of the context."[104] However,

---

100. United States v. Maxwell, 45 M.J. 406, 410 (C.A.A.F. 1996).

101. Marron v. United States, 275 U.S. 192, 196 (1927) (noting that the description should be particularized such that nothing is left to the discretion of the officer executing it).

102. *Id.*

103. *The Sedona Conference Best Practices Commentary on the Use of Search and Retrieval Methods in E-Discovery*, 8 SEDONA CONF. J. 189, 201-02 (2005); *see also* UNITED STATES DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTER AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 96 (2002), *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm (on file with the *McGeorge Law Review*) (discussing the kinds of cases where keyword searches are particularly useful).

104. *Sedona Conference*, *supra* note 103, at 201.

beyond that, there are new programs that use specific phrases or concepts and then identify every document containing information relevant to those items.[105] As a result, officers can narrow the search to those documents containing information that is relevant to those phrases or concepts rather than opening and examining every document.

2. Metadata

Metadata is another valuable way to limit the scope of a search without unduly burdening the government's interests in effective law enforcement. Metadata is information that a computer automatically stores about every document or file contained on its hard-drive.[106] Some of the information captured by the computer includes: the date a document is created; if and when someone modified the document; the specific information that was modified; the date the document was printed; and even who created that document.[107] By using this information, officers can locate the items relevant to their investigation without conducting a general exploratory search through all of the documents contained on the computer.

B. Reestablishing a Magistrate as the Neutral Arbiter

Not only do search protocols prevent overly intrusive searches and seizures, they also reestablish the role of a magistrate as the neutral arbiter responsible for determining the constitutionality of police conduct. Currently, without search protocols, officers have the broad discretion to set the parameters for their own search.[108] This limits the ability of a magistrate to screen out unreasonable searches and seizures in advance,[109] and the protection of privacy interests is left to the discretion of the officers engaged in the "often competitive enterprise of ferreting out crime."[110] By mandating that officers include a search protocol along with their application for the warrant, courts will once again be in a position to screen out unreasonable searches and seizures and protect our constitutional right to privacy.

C. Gaining Support for Search Protocols

The U.S. Department of Justice (DOJ) issued a report that recognized the potential benefits of mandating the use of search protocols in cases involving

105. *Id.*

106. *Id.*

107. J. Brian Beckham, *Production, Preservation and Disclosure of Metadata*, 7 COLUM. SCI. & TECH. L. REV. 1, 11 (2006).

108. United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999).

109. Johnson v. United States, 333 U.S. 10, 14 (1948).

110. *Id.*

electronic evidence.[111] Based on the intermingled nature of electronic information, the DOJ explained that it can be very difficult for officers to locate relevant information amidst the unrelated data generally found on a computer.[112] As a result, the DOJ recommends that officers establish search protocols detailing how they will limit their search to prevent an overly intrusive infringement on a person's privacy interests.[113] Specifically, "[w]hen agents have a factual basis for . . . locat[ing] the evidence[,] . . . the affidavit should explain the techniques that the agents plan to use to distinguish incriminating documents from commingled documents."[114]

D. Dispensing with the Counterarguments

Over the last couple of years, courts and commentators have made several arguments for why search protocols are unnecessary. These arguments range from insisting that traditional doctrines offer sufficient protections and therefore a new approach is unnecessary,[115] to admitting the need for a new approach but refusing to adopt search protocols.[116] However, after reviewing these arguments it is clear that they are based on a very basic misunderstanding of electronic evidence and the purpose behind search protocols.

1. Traditional Doctrines Are Sufficient

Some commentators argue that special rules governing electronic evidence are entirely unnecessary because the traditional doctrines governing searches and seizures of physical documents offer sufficient protections.[117] Commentators base this argument on the premise that electronic evidence is *not* fundamentally different from physical evidence and, therefore, courts should simply apply the same rules in both situations.[118] However, that premise is clearly flawed given the decision by the Advisory Committee on the Federal Rules of Civil Procedure to amend the rules.[119] As discussed earlier in this Comment, the Advisory Committee amended the Federal Rules of Civil Procedure because electronic evidence *is* fundamentally different from physical evidence.[120] Therefore, to

---

111. UNITED STATES DEPARTMENT OF JUSTICE, *supra* note 103, at 1.

112. *Id.*

113. *Id.*

114. *Id.*

115. Thomas Clancey, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and Priner*, 75 MISS. L.J. 193, 205 (2005).

116. *Id.* at 213-14.

117. *Id.* at 205-06.

118. *Id.*

119. Salvatore Joseph Bauccio, *E-Discovery: Why and How E-mail Is Changing the Way Trials Are Won and Lost*, 45 DUQ. L. REV. 269, 269-70 (2007).

120. *Id.*

argue that they are not fundamentally different ignores the developments in other areas of the law.

2. The Contents of a Document Can Only Be Determined by Looking at It

Some courts refuse to adopt search protocols by arguing that the only way to determine the content of a particular document is by opening and examining it.[121] However, this argument fails to understand the purpose and benefits of mandating the use of search protocols. Search protocols do not, and are not meant to, determine what information is contained in every document. They are simply methods for excluding irrelevant information from the scope of the search. For example, if officers establish probable cause to believe that Jack's computer contains pictures of a robbery that took place on August 11th, a court may utilize metadata to devise a search protocol that limits the scope of the search to documents created after August 11th. In that situation, officers do not have to look at the contents of the documents created before August 11th to determine that they fall outside the scope of the warrant.

3. Officers Do Not Have to Use the Least Intrusive Means

Some courts refuse to adopt search protocols based on the Supreme Court's ruling in *United States v. Sharpe*, which held that officers do not have to use the least intrusive means when conducting a search.[122] However, that argument is based on a basic misunderstanding of the Supreme Court's decision in *Sharpe*. In *Sharpe*, the Supreme Court explained that officers do not have to use the least intrusive means because "[a] creative judge engaged in *post hoc* evaluation of police conduct can almost always imagine some alternative means by which the objectives of the police might have been accomplished."[123] However, there is no "post hoc evaluation" with search protocols.[124] Courts determine whether the search method is reasonable before the warrant is even issued. Therefore, relying on the Supreme Court's decision not to require the use of the least intrusive means as the basis for rejecting the use of search protocols is ill-founded and fails to consider the underlying purpose for the Supreme Court's ruling.

121. United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999).

122. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 663 (1995); Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 453-54 (1990); United States v. Sokolow, 490 U.S. 1, 10-11 (1989); Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 629 n.9 (1989).

123. United States v. Sharpe, 470 U.S. 675, 686-87 (1985).

124. *Id.*

VI. CONCLUSION

Over the past several years, computers have developed into one of our most private possessions. With just a few clicks, an intruder can access a digital blueprint of who we are: financial information, daily planners, pictures, and some of our deepest thoughts.[125] However, according to a few recent decisions by the lower courts, the Constitution does not protect that information against an arbitrary and comprehensive invasion.[126] The courts reason that traditional doctrines governing searches and seizures allow officers to search in every location that an item may reasonably be located, and therefore, because an electronic document can be located anywhere on a computer, officers may open every document. [127] By applying these traditional doctrines to modern technology, courts have lost sight of the true purpose of the Fourth Amendment: to protect against unreasonable searches and seizures.[128] As a result, to protect our rights and bring clarity to this developing area of constitutional law, new rules should be developed to guide the application of the Fourth Amendment to electronic evidence.

Specifically, the Advisory Committee on the Federal Rules of Criminal Procedure should take the lead and propose an amendment to the Federal Rules that mandates search protocols in every case involving electronic evidence. As the Supreme Court explains, the reasonableness of a search and seizure is determined on a case-by-case basis.[129] If privacy interests increase in a particular case, the intrusiveness of police conduct should correspondingly decrease.[130] Therefore, with the heightened privacy interests associated with electronic evidence, the officers should be required to reduce the intrusiveness of their search. However, that does not mean that the search has to be any less effective. Modern technology, whether it be keywords or metadata, can actually make an officer's search of electronic information even more effective while still protecting the privacy interests of the individual.[131] Unfortunately, the courts continue to ignore the availability of these options, and until something changes, our privacy interests will continue to suffer.

---

125. Kerr, *supra* note 36, at 569.

126. United States v. Walser, 275 F.3d 981, 986-87 (10th Cir. 2001).

127. *Id.*

128. *See, e.g.*, Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("[L]imiting the authorization to search to the specific areas and things for which there is probable cause to search . . . ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.").

129. New Jersey v. T.L.O., 469 U.S. 325, 337 (1985).

130. *See id.* at 337 (holding that a balance is supposed to be struck between the competing interests based on the specific circumstances surrounding the case).

131. *See In re* Search of 3817 W. West End, 321 F. Supp. 2d 953, 959 (N.D. Ill. 2004) ("[C]omputer technology affords a variety of methods by which the government may tailor a search to target on the documents which evidence the alleged criminal activity.").