Warrant Searches of Computers

Jeff Welty

School of Government

June 2009

I. Searches of computers are increasingly important

Computers now permeate all strata of society and all aspects of people's lives. Unsurprisingly, then, computers are often used to commit, or contain evidence of, crimes. This is obviously true of computer-specific crimes, such as the computer fraud and computer trespass crimes in G.S. 14-453 et seq. It is also true of a category of crimes that, while theoretically not computer-specific, are in fact committed almost exclusively by means of or with the assistance of a computer. The production, distribution, and possession of child pornography is a prime example, but identity theft and certain forms of intellectual property piracy also fall in this category. Furthermore, computers may play a part in the commission of, or may contain evidence of, crimes that are not inherently tied to computers at all, such as murder (one recent case involved evidence that the defendant had Googled "how to dispose of a body"), drug distribution (computers may contain customer lists), and the like.

This paper focuses on searches of computers pursuant to a search warrant. Probable cause to support the issuance of a search warrant may arise in any number of ways. A spouse, roommate, or computer repairperson may accidentally discover child pornography on a suspect's computer and report it to police. See, e.g., State v. Dexter, __ N.C. App. __, 651 S.E.2d 900 (2007). A police officer posing as a minor may communicate with a sexual predator over the internet. See, e.g., State v. Ellis, __ N.C. App. __, 657 S.E.2d 51 (2008). Or, police may have developed probable cause to search a home for evidence of a crime, and may seek to search a computer simply as one facet of the broader search. See, e.g., State v. Peterson, 179 N.C. App. 437 (2006), aff'd, 361 N.C. 587 (2007). Of course, similar fact patterns may arise with respect to cellular phones or other electronic devices, and similar legal principles will apply.

One final caveat. While this paper is written with a North Carolina audience in mind, our appellate courts have decided relatively few cases concerning searches of computers. Therefore, most of the cited cases are federal cases, to which our trial and appellate judges might reasonably look for guidance.

II. Apparent and concealed data

Although this paper is not intended to be technical, it is worth describing briefly the ways in which data can be stored on a computer. Sometimes, computers contain valuable evidence that is stored in an obvious location, such as copyrighted music stored in the user's music library. But computers may also contain valuable evidence in less-obvious locations. And sometimes, computers contain evidence that users have gone to great lengths to hide or delete. Thus, rather than simply clicking through the file directory on a computer, law enforcement may seek authorization to search the computer using sophisticated forensic software – or may employ such software routinely, without specific authorization.

A. Apparent Files

Virtually all computers contain word processing documents, spreadsheets, and other files created by office or productivity software. Many contain photographs, videos, and audio files. Many have financial records created using Quicken or other financial software. A typical user makes no effort to hide these files, and any computer user who inspected the computer would be able to locate them easily. Using the Windows operating system, for example, the typical user will save word processing files in the "My Documents" folder (or a subfolder therein), and if the documents are created in Microsoft Word, they will be associated with a Word logo and will carry a .doc file extension.

If a computer has ever been used for web browsing, it will also normally contain information about the web sites it has visited. Obtaining this information requires a little more computer knowledge than, say, viewing a word processing document as described above, but not much, at least in some instances. For example, most web browsers have a history feature. The browser saves a list of all the web sites the computer has visited over the past few weeks or months, and upon command, the browser can display the list. Similarly, many web sites use "cookies" – small files automatically saved on the user's computer when the user first visits a particular web site – as a way of recognizing repeat visitors. Looking at the cookies saved on a computer will reveal many web sites recently visited by the computer. Other forms of temporary internet files may also be found on most computers.

B. Camouflaged files

If a user has information on his or her computer that the user does not want others to see – such as a spouse, a computer repair technician, or law enforcement – he may take steps to camouflage the files. At the simplest level, giving a file a misleading title, such as saving a child pornography photograph as "familyvacation002.jpg" may provide some concealment. Another common technique is changing the file extension. Saving the child pornography photograph as "familybudget.xls" will make it look like a Microsoft Excel Spreadsheet to the casual observer.

C. Encrypted files

More sophisticated users may use encryption to prevent others from accessing their files. An encrypted file is one that has been saved using a special code so that the file is unreadable unless it is decoded – and it cannot be decoded without a password. The codes used by the best modern encryption systems are practically unbreakable. Thus, if the police seize and search the computer of a drug dealer who stores all his business records and customer lists in encrypted word processing documents, they are not likely to obtain any readable, useful evidence unless they can guess the drug dealer's password.

D. Deleted files

Many computer users believe that once a file has been deleted, it is gone and cannot be recovered. In fact, when a file is deleted, the disk space where that file was stored is marked "available" by the operating system, but the file is not actually erased. Unless and until the disk space is actually used to save another file, the previous file remains on the disk, even though the operating system has "officially" marked the file as deleted. (It is a bit like removing the card catalog card for a book, but leaving the book on the shelf.) Given that most people have large amounts of empty space on their disk drives, and save

additional items to disk infrequently, deleted files often remain on disk drives for weeks, months, or years. A computer analyst can look through a disk drive using special software and find these deleted files.

Even if the area of the disk that was previously used to store the deleted file has been used to store a new file, some portion of the deleted file may remain. Disk drives are divided into chunks, or sectors, and most files take up a fraction of a sector (whether 2.04 sectors, or 40.77 sectors, the point is that most files don't take up exactly 3.00 or 158.00 sectors). When a file that took up 2.87 sectors is "deleted," and the disk space is later overwritten by a new file that takes up 2.12 sectors, only 12% of the third sector used by the new file is actually overwritten. Since the deleted file used 87% of that third sector, there is still a fragment of the deleted file on the disk, and a computer forensic analyst will be able to locate that fragment and see what it contains.

If a sector has been completely rewritten with a new file, or has been "zeroed," i.e., written over by a computer with meaningless material, the deleted file probably cannot be recovered using current technology. However, it may be possible in the future to recover the deleted file even under these circumstances.

E. Other evidence

There are other ways to recover information from a computer. For example, some recently-used information may be stored in the computer's RAM, for ready access. And because the field of computer forensics is rapidly evolving, additional ways of extracting information from computers (as well as additional ways of hiding or removing such information) are sure to be invented. Indeed, with the rise of solid-state disk drives (SSDs), which record and delete information in a slightly different way than traditional spinning hard disks, new techniques are sure to emerge.

III. Many computer searches require a warrant

Generally, people have a reasonable expectation of privacy in the contents of their computers. See, e.g., United States v. Lifshitz, 369 F.3d 173 (2d Cir. 2004); Guest v. Leis, 255 F.3d 325 (6th Cir. 2001). But cf., e.g., United States v. Angevine, 281 F.3d 1130 (10th Cir. 2002) (no reasonable expectation of privacy in employer-owned computer where employer had a clear policy that the computer and its contents were not confidential); United States v. Ganoe, 538 F.3d 1117 (9th Cir. 2008) (no reasonable expectation of privacy in a computer on which file-sharing software was installed and active); United States v. Caymen, 404 F.3d 1196 (9th Cir. 2005) (no reasonable expectation of privacy in a computer obtained by fraud). Thus, searches of computers normally must be conducted pursuant to a warrant. Of course, the police may legally search computers without a search warrant under certain circumstances, such as when the owner of a computer consents to a search, or when the police have probable cause to believe that a computer contains evidence of a crime and exigent circumstances require that the police search the computer immediately. However, such searches are beyond the scope of this paper.

In some instances, it may be necessary and appropriate to issue multiple warrants to search a single computer. For example, suppose that the police develop probable cause to believe that a person is involved in preparing fraudulent tax returns, and obtain a warrant to search his computer for evidence of

that offense. Then, while searching the computer, an officer inadvertently discovers evidence of child pornography. If the officer wants to continue looking for child pornography, at least in files and locations that are not likely to contain evidence of tax fraud (such as video files, perhaps), he may need a separate search warrant authorizing a search for child pornography. See, e.g., United States v. Carey, 172 F.3d 1268, 1270 (10th Cir.1999) (warrant authorizing search for evidence of drug offenses did not permit search of numerous image files with sexually suggestive names, that turned out to contain child pornography).

IV. Showings of probable cause

An application for a warrant to search a computer must establish probable cause to believe that the computer contains evidence of, or was used in, a crime. Although probable cause is a familiar standard, there are at least two specific, recurrent issues that arise with respect to computer search warrants.

A. Descriptions of child pornography

First, many computer search warrants are issued based on probable cause to believe that the suspect's computer contains images of child pornography. Sometimes the applicant has seen the images himself, while sometimes he has not viewed the images but has been told about them by, for example, a computer repair technician. In order for a judicial official to make an independent determination about whether the images are likely child pornography, the judicial official probably must (1) view the images (they may be attached to application in a sealed envelope), or (2) receive a detailed description of the images that allows the judicial official to reach an *independent* conclusion about the content of the images. A statement from the applicant that the images "are child pornography" is probably insufficient, as it does not provide factual information that the judicial official can use to determine probable cause. See, e.g., United States v. Brunette, 256 F.3d 14 (1st Cir. 2001) (an officer determined that the defendant had posted several images online; the officer applied for a search warrant for the defendant's computer, describing the images only as "a prepubescent boy lasciviously displaying his genitals," parroting the language of 18 U.S.C. §2256(2)(E), which defines such genital displays as child pornography; the reviewing court held that description was conclusory and failed to provide probable cause; generally, "[a] judge cannot . . . make this determination without either a look at the allegedly pornographic images, or at least an assessment based on a detailed, factual description of them"); United States v. Battershell, 457 F.3d 1048 (9th Cir. 2006) (defendant's girlfriend showed a police officer several pictures she had found on defendant's computer; the officer then applied for a warrant to search the computer for child pornography; he did not attach the images; he described the images as showing "a young female (8-10 YOA) naked in a bathtub" and "another young female having sexual intercourse with an adult male"; the reviewing court found that the former description was insufficient to show probable cause that the computer contained child pornography, as opposed to, say, a family photograph, but that the latter was sufficient, especially combined with the girlfriend's statement that the computer had pictures of "kids having sex"; although it "would have been preferable if the affiant in this case had included copies of the photographs in the warrant application," an officer's failure "to include a photograph in a warrant application is not fatal to establishing probable cause"). But cf. United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998) (warrant application established probable cause to believe that the defendant's computer

would contain child pornography despite failure to attach or describe images, where the defendant had engaged in online "chat" with undercover officer and had offered to supply computer disks with images of pre-pubescent children engaged in sexual activity).

Second, when an officer applies for a search warrant based on information that is several weeks or months old, the judicial official should consider whether the information continues to provide probable cause or whether it has become outdated, or "stale." This issue has been litigated most often in connection with child pornography cases. Some courts have recognized that people who obtain child pornography tend to hoard, or retain it, meaning that evidence that a person obtained digital child pornography months, or even years, ago may provide probable cause to believe that the person's computer will contain child pornography. See, e.g., United States v. Riccardi, 405 F.3d 852 (10th Cir. 2005) ("Since the materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to destroy them." (quoting United States v. Lamb, 945 F.Supp. 441, 460 (N.D.N.Y.1996))). Other courts have been less willing to find probable cause based on information that is not recent, at least absent a specific reason to believe that the particular suspect at issue is likely to have retained the pornographic images. See, e.g., United States v. Greathouse, 297 F. Supp. 2d 1264 (D. Or. 2003) (evidence that, thirteen months prior to the issuance of a search warrant, the defendant shared child pornography from his computer with other people over the internet was stale; there was no evidence of more recent, or ongoing, criminal activity; no evidence that the defendant was a pedophile and so especially likely to hoard such material; and computer technology evolves quickly, so that whole hard drives become obsolete or are replaced frequently; the court also noted that the government presented no empirical evidence that people who obtain child pornography are prone to keep it for protracted periods); cf. United States v. Zimmerman, 277 F.3d 426 (3d Cir. 2002) (police suspected that the defendant had showed a single adult pornography video to minors six, ten, or more months earlier; they applied for and obtained a search warrant authorizing a search of the defendant's computers for child and adult pornography; the Third Circuit ruled that there was nothing at all to support a search for child pornography, and as to adult pornography, the evidence was stale; there was no reason to believe that the defendant would have kept the video for a long period of time, since unlike child pornography, it was presumably legal and easy to obtain; the court also expressed doubt about the utility of boilerplate affidavits about the tendency of pedophiles to hoard child pornography absent some knowledge of the specific defendant and case).

V. The scope of the warrant

Another area in which computer search warrants can be tricky concerns the scope of the search authorized by the warrant.

First, although a warrant must particularly describe the location to be searched, it does not always need to include computer-specific language to authorize the police to search computers. The general rule is that a warrant authorizing the search of a particular location for a particular item also authorizes the search of any closed container at the location if the item might reasonably be found inside the container. Wayne R. LaFave, Search and Seizure § 4.10(b) (4th ed. 2004); cf. United States v. Ross, 456 U.S. 798 (1982) (expressing a similar rule as to warrantless vehicle searches). Thus, a warrant authorizing the search of a home for records of drug sales, lists of drug customers, etc., also authorizes the search of any

container within the home in which the records could reasonably be found. Several courts have applied this rule to hold that a warrant need not specifically refer to the existence of a computer in order to authorize a search of the computer, so long at the items or evidence sought might reasonably be found on the computer. See e.g., United States v. Giberson, 527 F.3d 882 (9th Cir. 2008) (holding that a search warrant authorizing a search for "documents," without mentioning computers or electronic storage, allowed police to search computers, as documents may be found in computers); United States v. Hudspeth, 459 F.3d 922 (8th Cir. 2006), rev'd in part on other grounds, 518 F.3d 954 (8th Cir. 2008) (en banc) (upholding a computer search conducted pursuant to a warrant allowing the search of any and all "records or documents regarding sales, payables, inventory, customer lists, financial statements, and personnel files" but not specifically mentioning computers: "While the inclusion of the word 'computer' would have specified one location among several where the officers might look for those items, its omission did not prevent the officers from searching [a] computer for such records."); cf. United States v. Hunter, 13 F.Supp.2d 574 (D. Vt. 1998) (proper for warrant to authorize search of computers although nothing in the warrant application showed that the records the police sought were specifically likely to be stored on computer; most businesses' records and documents are stored that way).

Second, when confronted with a warrant application that does contain computer-specific language, a judicial official should carefully consider whether the probable cause that supports the warrant extends to the particular computers or other devices in question. If not, the warrant will be overbroad. For example, in State v. Peterson, 179 N.C. App. 437 (2006), aff'd, 361 N.C. 587 (2007) , the Court of Appeals ruled that the police had probable cause to believe that a woman had been murdered at her home, and they properly obtained a search warrant to search for and seize fingerprints, hair, fiber, weapons, etc. However, the court determined that a separate warrant, authorizing the police to seize "computers, CPUs, files, software, accessories and any and all other evidence that may be associated with this investigation," was overbroad as there was no probable cause to believe that the computers at the home would contain any relevant evidence. By contrast, in United States v. Summage, 481 F.3d 1075 (8th Cir. 2007), the police suspected that the defendant had paid a mentally handicapped man to engage in a sex act with a woman, and had videotaped and photographed the encounter. The officer applied for a warrant to search the defendant's home and to examine "[a]ll video tapes and DVDs . . . [a]ll video and/or digital recording devices and equipment . . . [and] computer(s)." In the course of the search, the officer found some child pornography among the digital media, leading to charges against the defendant. The defendant moved to suppress, arguing, among other things, that the warrant was overbroad in authorizing a search of all the digital media. The Eighth Circuit held that there was probable cause to believe that the video and photographs would be stored digitally, and that the officer had no way to know the format or device in which the video and photographs would be found, and that it was therefore reasonable to believe that the video and photographs might be present in any of the digital media. Thus, the search was upheld.

Third, the warrant must particularly describe the items to be seized. It is important to recognize that computers and electronic devices are normally *locations to be searched*, while files or data, not the physical computers themselves, are the items to be seized.[1] Thus, the warrant should describe the files or

[1] There are exceptions to this rule. For example, if a suspect is believed to have stolen a particular computer during a break-in, and the police obtain a search warrant for suspect's home, the computer itself would be an item to be seized, regardless of what files or data it might contain.

data as specifically as possible, not merely the computers or devices. However, courts have recognized that computer searches are similar to searches for incriminating documents, in that officers often do not know exactly what type of information the search will uncover. Thus, courts have allowed somewhat flexible descriptions. See, e.g., United States v. Hunter, 13 F.Supp.2d 574 (D. Vt. 1998) (upholding a warrant authorizing a search of a suspect's office and computer for documents related to money laundering; the warrant was sufficiently specific because it identified a particular offense and included an illustrative list of types of documents that would be relevant; although officers would have to make some judgments about which documents met the description, and would necessarily scan many irrelevant documents, no greater specificity was possible in advance). This flexibility is not infinite; search warrants that have not limited the items to be seized to, for example, evidence of a particular offense have been held to lack particularity. See, e.g., United States v. Riccardi, 405 F.3d 852 (10th Cir. 2005) (warrant in child pornography investigation authorized officers to search defendant's computer "and all electronic and magnetic media stored therein," etc.; the warrant did not specifically state that the search was limited to evidence of child pornography offenses, and "thus permitted the officers to search for anything – from child pornography to tax returns to private correspondence"; it was therefore lacking in particularity and was invalid, though the court ultimately found the search to be permitted under the good-faith exception to the valid warrant requirement).

Fourth, although in most cases, computers are locations to be searched and not items to be seized, the police will often want to take the computers off-site to search them, i.e., they will want to seize the computers.[2] Courts have often, though not always, found this to be justifiable, partly as a matter of simple practicality: a complete forensic analysis of a computer can take weeks, and it would be burdensome (to the police) and intrusive (to the computer's owner) to insist that the police remain on-site for the entire time. See, e.g., United States v. Hill, 459 F.3d 966 (9th Cir. 2006) (officers obtained a search warrant to search the defendant's computer and storage media for child pornography; they seized all his disks, etc., for off-site analysis; he argued that they should have been required to search the storage media on-site and release anything that didn't contain child pornography; both the district court and the reviewing court held otherwise, concluding that it was reasonable, given the difficult, time-consuming nature of computer searches, to take the computers off-site; the district court ruled that the defendant was entitled to copies of his data, which would ameliorate the hardship of the seizure). It is probably wise for officers to seek authorization in the search warrant to seize the computers and analyze them off-site. See United States v. Grimmett, 439 F.3d 1063 (10th Cir. 2006) (upholding warrant where the "affidavit also made clear that the search of the computer would be off-site in a laboratory setting" because only careful laboratory analysis allows all relevant evidence to be exploited).

Finally, there has been considerable debate about whether a warrant authorizing the search of a computer should include a "search protocol" that explains how the police intend to go about searching the computer. The idea is that most computers contain vast amounts of innocent, but personal, information intermixed with any incriminating information, and that the police should demonstrate that they plan to search the computer in a way that is calculated to minimize the invasion of privacy vis-à-vis the former

[2] Agents can search computers in several ways: on-site (by printing out, or copying, relevant files on the spot), by copying the computer's hard drive or other storage medium on-site, then later searching the copies off-site, or by seizing the computer and associated hardware and storage media, then later conducting an off-site search.

while unearthing the latter. Although an important early case suggested that such a protocol might be required, see United States v. Carey, 172 F.3d 1268 (10th Cir. 1999), more recent cases generally hold otherwise, see, e.g., United States v. Khanani, 502 F.3d 1281 (11th Cir. 2007) (search protocol not required); United States v. Brooks, 427 F.3d 1246 (10th Cir. 2005) ("[W]e disagree with [the defendant] that the government was required to describe its specific search methodology. This court has never required warrants to contain a particularized computer search strategy.").

VI. Special cases

A. Searching computers that may contain privileged material

Special care must be taken when searching computers that may contain privileged material, such as a computer at an attorney's office or in a medical practice. One solution is to seize the computers, then have a special master, not employed by the police or the prosecutor's office, do the search. See, e.g., United States v. Hunter, 13 F.Supp.2d 574 (D. Vt. 1998) (suggesting this procedure, though approving as a less-satisfactory alternative having the search done by officers not involved in the investigation at issue). Alternatively, a procedure may be established by which claims of privilege are resolved among the defense, a "taint team" working for the prosecution, and the court. See, e.g., United States v. Triumph Capital, 211 F.R.D. 31 (D. Conn. 2000).

B. Issues regarding multiple residents or multiple users

Sometimes the police will seek authorization to search a shared computer, or all computers in a shared residence. Such requests raise questions. For example, if two users share a computer, and the police have probable cause to believe that one of them has committed a crime of which evidence can be found on the computer, may the police search the entire computer? Even if the users have separate password-protected accounts? And, if several residents of an apartment establish a computer network, does probable cause to search one resident's computer entail probable cause to search the other computers? Few cases bear on these questions. Cf. United States v. Greathouse, 297 F. Supp. 2d 1264 (D. Or. 2003) (police obtained a warrant to search the computers at a specific residence for child pornography; upon entering, they determined that several people lived at the residence, including the defendant, who had his own bedroom with a "Do Not Enter" sign on the door; the court held that the defendant's bedroom was essentially a separate residence, for which a separate warrant was required)