Cleveland State Law Review

Volume 48
Issue 1 *Symposium: Re-Orienting Law and Sexuality*

Note

2000

Computer Searches and Seizure

Donald Resseguie

COMPUTER SEARCHES AND SEIZURE

I. INTRODUCTION 185
II. CONSTITUTIONAL LIMITATIONS ON SEARCHES AND SEIZURES 186
III. THE PLAIN VIEW DOCTRINE 190
IV. INFORMANTS 198
V. SCOPE OF SEARCH AND SEIZURE AND PARTICULARITY OF WARRANTS 203
A. The Closed Container Analogy & Particularity of Warrants 203
B. The Problem of Intermingled Documents 205
VI. THE SUBPOENA PROCESS 210
VII. CONCLUSION 212

I. INTRODUCTION

Computers have become a principal means for storing both personal and business information for large numbers of people. In addition, with the increasing use of the Internet and e-mail many people use computers as a means of accessing information and communicating with others both in personal and business contexts. People increasingly store and manipulate accounting and business records with computer systems. At the same time, commercially available computerized accounting software has dropped significantly in price and has become increasingly easy to use. At one time, maintaining a detailed and accurate set of accounting records was beyond the ability of all but well trained and experienced professionals. Today, however, persons with little or no accounting or business background are able competently to maintain their business and accounting records. The trend is one of greater availability and constantly dropping prices. As this trend continues, we will see an increased use of computers by all sectors of the population. Along with the use of computerized record keeping and communication in legitimate enterprise has come the use of the same technology by criminal enterprises in carrying out their activities.

As a result of this trend, computer storage devices have increasingly become the targets of government investigations of criminal activity. The government has used evidence gathered from computers countless times in criminal prosecutions. The methods by which government officials seek to gather evidence from computers couple with the limits placed on the state by the United States Constitution, and the courts raise critical issues of personal privacy for all citizens who use computers in their daily lives.

This note will discuss legal issues related to search and seizure of computers and define the trend that the law is taking in the emerging area of inquiry. Personal privacy protection will be adequate regarding computer searches and seizures only if the courts properly balance the government's interests in bringing criminals to justice against citizens' interests against overly broad inquiries into the personal affairs. The government's interest cannot be placed so high that all areas of one's personal life becomes the subject of governmental scrutiny. This inquiry will proceed in

several parts. Section II provides a limited general discussion of constitutional limitations on search and seizure. Section III will discuss search and seizure of computers in the context of the "plain view" doctrine as an exception to the general requirement of a warrant for searches and seizures and will show that the "plain view" doctrine does not apply to closed computer files. Section IV will focus on search and seizure of computers based on information provided by private party informants. While the government may make use of informant provided information, the use is limited and subject to specific criteria. The note will examine the scope of search and seizure and particularity of warrants with regard to the problem of intermingled documents and the closed container analogy in Section V. A brief review of the grand jury subpoena process, as an alternative to the search warrant, will be considered in Section VI. In closing, this note will summarize the general direction that computer search and seizure law has taken and provide comments as to the appropriateness of the direction that the law has taken.

II. CONSTITUTIONAL LIMITATIONS ON SEARCHES AND SEIZURES

The Fourth Amendment protects against unreasonable searches and seizures and certain governmental invasions into private affairs. The Fourth Amendment 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 or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[1]

---

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

The history of the Fourth Amendment indicates that it was drafted in reaction to the use of general warrants in England that the drafters of the Constitution considered to be an unreasonable intrusion into privacy that should be prohibited. I WAYNE R. LaFave, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT, 5-7 (1996). The Fourth Amendment, as adopted, is both brief and ambiguous. *Id.* The Fourth Amendment gives no definition of "unreasonable" and does not set forth detailed information regarding the conditions for proper issuance of a warrant. *Id.*

Another commentator noted that:

> Moreover, the Fourth Amendment, more than many other parts of the Constitution, appears to require a fairly high level of abstraction of purpose; its use of the term "reasonable" (actually "unreasonable") positively invites construction that change with changing circumstances. Carol S. Steiker, *Second Thoughts About First Principles,* 107 HARV. L. REV. 820, 823-24 (1994).

If we accept this proposition - that the construction of the Fourth Amendment's "reasonableness" clause should properly change over time to accommodate constitutional purposes more general than the Framer's specific intentions . . . focus on colonial history to support a disjunctive reading of the "reasonableness" clause and the Warrant Clause and to attack the exclusionary rule seem short-sighted. Such a focus ignores at least two crucial changes between colonial times and the present that must inform our current readings of the Fourth Amendment as a whole. First, at the time of the drafting and ratifying of the Fourth Amendment, nothing even remotely resembling modern law enforcement existed. The invention in the nineteenth century of armed, quasi-military, professional police forces, whose form, function, and daily presence differ dramatically from that of the colonial constabulary, requires that modern-day judges and scholars rethink both the relationship between

The protections of the Fourth Amendment apply equally to corporations as well as to natural persons.[2]

The Court noted that in protecting privacy interests the courts must act as a check on "the 'well-intentioned but mistakenly over-zealous executive officer' who are a party of any system of law enforcement."[3] As a result, the Supreme Court has generally held that unless justified by an exception to the warrant requirement, all searches should proceed only after issuance of a warrant by a neutral and detached magistrate.[4] It is a well-established doctrine that "searches conducted outside the judicial process, without prior approval by a judge or magistrate, are per se unreasonable under the Fourth Amendment subject only to a few specifically established and well-delineated exceptions."[5]

In addition, a neutral magistrate should only issue warrants after demonstration of probable cause that evidence of a particular crime will be found, and that the warrant must describe with particularity the place to be searched and the items to be seized.[6] There are numerous exceptions to the warrant requirement including search incident to arrest, exigent circumstances, inventory searches and searches necessary to protect officers and others.[7]

A Fourth Amendment enforcement doctrine, first discussed by the Court in 1914, is the exclusionary rule.[8] The Court held that the courts should exclude from evidence any evidence seized in violation of the Fourth Amendment from any prosecution of the defendant from whom the items had been improperly seized.[9] Subject to certain exceptions,[10] the exclusionary rule prohibits use of any evidence illegally obtained, testimony regarding observations made during the illegal search, and any evidence obtained in the illegal search may not be used as a basis for additional warrants concerning the matter under investigation.[11]

The Court also views search and seizure in light of a reasonableness test, defined by *Katz v. United States*, to determine if a search warrant is required.[12] The *Katz* test

---

"reasonableness" and "warrants" and the nature of Fourth Amendment remedies. Second, the intensification of inter-racial conflict in our society . . . necessitate new constructions of the Fourth Amendment. *Id.*

[2]General Motors Leasing Corp. v. United States, 429 U.S. 338, 353 (1977).

[3]United States v. United States District Court, 407 U.S. 297, 316 (1972) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).

[4]*Id.* at 316-17.

[5]Katz v. United States, 389 U.S. 347, 357 (1967).

[6]Dalia v. United States, 441 U.S. 238, 255 (1979).

[7]California v. Acevedo, 500 U.S. 565, 582 (1991) (Scalia, J., concurring).

[8]Weeks v. United States, 232 U.S. 383 (1914).

[9]*Id.* at 398.

[10]*See* Massachusetts v. Sheppard, 468 U.S. 981 (1984); United States v. Leon, 468 U.S. 897 (1984); Walder v. United States, 347 U.S. 62 (1954).

[11]Wong Sun v. United States, 371 U.S. 471, 485-86 (1963).

[12]*Katz*, 389 U.S. at 347.

has two parts: 1) does the individual have a subjective expectation of privacy in the item or items to be searched and 2) is the subjective expectation of privacy one that society is prepared to accept as reasonable.[13] In *California v. Greenwood,* the Court held that although the defendants had a subjective expectation of privacy in garbage placed at the curb for collection, that expectation was not one which society was prepared to accept as reasonable.[14] The courts have recognized that enclosed spaces like suitcases, footlockers, briefcases and other closed containers are generally subject to a very high level of privacy expectation.[15] In addition, in 1967 the Supreme Court held that privacy expectations extend not only to tangible objects but to intangible items as well.[16] When a privacy expectation exists with regard to the contents of a closed container, a warrant to search the containers contents will generally be required.[17] There are, however, exceptions to the requirement to obtain a warrant to search the contents of a closed container. For example, the Court recognized that the government may search a vehicle without a warrant if the search is supported by probable cause, unlike homes or similar places.[18]

In *Carroll*, the Court noted that there was an essential difference between a vehicle and a fixed structure, where the government may readily obtain a warrant, "because the vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought."[19] In *United States v. Ross*, the Court held that searching an automobile without a warrant, when the search of the automobile was supported by probable cause, included the right to search closed containers or packages found in the automobile.[20] This does not, however, mean that the government has an unlimited right to undertake warrantless searches of closed containers found in automobiles. In *United States v. Chadwick*, the Court refused to extend the rationale of *Carroll* to a locked footlocker that the government had probable cause to believe contained marijuana.[21] The Court refused to extend *Carroll* to this situation indicating that people have greater privacy expectations in luggage than in their automobiles.[22] Police may secure seized luggage in anticipation of obtaining a warrant to search its contents, unlike the case however with automobiles that suspects may easily remove from the jurisdiction.[23]

---

[13]*Katz*, 389 U.S. at 361 (Harlan, J. concurring).

[14]California v. Greenwood, 486 U.S. 35, 39 (1988).

[15]United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978).

[16]Warden v. Hayden, 387 U.S. 294, 305 (1967).

[17]United States v. Chadwick, 433 U.S. 1, 10-11 (1977).

[18]Carroll v. United States, 267 U.S. 132 (1925).

[19]*Id.* at 153.

[20]United States v. Ross, 456 U.S. 798 (1982).

[21]United States v. Chadwick, 433 U.S. 1 (1977).

[22]*Id.* at 13.

[23]*Id.*

The Court, in *California v. Acevedo*, limited the doctrine established in *Chadwick*.[24] In *Acevedo*, the Court held that the government may undertake a warrantless search of a container located in an automobile, even if they only had probable cause to believe that the container held evidence of a crime and did not have probable cause to search the entire vehicle.[25] Although an officer may take possession of a container in anticipation of obtaining a warrant to search its contents, that authority is separate from any authority to search through the contents of the container.[26] Additionally, a district court held that electronic storage devices, such as computers, enjoy the same privacy interest as any other closed container.[27] Unlike the garbage in *Greenwood*[28] where the expectation of privacy was not reasonable, a computer user should have little difficulty establishing a subjective expectation of privacy in the contents of their computer storage which society is likely to accept as reasonable. Of course, should the computer be located in an automobile, the government could argue under *Acevedo*[29] and *Ross*[30] that the government may have the right to search the computer without a warrant. There are no reported cases of this scenario, but with the increased use of portable and laptop computers it may occur in the future. Thus, while a computer is likely to enjoy the same Fourth Amendment protections as other closed containers, this protection clearly has limits and depends upon where the container is located.

One does not lose their expectation of privacy in a closed container simply because it is temporarily out of their control.[31] One court noted that such expectations of privacy "may well be at their most intense when such effects are deposited temporarily or kept semi-permanently in public places or under the general control of another."[32] Because a computer is not located in one's home or not under one's control does not lead to the loss of a reasonable expectation of privacy. There are, however, circumstances under which computer users may lose their reasonable expectation of privacy. Case law suggests that if a person abandons or otherwise disclaims his interest in property, the police may properly seize the items and the evidence can be properly admitted against the defendant.[33] Thus if a computer user makes his equipment readily or routinely available to others, the computer user's expectation of privacy may be diminished.

The Court has held, additionally, that disclosure of information to third parties made voluntarily is done at the risk of loss of a privacy interest of the person making

---

[24]California v. Acevedo, 500 U.S. 565 (1982).

[25]*Id.*

[26]Walter v. United States, 447 U.S. 100 (1980).

[27]United States v. David, 756 F. Supp. 1385 (D.Nev. 1991).

[28]*Greenwood*, 486 U.S. at 35.

[29]*Acevedo*, 500 U.S. at 565.

[30]*Ross*, 456 U.S. at 798.

[31]*Block*, 590 F.2d at 541.

[32]*Id.*

[33]California v. Hodari D., 499 U.S. 621, 624, 629 (1991).

the disclosure.[34] The persons to whom the information is disclosed may do with the information as they please including disclosing it to authorities.[35] This becomes an issue when a computer is surrendered to a technician for repair and will be discussed in more detail in a later section on use of informants. Furthermore, any computerized information found to fall within the "plain view" doctrine will also loose any expectation of privacy. The "plain view" doctrine will be discussed in more detail in the next section.

III. THE PLAIN VIEW DOCTRINE

In *Coolidge v. New Hampshire*, the Court held that authorities may seize evidence without a warrant provided the evidence is in plain view.[36] In *Coolidge,* the Court set forth the requirements for the plain view exception to the warrant requirement as follows: 1) the officer must be legally in a position to view the object that is in plain view; 2) the incriminating character of the object must be immediately apparent to the officer; and 3) the officer must have a lawful right to access the object itself.[37] The Court additionally indicated that "the 'plain view' doctrine may not be used to extend a general exploratory search from one object to another until something incriminating . . . emerges."[38]

The Court again explored the limits of the plain view doctrine in *Arizona v. Hicks*.[39] In *Hicks*, a suspect fired a bullet through the floor of his apartment injuring a man living below.[40] Police arrived and entered the suspect's apartment to search for evidence related to the shooting. [41] A police officer noticed several sets of expensive stereo equipment that seemed out of place in the suspect's apartment.[42] The police officer suspected the suspect had stolen the components and moved several of them so that he could record their serial numbers.[43] The officer telephoned police headquarters, who advised him that they were stolen, and he seized them.[44] The Court found that the officer's moving of the equipment "did constitute a 'search' separate and apart from the search for the shooter, victims, and weapons that was the lawful objective of his entry into the apartment."[45] The Court concluded in *Hicks*

---

[34]Hoffa v. United States, 385 U.S. 293, 414 (1966).

[35]*Id.*

[36]Coolidge v. New Hampshire, 403 U.S. 433 (1971).

[37]*Id.* at 466-67. *Coolidge* additionally required that the discovery of the object or evidence be inadvertent. This requirement of inadvertent discovery was later dropped by the Court. *See* Horton v. California, 496 U.S. 128 (1990).

[38]*Coolidge*, 403 U.S. at 466.

[39]Arizona v. Hicks, 480 U.S. 321 (1987).

[40]*Id.* at 323.

[41]*Id.*

[42]*Id.*

[43]*Id.*

[44]*Hicks*, 480 U.S. at 321.

[45]*Id.* at 324-25.

that the difference between "'looking' at a suspicious object in plain view and 'moving' it even a few inches is much more than trivial for purposes of the Fourth Amendment."[46] Thus, any action beyond the mere observation of an object will violate the plain view exception to the warrant requirement.

In *Horton v. California*, the Court further refined the definition of the "plain view" doctrine.[47] In *Horton*, the government executed a search warrant to look for stolen property and found none.[48] The police did, however, discover in "plain view" weapons and other evidence which the police had reason to know was connected to the robbery under investigation.[49] Thus, although the weapons were found in "plain view" their discovery was not inadvertent since the police were interested in finding such other evidence that connected the suspect with the robbery.[50] The Court held "that even though inadvertence is a characteristic of most legitimate 'plain view' seizures, it is not a necessary condition."[51]

Scenarios involving computer search and seizure are somewhat different than the circumstances described in *Hicks*[52] and *Horton*[53] where the officer was in view of a physical object. In searches involving computer systems the only thing that arguably could be in "plain view" is anything that is displayed on the computer screen without any interference with the computer system by the government. Since even the most trivial disturbance of an object under *Hicks*[54] violates the plain view doctrine the question remains whether closed computer files stored on a computer hard drive can ever fall within the plain view exception. Reviewing the listing of computer files may indicate that the files contain graphics or pictures (such as those with .jpg or .gif extensions) just as other file extensions may suggest that they are database or word processing files.[55] The contents of the files, however, cannot be determined unless one opens the file with the appropriate software and disturbing of the file by opening or accessing it with software is arguably enough to violate the "plain view" exception to the warrant requirement. The incriminating character of a

---

[46]*Id.* at 325

[47]Horton v. California, 496 U.S. 128 (1990).

[48]*Id*. at 131.

[49]*Id.*

[50]*Id.*

[51]*Id*. at 130.

[52]*Hicks*, 480 U.S. at 321.

[53]*Horton*, 496 U.S. at 128.

[54]*Hicks*, 480 U.S. at 321.

[55]The Department of Justice, in discussing search and seizure of computers and computer files indicates that "if agents with a warrant to search a computer for evidence of narcotics trafficking find a long list of access codes taped to the computer monitor, the list should also be seized." The Department of Justice does not take the position that closed files in the computer's memory or storage devices are ever in plain view. *Federal Guidelines for Searching and Seizing Computers* (1994), Supplement (October 1997) and Supplement (January 1999), Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section. <http://www.usdoj.gov/criminal/cybercrime>.

closed computer file is not immediately apparent as incriminating and cannot fall within the "plain view" exception to the warrant requirement as defined by *Coolidge*[56], *Hicks*[57], and *Horton*[58].

Two recent cases suggest that courts will not apply the "plain view" doctrine to closed computer files on a hard drive. In *United States v. Carey*, a suspect was under investigation for illegal drug trafficking and while executing an arrest warrant the police noticed drug paraphernalia in plain view.[59] A police officer asked the suspect's consent to search his apartment which he gave fearing that the officers would trash his apartment if he did not consent.[60] During the search police found quantities of various illegal drugs and two computers.[61] Police seized the computers believing that they would either be subject to forfeiture or contain evidence of drug dealing and removed them to the police station.[62] Later a warrant was obtained allowing the search of the computer files for "'names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances.'"[63]

A detective searched the hard drives for text-based files related to the suspected drug activity using relevant search words; the search produced no files related to any drug activity.[64] Along with the other files the detective downloaded more than two hundred JPG or image files alleging that the image files could contain evidence pertinent to a drug investigation.[65] Upon opening one JPG file, the detective discovered that the file contained child pornography.[66] After discovering the first child pornography file he abandoned his search for drug related files and opened many JPG files that also appeared to contain images of child pornography.[67] He did not, however, obtain a separate warrant to continue the search for child pornography after opening the first JPG file.[68] The government argued that the child pornography files were in plain view and officers needed no separate search warrant.[69]

---

[56]*Coolidge*, 403 U.S. at 433.

[57]*Hicks*, 408 U.S. at 321.

[58]*Horton*, 496 U.S. at 128.

[59]United States v. Carey, 172 F.3d 1268, 1270 (10th Cir. 1999).

[60]*Id.*

[61]*Id.*

[62]*Id.*

[63]*Id.*

[64]*Carey*, 172 F.3d at 1270-71.

[65]*Id.* at 1271.

[66]*Id.*

[67]*Id.*

[68]*Id.*

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

The court held that the detective expanded the scope of his search beyond that permitted by the warrant when he began opening JPG files.[70] The court stated that after opening the first JPG file the detective "was in the same position as the officers had been when they first wanted to search the contents of the computers for drug related evidence. They were aware they had to obtain a search warrant and did so."[71] The court also noted that the images "were in closed files and thus not in plain view."[72] Additionally, since the government had removed the computers to police custody there were no exigent circumstances or practical reasons to permit the warrantless search of the JPG files.[73] The court concluded in *Carey* that once the detective viewed the contents of the first JPG file, the law required him to shut down his search for evidence of child pornography and apply for a separate warrant to search for child pornography before proceeding to open further JPG files.[74] Because the officer did not follow this procedure, the court suppressed all evidence of child pornography.[75]

Another recent case addresses these same issues in a somewhat different context. In *United States v. Turner*, an intruder with a knife awakened a woman in her bedroom at around 2:00 a.m..[76] A neighbor in the adjacent apartment who claimed he was seated working at his computer at the time of the assault, telephoned police saying that he had observed someone fleeing his neighbor's apartment.[77] When police returned to the scene the next morning, they noticed that the victim's window screens and those of the neighbor who had called police the prior morning were ajar and appeared to be smeared with blood.[78] Police asked permission to search the apartment of the neighbor to look for evidence that the assailant had been in his apartment, suspecting that the assailant may have entered his apartment as well; he freely consented to the search.[79] While searching the apartment, the computer screen suddenly illuminated and displayed a photograph of a nude woman who was physically similar to the neighbor who had been assaulted.[80] Upon seeing this image, an officer seated himself at the suspect's computer and began searching for recently accessed files.[81] The officer opened a number of JPG files finding various images of nude women in bondage.[82] Upon finding these files, the officer continued to search

---

[70] *Id.* at 1273.

[71] *Id.*

[72] *Id.*

[73] *Id.* at 1275.

[74] *Carey*, 172 F.3d at 1276.

[75] *Id.*

[76] United States v. Turner, 169 F.3d 84, 85 (1st Cir. 1999).

[77] *Id.*

[78] *Id.*

[79] *Id.* at 85-86.

[80] *Id.* at 86.

[81] *Turner*, 169 F.3d at 85-86.

[82] *Id.*

the hard drive for other files noting that several bore labels like "young" or "young with breasts."[83] When the officer opened these files, he found what he considered child pornography files and seized the computer.[84]

In *Turner*, the court held that the sexually suggestive image which suddenly came into "plain view' did not make Turner's computer and files subject to search just because the assault on his neighbor had a sexual component.[85] The court noted that the search of the suspect's computer files exceeded the scope of his consent.[86] When Turner consented to the search of his apartment for "evidence of an assault" this would reasonably mean physical evidence of the assault and not the type of documentary evidence one would expect to find stored on a computer hard drive.[87] Finding that the search exceeded the reasonable scope of the consent the court suppressed all evidence that the government had obtain in the warrantless search of Turner's apartment.[88]

Turner[89] and *Carey*[90] both illustrate the limits of the "plain view" doctrine with regard to closed computer files. *Carey*[91] illustrates that even with a proper warrant to search a suspect's computer the scope of the search is limited by the terms of the warrant. Where police are authorized to search for evidence of illegal drug activity stored on a computer it is not likely that this evidence will be stored in image or graphics files. In *Carey*, the court accepted the government's argument that image files could potentially show some evidence of illegal drug activity such as photographs of drugs or growing systems.[92] This is absurd in the face of a warrant that was aimed at names, addresses, and other such documentary evidence of illegal drug activity.[93] No reasonable person would expect lists of names and addresses to be found in a graphics file; this type of data would generally be stored in word processing or data base files.[94] *Carey* further allowed that once the officer opened

---

[83]*Id.* at 86.

[84]*Id.*

[85]*Id.*

[86]*Turner*, 169 F.3d at 86.

[87]*Id.* at 88-89.

[88]*Id.*

[89]*Id.*

[90]*Carey*, 172 F.3d at 1268.

[91]*Id.* at 1274.

[92]*Id.* at 1271.

[93]*Id.* at 1270.

[94]Although the names or extensions of files (like .jpg or .gif) can be useful in determining what type of file one is looking at it is not entirely dispositive. A computer user can choose to save a file with any name or extension they choose. Thus, a criminal attempting to hide a database file could save it under a name that what would appear to be a graphics file. Without information leading the government to believe that the suspect is engaged in this type of deception most file names are reasonable indications of the type of information contained in a file.

the initial graphics file (finding what he believed to be an image of child pornography) he could have used this finding as probable cause to support a search warrant to look for evidence of child pornography, even though the court correctly held that the image was not in "plain view."[95]

This analysis is flawed in two ways. First, since it was not reasonable to open a graphics file under a warrant looking for evidence of illegal drug activity aimed at names, addresses, and other documentary evidence should not be allowed as probable cause for a warrant to investigate child pornography. The initial opening of the first closed graphics file, which was not in "plain view," was unreasonable and should invalidate any further search based on this information. Second, in executing a search warrant for computerized data the government should be required to employ officers with sufficient knowledge to distinguish various types of computer files. The officer in *Carey* claimed that he did not initially know to distinguish a text file from an image or JPG file.[96] If the government is not compelled to employ knowledgeable officers in executing searches of computers, citizens will be exposed to unreasonably broad searches of their computer files simply because the government employs ignorant personnel. The courts should set minimum standards for the training of personnel involved in investigations of computer based crimes.

Turner provides that even if an image comes into plain view on a computer screen this does not necessarily support expansion of a search to the contents of the computer's memory and closed files.[97] If the image does not relate to the evidence for which the officer has consent to search he or she cannot expand his or her search to the computer's memory when this extension is not reasonable.[98] In *Turner*, the image that came into "plain view" was a picture of a nude woman with "light-colored hair."[99] This photograph was not evidence of any crime and did not support the officer's review of closed computer files on Turner's computer which went beyond the scope of Turner's consent.[100]

Three other cases illustrate situations where computer files or machine-readable media were considered to meet the definition of "plain view." In *City of Akron v. Patrick*, a suspect was under investigation for suspected illegal gambling activities.[101] Police executed a search warrant on the suspect's home and observed two computers.[102] The screen of one computer displayed the words "Advanced, Declined, Unchanged."[103] One officer, based on his experience, recognized these terms as relating to a gambling game based upon stock quotations and called in a police expert who determined that the computers were being used in a gambling

---

[95]*Carey*, 172 F.3d at 1273.

[96]*Id.* at 1271.

[97]*Turner*, 169 F.3d at 88.

[98]*Id.*

[99]*Id.* at 86.

[100]*Id.*

[101]City of Akron v. Patrick, 1982 WL 5049 (Ohio Ct. App. 1982).

[102]*Id.* at *1.

[103]*Id.*

operation.[104] Officers then seized the computers and various diskettes as evidence.[105] The defendant in *Patrick* argued that since the warrant did not specifically list the computers, the seizure was unlawful.[106] One of the officers testified that when the computer screen displayed the words "Advanced, Declined, Unchanged" based on his experience and knowledge of gambling operations, he immediately recognized that the suspect was using the computers in an illegal gambling operation.[107]

The court held that the officer's observation of the words on the computer display was in "plain view" since the officer was legally in a position to view the computer screen, the incriminating character of the information on the computer screen was immediately apparent to the police officer, and the officer had the legal right to view the computer screen by virtue of the search warrant.[108] This case is unlike *Carey*[109] and *Turner*[110] where the government argued in an attempt to extend the "plain view" doctrine to closed files on the computer hard drive. In *Patrick,* the "plain view" doctrine was applicable because the incriminating use of the computer was immediately apparent to the officers from the information displayed on the computer monitor.[111] *Patrick* did not involve an attempt by the government to apply to "plain view" doctrine to closed files on the computer hard drive.[112] Because the incriminating use of the computer was immediately apparent to the officers, the search and seizure fulfilled the requirements of the "plain view" doctrine in *Patrick*.[113] The court allowed the seizure of the computers as gambling paraphernalia under the original search warrant.[114] The opinion does not indicate that any further warrants were required to search the contents of the seized computer equipment.[115]

In *Oklahoma v. One Pioneer CD-ROM Changer*, a suspect was under investigation for violations of state obscenity laws.[116] Having purchased obscene CD ROMs from the suspect the police obtained a search warrant for the suspect's home.[117] While executing the warrant the officers came upon a large computer system the monitor of which displayed the words "viewing" and/or "copying" along

---

[104] *Id.*

[105] *Id.*

[106] *Patrick*, 1982 WL 5049 at *4.

[107] *Id.*

[108] *Id.*

[109] *Carey*, 172 F.3d at 1268.

[110] *Turner*, 169 F.3d at 84.

[111] *Patrick*, 1982 WL 5049 at *4.

[112] *Id.*

[113] *Id.*

[114] *Id.*

[115] *Id.*

[116] Oklahoma v. One Pioneer CD-ROM Changer, 891 P.2d 600 (Okla. Ct. App. 1994).

[117] *Id.* at 604.

with other descriptions like "lesbian sex" and/or "oral sex."[118] The court noted that the display of these words was in "plain view" during the search, making the incriminating use of the computer immediately apparent to the government, and therefore, the seizure of the computers was justified without a warrant under the "plain view" doctrine.[119]

In *Ivatury v Texas*, police were investigating a defense industry espionage case.[120] The police executed a warrant for the search of the suspect's safe deposit box for certain photographs and other evidence.[121] The police discovered a computer tape among the contents of the safe deposit box and recognized it as a special type of tape used in the defense industry and seized it.[122] The court held that the seizure met the requirements of the "plain view" doctrine noting that: 1) the police possessed a valid search warrant for the safe deposit box; 2) police discovered the tape inadvertently; and 3) it was immediately apparent that the tape was contraband.[123] Here the officer recognized the tape as a special type used in the defense industry and as the type of tape the suspect had previously offered to sell him with stolen defense industry information.[124]

Viewed together, these cases indicate that courts will not extend the "plain view" doctrine to unopened computer files on a computer hard drive. When authorities fail to discover evidence of the crime for which they have a proper warrant or consent, the courts will not permit them to abandon this search in hopes of finding evidence of other unspecified criminal activity. In keeping with *Coolidge*,[125] the cases involving computers and the "plain view" doctrine have not allowed extensions of general exploratory searches. In addition, in *Carey*[126] when an officer inadvertently came across evidence of another crime for which he did not have a valid warrant, the court required the officer to shut down the search and apply for further authorization from a neutral magistrate. The three cases where the courts extended the "plain view" doctrine to computer files or computer media all involved cases where the computer screen clearly and prominently displayed evidence of a crime without any disturbance from the authorities or where the officers knew that an item of machine readable media was contraband from their prior dealings with the suspect.[127] The courts did not, however, extend the "plain view" doctrine to closed computer files on a computer hard drive.

---

[118] *Id.*

[119] *Id.* at 605.

[120] Ivatury v. Texas, 792 S.W.2d 845 (Tex. Ct. App. 1990).

[121] *Id.* at 850.

[122] *Id.*

[123] *Id.* at 851.

[124] *Id.*

[125] *Coolidge*, 403 U.S. at 466.

[126] *Carey*, 172 F.3d at 1275.

[127] One Pioneer CD-ROM Changer, 891 P.2d 600; *Ivatury*, 792 S.W.2d at 845; *Patrick*, 1982 WL 5049.

Thus, although the cases dealing with computer systems are few in number as of this time, a general exploration of any and all closed files on a computer is not likely to be upheld by the courts nor will the closed files be found to fall under the "plain view" doctrine. This approach is proper and in line with *Hicks.*[128] If the mere movement of a stereo component a few inches was sufficient to violate the Fourth Amendment, the random opening of numerous closed computer files, when not properly authorized by a search warrant or covered by the scope of a consent, also violates the Fourth Amendment.

IV. INFORMANTS

The Fourth Amendment limits state action with regard to searches and seizures. The limitations of the Fourth Amendment do not bind the actions of private parties. The Supreme Court has held that "a wrongful search or seizure conducted by a private party does not violate the Fourth Amendment and that such private wrongdoing does not deprive the government of the right to use evidence that it has acquired lawfully."[129] In *Coolidge,* the Court established that the court must determine if the private party acted as the "instrument or agent" of the government when the private party conducted the search.[130] In *United States v. Miller*, the factors to be considered in determing if a private party acted as an instrument or agent of the government are listed as: "(1) whether the government knew of or acquiesced in the intrusive conduct, and (2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends."[131]

The fact that there are but a few reported cases involving private party searches of computers should not be taken as an indication that this situation does not raise serious privacy concerns. Whenever citizens take their computers for repair or upgrade, the equipment is exposed to the prying eyes of the technician who works on the equipment. In the course of making the necessary repairs, the technician has a legitimate need to access computer files to determine if the machine functions properly. In this process, all of the computer's files are potentially exposed to review by the technician. This raises concerns in that, as we have seen, private parties are not bound by the limitations of the Fourth Amendment, and therefore, any evidence of suspected criminality could be reported to the police by the repair company and potentially used by the government to support a search warrant for the computer files.[132] How courts viewed reports of potential evidence of criminality by informants played out differently in the reported cases as we will see.

---

[128]*Hicks*, 480 U.S. at 321.

[129]Walter v. United States, 447 U.S. 649, 656 (1980). *See also*, Coolidge, 403 U.S. at 487-90; United States v. Blocker, 104 F.3d 720, 725 (5th Cir. 1997).

[130]*Coolidge*, 403 U.S. at 487.

[131]United States v. Miller, 688 F.2d 652, 657 (9th Cir. 1982).

[132]Although this will not be discussed in this note, the repair process raises client confidentially concerns for professionals like attorneys, accountants, or physicians who's computers may contain client information that they are required, by the standards of their respective professions, to hold in confidence.

In *United States v. Hall*, a defendant took his computer to a computer repair company.[133] A computer technician accessed several file directories in an attempt to diagnose the problems with the computer.[134] The technician noted that some directories and files had unusual names that implied sexual content; one file was titled "Boys 612."[135] The technician viewed the file and found that it appeared to contain an image of young naked boys, who he estimated to be between ten and twelve years of age engaged in anal sex.[136] The technician proceeded to view a number of other files that he also judged to contain images of child pornography and estimated that there were around 1,000 files on the hard drive that had names implying that they contained images of child pornography.[137] The technician subsequently telephoned a member of the Illinois State Police, who was a personal friend of his, and informed him of what he had found on the computer.[138]

At the request of police, the repair person copied a number of the images to a diskette which he gave to the police (according to the opinion no officers viewed the contents of the diskette).[139] The police and FBI requested that the repair company inform the customer that his computer repairs would take several additional days since the store needed to order additional parts.[140] Using the informant's descriptions of what he had viewed, but not the information on the diskette, the government obtained a warrant to search the customer's computer and residence.[141] The search of the computer hard drive confirmed that it contained child pornography and they prosecuted the customer for possession of the images.[142] The defendant moved to suppress the evidence contending that it was discovered in violation of the Fourth Amendment.[143] The court found that the repairman's viewing of computer files was done in the course of repairing a computer in the normal course of business with the sole purpose of repairing the computer.[144] The Government had no knowledge of the repair and did not instruct the repair person to inspect the files; in fact, no government officials were contacted until after the files were discovered.[145] The court further noted that the repairman's "statements to law enforcement personnel formed a sufficient basis of probable cause to support the search warrants. With

---

[133]United States v. Hall, 142 F.3d 988, 991 (7th Cir. 1998).

[134]*Id.*

[135]*Id.*

[136]*Id.*

[137]*Id.*

[138]*Hall*, 142 F.3d at 991.

[139]*Id.*

[140]*Id.*

[141]*Id.*

[142]*Id.* at 992.

[143]*Hall*, 142 F.3d at 992.

[144]*Id.* at 993.

[145]*Id.*

lawfully issued warrants, the same files that [the repairman] copied onto disk for [police] were independently discovered by the Government. . ."[146] Citing the independent source doctrine, the court allowed the admission of the evidence.[147]

In *United States v. Barth*, a defendant took his computer to a self-employed computer consultant for repairs.[148] In diagnosing the computer problems, the consultant happened upon and viewed several JPG files and observed images of child pornography.[149] He then contacted an FBI agent who was his supervising agent as a confidential informant for the bureau.[150] The agent instructed the consultant to copy all of the hard disk files onto diskettes and that the agent would have the diskettes picked up.[151] The court found that the consultant's initial viewing of the JPG files did not violate the Fourth Amendment because he did not intend to assist law enforcement officers when he initially viewed the file and merely did so in an effort to repair the computer.[152] Once the consultant notified his supervising agent at the FBI and was instructed to view and copy additional files, the court concluded that these actions were attributable to the Government.[153] Additionally, once the consultant had copied the contents of the hard disk to diskette, these files were subsequently viewed by law enforcement officials without the benefit of a search warrant.[154] The court held that the search violated the two part test in *Miller*[155] and ordered the evidence from the search of the defendant's computer suppressed.[156]

A third case, *United States v. Harned*, involving an informant resulted in the exclusion of evidence for an entirely different reason than the previous case.[157] A customer had taken a computer to a repair shop for service and, in the course of testing the computer, the technician discovered a CD-ROM disk with files labeled with boys names.[158] The technician viewed several of the files and felt that they depicted child pornography.[159] The technician notified the police and an officer went

---

[146] *Id.* at 994.

[147] *Id.*

[148] United States v. Barth, 26 F. Supp.2d 929 (W.D. Tex. 1998).

[149] *Id.* at 932.

[150] *Id.* The opinion does not give any indication as to nature of the consultant's involvement with the FBI but simply indicates that he was a confidential informant for the FBI.

[151] *Id.*

[152] *Barth*, 26 F. Supp.2d at 935-36.

[153] *Id.* at 936.

[154] *Id.* at 937.

[155] United States v. Miller, 688 F.2d 652, 657 (9th Cir. 1982).

[156] *Barth*, 26 F. Supp.2d at 942.

[157] United States v. Harned, 182 F.3d 928 (9th Cir. 1999).

[158] *Id.*

[159] *Id.*

to the repair shop to view several of the described files.[160] The officer prepared a search warrant application and stated to the judge that there were around 489 files and that they involved acts of masturbation.[161] The government subsequently indicted the defendant on child pornography charges.[162] The defendant moved to suppress the evidence based on grounds that the officer had intentionally or recklessly included material false statements in his warrant application.[163] The court found two falsehoods in the application: first, very few of the images involved depictions of both children and adults; and second, the description of the sexual acts as masturbation was found to be false.[164] "The court also found that the affiant acted with reckless disregard for the truth by including those false statements in the affidavit. Finally, the court held that the affidavit provided only a 'bare conclusion' insufficient for probable cause once the false statements were redacted."[165] The court found that the government based the warrant application exclusively on "the conclusory statement of a computer store employee."[166] The court noted that what may have been an explicit sexual act involving child pornography to the computer store employee, may not have been so to a neutral magistrate.[167] Neither the employee nor the officer who prepared the affidavit had sufficient experience to adequately judge the nature of the files they had viewed.[168] The court suppressed all of the evidence and noted "that probable cause for a search warrant may not rest entirely upon the bare conclusion of a computer store employee as to the nature of the photographs."[169]

Certain guidelines are apparent from these three cases regarding use of third party informants. Taking *Barth*[170] and *Hall*[171] together, it appears that government use of information from a private party search is a simple matter. Since private searches do not implicate the protections of the Fourth Amendment, it would appear

---

[160]*Id.*

[161]*Id.*

[162]*Harned*, 182 F.3d at 928.

[163]*Id.*

[164]*Id.*

[165]*Id.*

[166]*Id.*

[167]*Harned*, 182 F.3d at 928.

[168]*Id.*

[169]*Id.* In another case involving a prosecution involving child pornography one expert testified at trial regarding how individuals who use computers to view child pornography, name, and organize their files. United States v. Simpson, 152 F.3d 1241, 1245 (10th Cir. 1998). A second expert, with extensive expertise in determining the age children of children in images, provided testimony to determine that images were actually child pornography and to testify to the age of the children portrayed in the images. *Id.* The determination of what constitutes child pornography is not a simple matter within the grasp of the average lay person.

[170]*Barth*, 26 F. Supp.2d at 929.

[171]*Hall*, 142 F.3d at 988.

that such information is readily usable by law enforcement. In *Barth* however, if the private party acts as an "instrument or agent" of the government, the search may implicate Fourth Amendment considerations. *Barth*[172] tells us that if law enforcement provides direction to the third party with regard to expanding the private search and thus the additional intrusion by the third party is intended to assist law enforcement, the two part *Miller*[173] test is violated. In *Hall*,[174] the *Miller*[175] test was not violated because law enforcement used the information provided by the third party to apply for a search warrant only. Law enforcement did not direct the third party in *Hall* to expand his search and the informant did not make the initial discovery of contraband in an attempt to assist law enforcement.[176] In addition, in *Barth*,[177] law enforcement officials viewed a number of computer files before obtaining a warrant; in *Hall,* the government testified that they had not viewed the contents of any files before obtaining a search warrant for the computer.[178]

In the alternative, *Harned*[179] indicates that courts may be reluctant to base probable cause on the conclusion of a layperson informant in certain situations. Judging what constitutes child pornography may require considerable expertise. *Harned* indicates that unless the third party informant has the expertise to properly evaluate the information he has found, his conclusions about the nature of the material may not be sufficient to support a search warrant.[180] While the *Harned*[181] case involved child pornography, if a case involved such items such as financial, insurance or medical information, the government should be required to show that the informant had the proper expertise to judge the nature of the information he or she had viewed that was used as a probable cause for a search warrant application. Law enforcement must use care when using the results of third party information as a basis for broad searches of computer data. Based on the cases reviewed above, defendants can challenge informant information if the informant's actions implicated government action; if the government in any way directs the informants actions or views informant provided evidence prior to obtaining a warrant the courts have been reluctant to find the search valid. In addition, the defendant can challenge the expertise of the informant in judging the nature of the information he or she has discovered if the evidence is of the type that generally require specialized training or knowledge to make a correct assessment of what the informant discovered. Taken together, the cases to date indicate that although the government is free to use information from private party searches the information must be properly evaluated,

---

[172]*Barth*, 26 F. Supp.2d at 936.

[173]*Miller*, 688 F.2d at 657.

[174]*Hall*, 142 F.3d at 993-94.

[175]*Miller*, 688 F.2d at 657.

[176]*Hall*, 142 F.3d at 993.

[177]*Barth*, 26 F. Supp.2d at 933.

[178]*Hall*, 142 F.3d at 993.

[179]*Harned*, 182 F.3d at 928.

[180]*Id.*

[181]*Id.*

used with care, and the government must avoid directing the efforts of the informants with which the government has contact.

V. SCOPE OF SEARCH AND SEIZURE AND PARTICULARITY OF WARRANTS

A. The Closed Container Analogy & Particularity of Warrants

This note explained earlier that computer storage has been compared to other non-electronic closed containers for purposes of the Fourth Amendment. Analogizing computer storage to a closed container establishes a high level of Fourth Amendment protection for computer memory. This analogy, however, does present certain problems. When a small computerized address book or pager is compared to a closed container, this makes a great deal of sense since these devices will generally have the ability to store a limited amount of information all of which is similar. When applied to a larger computer storage device, such as a PC hard drive that has the ability to store a vast amount of information of various types, the closed container analogy is limited. If the closed container analogy is applied to a large computer system, then a warrant issued for a search of the computer would allow for unlimited review of the entire contents of the computer's memory. If the computer contains information subject to lawful search and seizure which is intermingled with other information that is not evidence of any crime, should the police be required to do any initial sorting to determine what files are within the scope of the warrant or simply go randomly looking through any and all files they may encounter? The courts have applied the closed container analogy to computer systems on a number of occasions.

In *United States v. Simpson*, the police obtained a warrant to search for evidence of child pornography.[182] In executing the warrant the police seized 19 videotapes, 18 diskettes, a number of documents and the suspect's entire computer.[183] The defendant argued that the computer disks and hard drives are closed containers separate from the computer itself, and that in the absence of exigent circumstances, a separate search warrant to look at the contents of these components was required.[184] The court rejected this argument, finding that once a warrant was issued for search of child pornography files, the computer and any components and storage devices on the computer were within the scope of the warrant since the evidence covered by the warrant could reasonably be found in computer storage.[185] Essentially, the court used the closed container analogy making the entire contents of the computer storage subject to review without further supervision from a neutral magistrate.[186]

---

[182]United States v. Simpson, 152 F.3d 1241, 1244 (10th Cir. 1998).

[183]*Id.*

[184]*Id.* at 1248.

[185]*Id.*

[186]In an earlier case the same court upheld the wholesale seizure to computer equipment where the warrant only specified that "equipment" could be seized without specifying that computers were included under this description. Davis v. Gracey, 111 F.3d 1472, 1478-79 (10th Cir. 1997). The court noted that the test for overbreadth of a warrant should be applied in a "common sense fashion." *Id.* at 1478. The description need only be as specific as the nature of the activity under investigation allows. *Id.* In this case, where the police were searching for obscene materials, it could be reasonable to assume that computers could contain

In *United States v. Lacey*, the court allowed another wholesale seizure of a defendant's computer system.[187] The warrant application described the computer in generic terms and also allowed for seizure of any computer diskettes found at the scene.[188] The government had probable cause to believe that the defendant had downloaded child pornography files but did not know if the images were stored on the computer's hard disk or on one of many computer disks in the defendants possession.[189] There was simply no way to specify what hardware and software had to be seized in order to retrieve the images.[190] In addition, the court noted that the warrant application "established probable cause to believe that [the defendant's] entire computer system was 'likely to contain evidence of criminal activity.'"[191] The court also found that the warrant contained objective limits to direct officers to the acceptable range of files that they could seize.[192] The court allowed admission of the evidence and found no error in allowing the police to make a wholesale seizure of the computer equipment without any attempt to sort for relevant information on-site.[193]

The court in *United States v. Musson* permitted seizure of 54 computer diskettes for later review and sorting off-site under a warrant specifying "correspondence, memoranda, ledgers, and any records and writings of whatsoever nature" detailing transactions of certain companies.[194] The defendant argued that seizure of the computer disks was outside the scope of the warrant since computer disks where not described in the warrant as an item to be seized and that the evidence on the disks should be excluded.[195] The court noted that in the age of modern technology and the commercial availability of various storage media, it was not possible for a warrant to specify what form the records might take.[196] Again, this consisted of a wholesale seizure of a large volume of intermingled documents without any need to attempt to sort them on-site.[197]

---

such items. *Id*. at 1479. The fact that computer equipment was not specifically listed in the warrant application was not considered relevant by the court. *Id.* The court noted that the only basis for invalidating warrants for overbreadth is where the language of a warrant authorizes the seizure of all documents without regard to their relevance to criminal activity. *Davis*, 112 F.3d 1478-89. The court did not require the police to undertake any on-site sorting for relevant information as suggested in *Tamura*. *Id.*

[187]United States v. Lacey, 119 F.3d 742 (9th Cir. 1996).

[188]*Id.* at 746.

[189]*Id.*

[190]*Id.* at 746-47.

[191]*Id*. at 746 (quoting United States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995)).

[192]*Lacey*, 119 F.3d at 746.

[193]*Id.* at 746-47.

[194]United States v. Musson, 650 F. Supp. 525, 531-32 (D. Colo. 1986).

[195]*Id.* at 532.

[196]*Id.*

[197]A number of other cases allowed for wholesale seizure of computer equipment for later off-site sorting without additional approval from a magistrate essentially applying the closed

B. The Problem of Intermingled Documents

The problem of over broad searches and seizure arise when executing warrants to search the contents of computer storage devices. The hard drives of computers frequently store information of various types and many people use their computers as repositories for both business and personal information. The problem arises when information related to criminal activity and subject to lawful search and seizure is intermingled with personal information not subject to seizure that is likely to be the case with computer storage. In *Andresen v. Maryland*, the Supreme Court recognized the problem of intermingled documents when it noted the following:

We recognize that there are grave dangers inherent in executing a warrant authorizing the search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable. In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. . . . In . . . searches, responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.[198]

Because computers contain a large quantity and variety of information, police must conduct searches carefully to prevent unwarranted intrusions on privacy warned of in *Andresen*.[199]

In *United States v. Tamura*, the Ninth Circuit court addressed the problem of intermingled documents directly and formulated a special method for handling these searches.[200] Although this search did not involve computer files, the principles apply well to search of computerized files. In *Tamura,* the police had a warrant that listed three specific categories of accounting records that the government could properly seize.[201] The records that the officers were looking for were intermingled with thousands of other accounting records and finding any one item of evidence involved

---

container analogy to computer equipment. *See*, United States v. Longo, 70 F. Supp.2d 225 (W.D.N.Y. 1999) (allowing broad search of computer files); United States v. Gawrysiak, 972 F. Supp. 853 (D. N.J. 1997) (seizing all computer files without determination of those relevant to the scope of the search warrant was permissable and did not allow for blanket suppression of all evidence), *aff'd*, 178 F.3d 1281 (3d Cir. 1999); United States v. Kufrovich, 997 F. Supp. 246 (D. Conn. 1997) (permitting blanket seizure of computer without any on-site sorting for evidence relevant to the crime under investigation); United States v. Stewart, No. CRIM.A. 96-583, 1997 WL 189381 (E.D.Pa. Apr. 16, 1997) (allowing seizure of all computer hardware and software along with a large quantity of documents for later review off-site); United States v. Hersch, No. CRIM.A. 93-10339-Z, 1994 WL 568728 (D. Mass. Sept. 27, 1994) (finding that a search warrant calling for the seizure of all computer hardware, software and related equipment was not a general search given the complexity of the scheme under investigation).

[198]Andresen v. Maryland, 427 U.S. 463, 482 (1976).

[199]*Id.* at 463.

[200]United States v. Tamura, 694 F.2d 591 (9th Cir. 1982). *See also*, United States v. Shilling, 826 F.2d 1365 (4th Cir. 1987), *cert. denied*, 484 U.S. 1043 (1988); United States v. Abram, 830 F. Supp. 551, 554 (D.Kan. 1993) (citing *Tamura*, and holding that large seizure of intermingled documents for later sorting without judicial supervision violated the Fourth Amendment).

[201]*Tamura*, 694 F.2d at 594.

tracing the transaction through a string of printouts.[202] After searching for records for a short time the agents felt that the process would take inordinate amounts of time unless the employees of the suspect company assisted them in their search.[203] The employees refused to help the officers whereupon they seized all of the company's accounting records for the years in question, removed the records to another location, and sifted through the records to extract the evidence at a later date.[204] As a result of seizing all of the accounting records for several years, the government took large quantities of documents that the search warrant did not list.[205]

In *Tamura*, the government argued that since the documents were intermingled and separating those described in the warrant from irrelevant ones was difficult, the wholesale seizure for later sorting off-site was reasonable.[206] The suspect argued that the government should have remained on the premises until all relevant items were found or should have obtained an additional warrant to seize all of the accounting records.[207] The court stated that such a wholesale seizure of items not listed in the warrant for later examination did not comport with the requirements of the Fourth Amendment.[208] The court stated that "[i]n the comparatively rare instances where . . ." relevant and irrelevant documents are so intermingled such that sorting on-site is not practical, the court stated that the government should seal the records and a neutral magistrate should approve any further search.[209] "If the need for transporting the documents is known to the officers prior to the search, they may apply for specific authorization for large-scale removal of material, which should be granted only where on-site sorting is infeasible and no other practical alternative exists."[210] The *Tamura* court noted that the essential safeguard is that in a wholesale removal of documents a neutral magistrate must monitor the process.[211] Simply because wholesale removal is convenient to the government, when a neutral magistrate has not monitored it, does not make it reasonable.[212] The court did note, however, that "where the Government's wholesale seizures were motivated by considerations of practicality rather than by a desire to engage in indiscriminate 'fishing'" the seizure may be reasonable.[213] In *Tamura,* the government found it convenient to seize a large volume of paper documents containing both relevant and irrelevant information. Government seizure of an entire personal computer and hard disk that

---

[202] *Id.* at 594-95.

[203] *Id.* at 595.

[204] *Id.*

[205] *Id.*

[206] *Tamura*, 694 F.2d at 595.

[207] *Id.*

[208] *Id.*

[209] *Id.*

[210] *Id.* at 596.

[211] *Tamura*, 694 F.2d at 595.

[212] *Id.*

[213] *Id.* at 597.

is small and easy to transport for later off-site sorting may be a tempting alternative. In addition, in the age of computerization, the cases of intermingled documents will no longer be comparatively rare but more than likely the case. Next we will examine several cases that apply elements of the *Tamura* test to computer search and seizure.

In *United States v. Upham*, the government obtained a warrant to search a suspect's computer for images of child pornography.[214] The warrant listed material to be seized with particularity and among other items it authorized seizure of "any and all computer software and hardware, . . . computer disks, disk drives . . . Any and all visual depictions, in any format or media, of minors engaging in sexually explicit conduct."[215] The court indicated that if the images could have been obtained easily by on-site inspection and sorting there would be no justification for wholesale seizure of the computer hardware that contained intermingled relevant and irrelevant files.[216] However, the court went on to note that it is not an easy task to search every item of a hard drive, here even searching for previously deleted information that the police recovered, looking for relevant information.[217] The record in this case showed that the off-site search for images could not have readily been done on-site and based on considerations of practicality the court allowed the wholesale seizure.[218] The warrant in *Upham* fulfilled the requirements of *Tamura* in that the warrant specifically authorized, in advance, the wholesale seizure of the computer equipment allowing the later off-site sorting of the information.[219] In an additional twist the court allowed admission of evidence of images that the suspect had previously deleted from his hard drive, finding that the recovered files were competent evidence of possession of the images prior to their deletion.[220] The government used a utility program to recover the previously deleted material and the court found that this "is not different than decoding a coded message lawfully seized or pasting together scraps of a torn-up ransom note."[221]

---

[214]United States v. Upham, 168 F.3d 532 (1st Cir. 1999).

[215]*Id.* at 535.

[216]*Id.*

[217]*Id.*

[218]*Id.*

[219]*Upham*, 168 F.3d at 532.

[220]*Id.* at 537. The admission of the evidence of the files, previously deleted by the suspect, that the government recovered using a utility program was erroneous. First, the government had sufficient evidence from files that the suspect had not deleted and this additional evidence was not necessary to obtain a conviction. Second, allowing evidence of recovered, previously deleted files does not allow for possible inadvertent acquisition of unwanted files by a computer user. Take for example a computer user who receives and e-mail message with an attached graphics file. Until the computer user instructs the computer to download the image, and subsequently opens the image with software the computer user has no knowledge of what the image contains. If after downloading and accessing the file the user finds the image of no use, offensive, or simply needs to clear hard disk space the user can delete the file. In such a case, the image was innocently obtained and should not be allowed as evidence if the government later recovers the image.

[221]When files are deleted from a hard drive a computer user can often recover the information using a utility program or the undelete function of the computer. Until the hard

United States v. Sissler involved a prosecution for sale and distribution of illegal drugs in which the police executed a search warrant authorizing the seizure of drugs, related paraphernalia, proceeds, records of drug transactions, records of marijuana customers, and suppliers among other items.[222] Officials seized a large number of documents, around five hundred computer disks and a personal computer.[223] Both the computer and disks contained a large number of items that the search warrant did not authorize.[224] Citing *Tamura,* the court noted that practical considerations justified the large seizure and not a desire to go on an indiscriminate "fishing" expedition.[225] Regarding the computer and the disks, the court noted that the suspects had often used passwords and other security devices to prevent access to the stored files and as such accessing the computer files was a relatively complex and time consuming procedure.[226] The police brought in a computer expert to "crack" these security measures and gain access to the information, a process that took a great deal of time and effort and could not reasonably be accomplished on-site.[227]

United States v. Abram involved another situation in which the police seized a large volume of items beyond those described in the warrant, and the seizure was found to violate the test in *Tamura*.[228] The warrant authorized agents to seize information primarily related to insurance income proceeds and premium payments and also computers and related equipment.[229] The government seized entire filing cabinets, a computer and a small green filing box without making any review of the contents before the seizure.[230] One officer later testified that it took no more than five to ten minutes to review the contents of the seized items to determine if they contained evidence relevant to the investigation and that undertaking this review on-site would not have been burdensome.[231] The court found that this case was unlike *Tamura* where practical considerations motivated the wholesale seizure, and found that agents have seized all documents they found simply for their own convenience without any review regarding relevance.[232] The court found that the agents had acted

---

drive space, previously occupied by the deleted information, is overwritten with new information this is generally possible. The court noted that the recovered images were competent evidence of a crime committed before they were deleted.

[222]United States v. Sissler, No.1:90-CR-12, 1991 WL 239000 (W.D. Mich. 1991).

[223]*Id.* at *4.

[224]*Id.*

[225]*Id.* at *3.

[226]*Id.* at *4.

[227]*Sissler*, 1991 WL 239000 at *4.

[228]United States v. Abram, 830 F. Supp. 551 (D. Kan. 1993).

[229]*Id.* at 552.

[230]*Id.* at 552-53.

[231]*Id.*

[232]*Id.* at 556.

"in flagrant disregard for the terms of the search warrant issued" and ordered all evidence suppressed.[233]

The approach set forth in *Tamura*[234] is a useful one which should be followed. If applied properly, the *Tamura*[235] procedure will provide that legitimate searches of computers are conducted in the least intrusive way possible. There are, however, problems with the approach as proposed in *Tamura*.[236] Although the court suggested that when wholesale seizure is to be anticipated, this should be indicated in the initial application for a search warrant. But the court went on to note that when the police arrive on the scene and find that practical considerations make on-site sorting for relevant information impossible, a wholesale seizure of files and equipment may be justified even if authority to do so was not applied for in advance. While there have been a limited number of cases involving computer search and seizure that followed *Tamura,*[237] it appears all too easy for police to show "practical considerations" to justify wholesale seizure and later off-site sorting for relevant information. Taken together, *Sissler*[238] and *Upham*[239] indicate that courts accept the assertion of "practical considerations" all too readily. In addition, there was no information in *Upham*[240] and *Sissler*[241] to suggest that the later off-site sorting was further supervised by judicial authority as *Tamura*[242] suggested was appropriate. In *Abram*,[243] the court excluded the evidence only because the government admitted that they made no attempt to sort the information prior to the wholesale seizure of the intermingled files.

The government's actions should not need to rise to this level to invoke the protections of *Tamura*.[244] How long should the government be required to stay on-site to sort for relevant documents? The courts simply do not provide any objective standards against which to judge the reasonableness of the government's assertion of "practical considerations" when providing a justification for a wholesale seizure of computer equipment. One can hardly imagine any case involving search of a computer hard drive, that may contain tens of thousands of intermingled relevant and irrelevant files, where a case could not be made that it is impracticable to sort through this mass of data on-site. Indeed, such a process would be time consuming. On the other hand, operating systems like Windows provides search engines which

---

[233] *Abram*, 830 F. Supp. at 556-70.

[234] *Tamura*, 694 F.2d at 591.

[235] *Id.*

[236] *Id.*

[237] *Id.*

[238] *Sissler*, 1991 WL 239000.

[239] *Upham*, 168 F.3d at 532.

[240] *Id.*

[241] *Sissler*, 1991 WL 239000.

[242] *Tamura*, 694 F.2d at 591.

[243] *Abram*, 830 F. Supp. at 551.

[244] *Tamura*, 694 F.2d at 591.

allow one to quickly narrow the search for relevant documents. It could be argued that searching for relevant documents on a computer hard drive, with the aid of search engines and utility programs, may actually be more efficient than manually searching through a large paper file cabinet unaided by technology. Allowing wholesale seizure of entire computers allows possible intrusions into private matters that have no relevance to commission of any crime. In addition, a computer user may make use of the equipment for a variety of purposes both criminal and legitimate. If the entire computer is seized to allow off-site sorting for relevant information, the users entire legitimate, business and personal life may be unreasonably disrupted in the process. A citizen should be able to pursue his legitimate business interests even while under investigation for an alleged criminal violation. Only through strict application of the *Tamura* approach to computer searches and seizures can peoples' legitimate privacy interests be adequately protected. The courts have simply applied the *Tamura*[245] approach far too carelessly.

The cases applying the closed container analogy to computer searches and seizures and allowing wholesale seizure of equipment for later off-site sorting are far more numerous than the cases which follow the *Tamura*[246] approach. Taken together, these "closed container" cases present several dangers. First, the government is given virtually free rein to seize computer systems and computer storage media when such items are not specified in the warrant. The courts have upheld, on many occasions, very broadly worded warrants. Second, unlike the *Tamura*[247] approach, these cases do not require the government to undertake any on-site sorting of relevant from irrelevant documents or a showing of practical considerations that such on-site sorting is not possible prior to a wholesale seizure of computer equipment. The privacy interests of the citizen who is under investigation are weighed against the convenience of the government in performing their investigative functions, and the balance is struck in favor of the interests of government convenience. If the government is compelled to follow the *Tamura*[248] approach, computer searches and seizures will be undertaken in the least intrusive way possible. This, however, is not the trend in which computer search and seizure cases are headed; the trend is headed, in fact, in the direction of allowing searches and seizures to be undertaken in a manner that allows greater and greater invasion of government into personal privacy.

VI. THE SUBPOENA PROCESS

Thus far this note has examined searches and seizures of computers in the context of search warrants and the different approaches that courts have taken in construction of warrants. There have been a limited number of cases involving government attempts to gain access to computerized evidence of a crime that involved grand jury subpoenas rather than search warrants. Reported cases of this process are few in number. They do, however, provide useful lessons with regard to how investigations of crimes that involve computers, at least in certain contexts, may be more

---

[245] *Id.*

[246] *Id.*

[247] *Id.*

[248] *Id.*

appropriately undertaken. The subpoena process generally analogizes computer equipment to a file cabinet rather than the "closed container" analogy that we have already examined.

In re Horowitz involved a grand jury subpoena for records that were not computerized.[249] The subpoena required a suspect's accountant to produce "the contents of all three file cabinets" located at the accountant's office.[250] Prior to the production of any documents the accountant challenged the subpoena arguing that the request for the contents of entire file cabinets, without regard to the relevance of what they contained, was overly broad.[251] The district court narrowed the subpoena to exclude personal documents contained in the filing cabinets.[252] The Second Circuit further narrowed the subpoena indicating that "the government must make a minimal showing that, in light of other evidence that has been obtained, the paper may be relevant to the grand jury's investigation of a federal crime."[253] The court allowed that if the defendants can show "that a particular category of documents can have no conceivable relevance to any legitimate object of investigation" they need not be produced.[254] This decision indicates that subpoenas should not be directed at whole filing cabinets, but at categories of documents that the cabinets may contain that may be relevant to investigation of a crime. Essentially, the person served with a subpoena is permitted to sort through and produce only documents relevant to the crime under investigation.

In re Subpoena Duces Tecum,[255] the court applied the approach in *Horowitz*[256] directly to a subpoena aimed at computer equipment.[257] The subpoena demanded production of computer hard drives, and floppy disks that the grand jury conceded contained information irrelevant to the investigation rather than being directed at categories of information contained on the computerized media.[258] The court noted that the government admitted that the subpoena demanded production of various irrelevant documents and that a "key word" search would readily reveal which items where relevant to the investigation.[259] The court went on to note that if the grand jury had reason to believe that relevant documents were being withheld, a court appointed expert could be used to search the computer equipment for relevant

---

[249]*In re* Horowitz, 482 F.2d 72, 73 (2d Cir. 1973), *cert. denied* 414 U.S. 867 (1973).

[250]*Id.* at 74.

[251]*Id.* at 74-75.

[252]*Id.* at 75.

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

[254]*Horowitz*, 482 F.2d at 80.

[255]*In re* Grand Jury Subpoena Duces Tecum dated Nov. 15, 1993, 846 F. Supp. 11 (S.D.N.Y. 1994).

[256]*Horowitz*, 482 F.2d at 72.

[257]*In re* Subpoena Duces Tecum, 846 F. Supp. at 12-13.

[258]*Id.* at 12.

[259]*Id.* at 13.

information.[260] The subpoena was quashed in its entirety since it unnecessarily demanded that irrelevant documents be produced.[261]

The file cabinet analogy is much more appropriate to a search of computer files than the closed container analogy that has been predominately followed regarding search and seizure of computer files. The closed container analogy allows for unlimited intrusion into the contents of a computer's storage without a showing of relevance. Just as police sort through the contents of paper filing cabinets, seizing only those documents that appear relevant to their investigation, so should they be required to sort through the storage devices of computers that are the object of investigation. First, it appears from the case law that courts are simply too willing to allow wholesale seizure of computers containing intermingled relevant and irrelevant documents. Second, we must ask why police tend to cart away entire computers while not taking with them large numbers of filing cabinets? The answer is simple--an entire personal computer is small and weighs only around fifteen pounds and is easy to take. It is not so simple to cart off the entire contents of ten or fifteen file cabinets full of paper documents.

The subpoena process, unlike the use of search warrants, requires the government to make some showing of relevance prior to the production of documents that are requested. In addition, the person served with a subpoena has the right to challenge the request prior to production of any of the information. This additional protection is not available to a citizen served with a search warrant. The Supreme Court noted that a search warrant is preferable in circumstances where it "is necessary to secure and to avoid the destruction of evidence."[262] The cases involving subpoenas involved financial and business related crimes in which destruction of evidence is not great a danger. First, if the focus of the subpoena is a professional, like the accountant in *Horowitz*,[263] the person served with the subpoena may not be under investigation but merely in possession of relevant records. There would be, therefore, no motivation to destroy evidence to avoid prosecution. Second, if the crime involves a financial scheme, relevant documents are likely to be found in the possession of persons other than those suspected of criminal activities. If the crime involved customers, banks, or other financial institutions, copies of relevant documents can be obtained from these sources even if the suspect destroys computerized records in the face of a subpoena. In addition, destruction of documents relevant to a grand jury subpoena would constitute an additional crime for which the suspect can be prosecuted.[264] Thus, in investigations of more complex financial transactions, where the possibility of destruction of evidence is not as great, the subpoena process should be the preferred approach.

VII. CONCLUSION

The Fourth Amendment provides an adequate framework for the protection of personal privacy interests against unreasonably intrusive searches and seizures of

---

[260] *Id.*

[261] *Id.* at 13-14.

[262] Zurcher v. Stanford Daily, 436 U.S. 547, 563 (1978).

[263] *Horowitz*, 482 F.2d at 72.

[264] United States v. Solow, 138 F. Supp. 812, 813 (S.D.N.Y. 1956).

computers and computer data. This framework, however, is only adequate if the courts interpret the contours of the Fourth Amendment in the context of changing times and circumstances. The advent of the widespread use of computer technology by large segments of the population to store a variety of information, presents the legal system with new and interesting challenges.

Several doctrines are apparent from the review of this emerging area of the law. First, the "plain view" exception to the warrant requirement will not be applied by the courts to closed files in computer storage. The only way in which a computer can be seized under the "plain view" doctrine, is in the event that some relevant evidence of criminality is prominently displayed on the computer screen. These cases are few in number with most searches aimed at the closed contents of computer memory. In such cases, the contents of computer storage are considered to carry a high level of Fourth Amendment protection and require a warrant to examine the contents of any files.

Second, although informant information can prove useful to the government, any such information must be used with great care. If the circumstances of the informant's actions are directed by or motivated by a desire aid the government, the informant provided information will not be useable. In addition, in cases where judging the nature of the content of computer files requires expertise, courts may not find the conclusions of the informant dispositive or a proper basis to support probable cause for a warrant. Judging what constitutes child pornography may not be within the grasp of average citizens. Defendants may be able to successfully challenge the state's use of conclusory informant statements.

The reported cases to date indicate that search warrants for computers are construed broadly and the analogy of the closed container is used by most courts in establishing the scope of the searches and seizures. This analogy is dangerous. If viewed as a closed container, a warrant authorizing search of computer memory provides a virtually unlimited right, on the part of the police, to review the contents of any files with any sorting as to relevance. Once you have the right to open a closed container that means that you may look at anything contained therein. This analogy is too simplistic and allows for search and seizure of computer to proceed in a very intrusive manner and should be abandoned.

The Ninth Circuit in *Tamura*[265] proposed that computer storage should be analogized to a filing cabinet. This approach recognizes certain aspects of computer storage that the closed container analogy ignores. First, a computer hard drive often contains tens of thousands of files that contain a mixture of personal files, in which the state does not have a legitimate interest, intermingled with those that may contain evidence of some crime. *Tamura*[266] suggests that police should be required to perform on-site sorting of computer data to isolate relevant from irrelevant, and possibly highly personal, data if at all possible. If on-site sorting is not possible, the later sorting requires supervision from an independent magistrate and a showing of the practical considerations that prevented the on-site sorting. In addition, *Tamura*[267] held that if the police feel that wholesale seizure of computer equipment will be

---

[265]*Tamura*, 694 F.2d at 595.

[266]*Id.*

[267]*Id.*

required, approval for this should be obtained in advance at the time of warrant application. The courts have, however, been all too willing to accept the government's assertions of practical considerations making on-site sorting of data impossible. The *Tamura*[268] approach is not valuable unless the courts apply its requirements strictly and consistently the state's interests and convenience will continue to be placed above those of personal privacy.

Finally, as an additional protection against invasion of personal privacy, the subpoena process should be the preferred approach to investigations of computer based crime if at all possible. Unlike the warrant search the legal process is available to challenge overly broad subpoenas prior to producing the information. Generally some minimal showing of relevance is required for subpoena to survive a challenge as to breadth. Obviously, the subpoena process is only appropriate in certain cases where the destruction of evidence is not probable. This may be the case in investigations or complex financial schemes. In child pornography cases, destruction of evidence is a real possibility and warrants should be used, but the warrants should be used in strict compliance with the requirements of *Tamura.*[269]

If these suggestions are followed, search and seizure of computers will proceed in a manner that properly balances the interest of society in prosecuting crime with those of personal privacy such that the process proceeds in the least intrusive manner possible. If the courts continue down the road of liberalizing search and seizure in favor of the convenience of the government, the trend towards erosion of Fourth Amendment privacy protections will continue. The courts can and should stop this trend.

DONALD RESSEGUIE

[268] *Id.*

[269] *Id.*