IN DEFENSE OF THE SUGAR BOWL

By James M. Rosenbaum[1]

The fourth amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]" The Amendment assures this protection by requiring that "no warrants shall issue, but upon probable cause … particularly describing the place to be searched, and the persons or things to be seized."

A constitutional warrant specifies the premises to be searched, the crime being investigated, and the evidence sought. If the investigator seizes evidence not reasonably related to the crime under investigation, the search goes beyond the warrant's scope. This relationship between the crime under investigation, and the search's extent leads to the maxim that "if you are looking for stolen televisions, you cannot look in sugar bowls."

Even if a yegg keeps cocaine in the sugar bowl, it is extremely unlikely stolen televisions will be found with it. There is a corollary, however: although investigators can only search for particular evidence of a described crime, they need not disregard obvious signs of other illegal activity in "plain view." Accordingly, a television-seeking officer is not barred from seizing a mirror, a razor blade, and a white crystalline substance divided into lines from the night stand.

A new device has complicated these precepts. The device is the computer. Warrants routinely issue for computers and the evidence they may contain. But computers compound the sugar bowl/television problem. The law is only beginning to consider the concepts of particularity and plain view in the electronic context. Stored memory in a computer is physically small – usually no larger than a compact disc, and frequently far smaller. The law needs to assure that diminished size does not weaken the fourth amendment's protections.

It is time for the Courts to define the electronic equivalent of unsearchable sugar bowls. It can do so by treating separate hard drive files as separate closed containers. The Courts should also borrow ideas developed in the context of civil discovery to address legitimate privacy concerns. And, finally, the law should require that forensic search methodology be subject to – and preserved for – judicial review.

A search warrant authorizing a search of a computer located at XYZ Main Street may appear specific in scope and locale. The appearance is deceiving. This is because computers have become a modern combination of file cabinet and Fibber McGee's closet. Computers contain a

[1] *James Rosenbaum is Chief Judge of the United States District Court for the District of Minnesota. All citations, and many valuable comments, are the product of relentless efforts by his law clerk, Karin Ciano. This article originally appeared in* THE GREEN BAG *(Volume 9, Autumn 2005) and is reprinted with its permission.*

slurry of filed material, internet visits, personal correspondence, and – perhaps – evidence of crime. Without controls, such a simple warrant fails to particularly describe the nature and scope of the investigation. This is the nub of the sugar bowl/television problem.

While an unrestricted hard drive examination may reveal evidence of the crime being investigated, it can also wander into evidence of other crimes.[2] Allowing an investigator access to such material has, perhaps, a superficial appeal. Why complicate the discovery of another crime? The answer lies in the Framers' wisdom and in the constitution they created.

Before the Revolutionary War, the British could – and did – search any Colonial's home and belongings. They simply ransacked any site they chose, looking for evidence. The Framers resolved to permanently end these "general warrants." They knew that in their new Republic crimes would need to be investigated. But they also knew that if authorities could simply rummage through citizens' homes, the path to tyranny would open again.

The law has long recognized – outside the computer context – a need for special control of electronic investigations. When executing wire taps, agents must "minimize" their surveillance, to avoid eavesdropping on idle chatter.[3] Minimization protects against over-breadth and over-intrusion. Similar reasoning applies to the computer searches.

The fourth amendment "provides protection to the owner of every container that conceals its contents from plain view," even though the degree of protection varies with the setting.[4] A computer raises the question of whether its memory comprises one container, or many. If it is a single container – a digital duffel bag – a simple warrant could render each hard drive file in "plain view."[5] If the law considers each file a separate closed container, the warrant must more particularly describe the matter sought.[6]

The separate file/separate container view recognizes the reality of computer use. Where historically a computer may once have executed a single task, today's computers are crammed with information relating to many subjects, one of which may be criminal activity. The particularity requirement forbids a rummage through this information into entirely unrelated areas. The Tenth Circuit has adopted the view that courts must "look to (1) the object of the

[2] See, e.g., United States v. Carey, 172 F.3d 1268, 1271 (10th Cir. 1999) (officer found child pornography while searching for evidence of drug dealing; United States v. Turner, 169 F.3d 84, 86 (1st Cir. 1999) (same, during search of evidence related to an assault).

[3] 18 U.S.C. § 2518(5) (2000).

[4] United States v. Ross, 456 U.S. 798, 822-23 (1982).

[5] See United States v. Runyan, 275 F.3d 449, 464 (5th Cir. 2001) (treating individual CD's and zip disks as closed containers, but finding the data files on each disk to be "items" within a closed container).

[6] See *Carey*, 172, F.3d at 1273 (closed files are not in plain view); see also United States v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998) (after delivering computer to repair service, defendant retained reasonable expectation of privacy in "closed, individual files").

search, (2) the types of files that may reasonably contain those objects, and (3) whether officers actually expand the scope of the search upon locating evidence of a different crime."[7]

In *Brooks*, officers avoided looking for televisions in the sugar bowl, and the search was upheld. After obtaining a warrant, they sought, and obtained, defendant's consent to search his computer for pornographic images. Because images were not likely to be found in text files, the warrant and defendant's consent contemplated that no text files would be opened or viewed. Both sides anticipated a search using a program which could find and display small "thumbnail" views of all image files. When the program did not perform, the official conducted a manual search with the same parameters, viewing only image files. The Tenth Circuit upheld the search.

There are certainly crimes where evidence might be found in multiple types of files. It is also possible to mislabel or conceal electronic information. These facts do not justify illegal searches.

In these cases, the Courts can benefit by looking at civil discovery where electronic discovery is a commonplace, and which has regularly confronted access to computerized information. In civil cases, a demand for access to the other side's computer frequently triggers negotiations over search terms and the scope of discovery. "Sampling," which allows limited review of potentially valuable data, is also used to cull digital wheat from unresponsive chaff. The parties and the Courts balance the need to examine computerized data, with the concomitant need to keep discovery within the case's proper scope.

These recognized restraints on civil discovery do not yet have their parallel in the criminal context. But civil discovery offers a useful analogue, subject to the obvious fact that in civil litigation each party knows discovery is taking place. Search warrants, to the contrary, are ex parte. In criminal cases, the party under investigation only infrequently knows the examination is underway. As a result, it falls to the Courts to impose effective restraints on the scope of an electronic search.

To do so a Court should require controls on the search terms to be examined. Investigators should also operate under protocols aimed at the particular case under investigation. To assure compliance with the Court's direction, it is appropriate for computer investigators to use keystroke-capturing devices or similar means to record the investigator's digital peregrinations and allow for judicial review. These methods will allow the Courts to properly limit computer searches, as they are limited in the physical world.

Constitutional compliance may cause a lapse of time between seizure and review of the computer. This should not create a problem; if immediate access is needed – when exigent circumstances are present – the investigator can demonstrate the need and be granted immediate access. Absent exigent circumstances, it is no burden to secure the computer, and negotiate the search's scope. Courts regularly balance the public's interest in criminal investigation with the fourth amendment's privacy protections.

[7] United States v. Brooks, 427 F.3d 1246, 1251 (10th Cir. 2005).

This suggestion complicates criminal investigations. So does the fourth amendment. The proposal also recognizes another of the computer's unique characteristics: its blessed/cursed inability to lose any information once it has been stored. While drugs can be flushed away as police knock and announce their warrant, computer data is nearly the contra-inverse – it is almost impossible to expunge its memory, no matter how hard its owner may try.[8]

For years, courts have treated computer data as fragile and ephemeral.[9] In fact it is anything but. Once a computer is seized, there will rarely be an exigent need to search it. This allows time for the government to develop, and a court to review, the scope and methodology of the search.[10]

The proposal does not force investigators to disregard other crime evidence in plain view. An investigator who opens a file looking for a record of drug sales, but finds instead pornography, is free to develop probable cause to seek another warrant. But plain view should not be equated with the mere fact that the material exists on the same hard drive. A bank robber's computer may catalogue get-away paths, but this does not justify a disc-wide general search. The fourth amendment requires specificity.

The Framers drafted the fourth amendment to protect a new country from the tyranny experienced at the hand of the old. It represents now, as it did then, a declaration that official power must be held in check, even while protecting the citizens. The amendment's protections remain as valuable in the 21st century as in the 18th. The constitution still protects our "papers and effects," even if stored in different devices.

[8] See S. Garfinkel and A. Shalat, *Remembrance of Data Passed: A Study of Disk Sanitation Practices*, 1 IEEE Security & Privacy 17 (January/February 2003).

[9] See, e.g., United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000).

[10] See *In re* Search of 3817 W. West End, 321 F.Supp. 2d 953, 956 (N.D. Ill 2004).