Volume 8, Number 1 Fall 1994

SEARCHES AND SEIZURES OF COMPUTERS AND COMPUTER DATA

*Raphael Winick**

INTRODUCTION

In 1928, Justice Brandeis predicted:

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?[1]

Technological developments have turned Justice Brandeis' foresighted prediction into reality. One man has been sentenced to death in a kidnapping and murder case following the electronic recovery by police of ransom notes which had been previously deleted from computer disks.[2] Government monitoring of a college student's electronic bulletin board and Internet site resulted in a recent felony indictment on fraud and software piracy charges.[3] Incriminating electronic mail messages led to pending criminal charges for theft of trade secrets against high-ranking executives at software giants Symantec and Borland.[4] A 1990 FBI and Secret Service seizure of computer hardware and software from a Texas distributor of computer-related literature deprived the publisher of documents necessary to complete several books and other projects,

---

* J.D., Duke University, 1992; B.A., Brown University, 1988. The author is an associate with the New York office of Latham & Watkins.

1. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967). Although Justice Brandeis wrote these words in dissent, the Court later accepted his position and overruled the *Olmstead* majority opinion in *Katz*.

2. Commonwealth v. Copenhefer, 587 A.2d 1353 (Pa. 1991).

3. Peter H. Lewis, *Student Accused of Running Network for Pirated Software*, N.Y. TIMES, Apr. 9, 1994, at A1.

4. John Markoff, *2 Executives Indicted in Trade-Secret Theft*, N.Y. TIMES, Mar. 5, 1993, at D3; *see also* Siemens Solar Indus. v. Atlantic Richfield Co., No. 93 Civ. 1126 (LAP), 1994 WL 86368 (S.D.N.Y. Mar. 16, 1994) ($150 million securities suit filed in federal court based on incriminating electronic mail messages).

magistrate issuing the warrant for permission to remove such material; permission should be granted only when on-site sorting of relevant and irrelevant material is infeasible and no other practical alternative exists.[169] "The essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate."[170]

The leading treatise on search and seizure law and the American Law Institute's *Model Code of Pre-Arraignment Procedure* both endorse this rule.[171] As one court has noted: "The wholesale seizure for later detailed examination of records not described in a warrant is the kind of investigatory dragnet that the fourth amendment was designed to prevent."[172]

The *Tamura* rule effectively balances the privacy needs of the individual against the need for law enforcement officers to conduct searches in the course of investigating possible criminal activity. By permitting the removal of computer hardware, the *Tamura* rule anticipates the exigent circumstance that to prevent the destruction of evidence, the computer disks may need to be removed from the premises for further analysis. Practical considerations and the fear of destruction or alteration of evidence mandate that officers remove computer memory from the suspect's control when a large quantity of information is discovered.[173]

---

169. *See Tamura*, 694 F.2d at 595-96.

170. *Id.* at 596.

171. *See supra* note 163.

172. United States v. Abram, 830 F. Supp. 551, 554-55 (D. Kan. 1993) (quoting *Tamura*, 694 F.2d at 595); *see also* United States v. Robbins, 21 F.3d 297, 300 (8th Cir. 1994) (citing *Tamura*, 694 F.2d at 595 n.2, and holding that officers could not seize a wallet and search, at a later time, items intermingled in the wallet merely because the warrant permitted a search for cash receipts); People v. Economy, 631 N.E.2d 827, 833 (Ill. App. 1994) (finding no Fourth Amendment violation where police seized file cabinets in a search for drugs, since police did not look through documents contained in files).

173. Several cases have upheld the *seizure* of irrelevant documents intermingled with documents within the scope of a warrant. However, these cases have been careful not to endorse wholesale *searches* of documents beyond the scope of the warrant, aside from brief examinations of the documents to determine whether they fall within the scope of the warrant. *See* United States v. Christine, 687 F.2d 749, 760 (3d Cir. 1982) (noting that "in searches for papers, it is certain that some innocuous documents will be at least cursorily perused in order to determine whether they are among those papers to be seized"); United States v. Wuagneux, 683 F.2d 1343, 1352 (11th Cir. 1982), *cert. denied*, 464 U.S. 814 (1983) (holding that agents may lawfully review documents on site to determine whether they fall within the warrant, and when necessary seize entire files so that agents can identify where individual documents belong if returned); United States v. Heldt, 668 F.2d 1238, 1267 (D.C. Cir. 1981) (Documents may be reviewed briefly to determine whether probable cause exists for their seizure. If their incriminating character is obvious, the documents may be seized; otherwise, the review must cease when the warrant's inapplicability to a particular document becomes clear); United States v. Slocum, 708 F.2d 587, 605-06 (11th Cir. 1983) (approving the seizure of an entire file after on-site review determined that it contained documents within the scope of the warrant, since seizing the whole file helped limit the time

Once computer data is removed from the suspect's control, there is no exigent circumstance or practical reason to permit officers to rummage through all of the stored data regardless of its relevance or its relation to the information specified in the warrant. After law enforcement personnel obtain exclusive control over computer data, requiring them to specify exactly what type of files will be inspected does not present any undue burden. A neutral magistrate should determine the conditions and limitations for inspecting large quantities of computer data. A second warrant should be obtained when massive quantities of information are seized, in order to prevent a general rummaging and ensure that the search will extend to only relevant documents.

The *Tamura* rule is well suited to the practical considerations involved in searching through computer memory. Once officers seize large quantities of computer memory, they have three methods of distinguishing relevant from irrelevant information. Officers can either read through portions of each file stored in the memory, conduct a key word search of the data stored on the disks, or print out a directory of the title and file type for each file on the disk.[174]

The effectiveness of key word searches to investigators and their importance in protecting privacy were recognized by both the Fifth Circuit and by the United States Secret Service in *Steve Jackson Games*. In that case, the court noted that key word searches could limit intrusions into personal privacy since: "[A]s the Secret Service advised the district court, technology exists by which relevant communications can be located without the necessity of reviewing the entire contents of all of the stored communications. For example, the Secret Service claimed . . . that it reviewed the private E-mail on the BBS by use of key word searches."[175]

Law enforcement officers, particularly federal officers, are sufficiently familiar with computer searches, and the likelihood that large quantities of personal information will be intermingled with relevant information, to be required to apply beforehand for permission to perform a large scale-removal of computer storage media.[176] A magistrate's review of the

---

necessary to conduct the search); United States v. Goff, 677 F. Supp. 1526, 1544 (D. Utah 1987) (holding that officers may conduct a brief review of computer disks at site of search to determine their relevancy).

174. *See In re* Subpoena Duces Tecum, 846 F. Supp. 11, 13 (S.D.N.Y. 1994) (noting that "it is easier in computer age to separate relevant from irrelevant documents").

175. Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 463 (5th Cir. 1994).

176. *See, e.g.*, Klitzman, Klitzman, and Gallagher v. Krut, 744 F.2d 955, 961 (3d Cir.

methods used to separate relevant from irrelevant information is necessary to ensure that the officers only read through files that there is reason to believe contain relevant information.

Once law enforcement officials seize a computer storage device, these officers should be required to specify which types of files are sought. Whenever possible, key word searches should be used to distinguish files that fall within the scope of a warrant from files that fall outside the scope of the warrant. In addition, the type of information stored in a particular file is often easily ascertainable. Computer programs store information in a wide variety of formats. For example, most financial spreadsheets store information in a completely different format than do word processing programs. Similarly, an investigator reasonably familiar with computers should be able to distinguish database programs, electronic mail files, telephone lists and stored visual or audio files from each other. Where a search warrant seeks only financial records, law enforcement officers should not be allowed to search through telephone lists or word processing files absent a showing of some reason to believe that these files contain the financial records sought. Where relying on the type of computer files fails to narrow the scope of the search sufficiently, the magistrate should review the search methods proposed by the investigating officers. Opposing counsel should be given the opportunity to propose less intrusive methods of screening the information. Alternatively, opposing counsel should be given an initial opportunity to identify those files that it believes fall outside the scope of the search. If the investigating officers are unable to provide any reason to believe that those files fall within the scope of the search, or are unable to propose any method for determining the relevance of these files, a search of these files should not be permitted. The basic principle is that before a wide-ranging exploratory search is conducted, the magistrate should require the investigators to provide an outline of the methods that they will use to sort through the information.

Of course, the facts of some cases, such as complex conspiracies, may justify the full-text search of all or mostly all of the records. However, the government should bear a heavy burden in demonstrating that no less intrusive method is available to separate files falling within the scope of the warrant from files falling outside the scope of the warrant. A vague

---

1984) (noting that federal officers should have been aware of, and followed, U.S. Attorney Guidelines of C.F.R. § 59.1-6 (1994), which the government must meet before using a search warrant to obtain documentary materials held by disinterested third parties).