The Legal Intelligencer

THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2011

PHILADELPHIA, WEDNESDAY, DECEMBER 21, 2011 VOL 244 • NO. 120 An ALM Publication

WHITE-COLLAR LAW

Courts Show Continued Deference to Broad Electronic Searches

BY PETER D. HARDY AND ABRAHAM REIN
Special to the Legal

Computers and related digital devices like smartphones store increasingly massive amounts of business and personal data. As a result, when law enforcement obtains a digital device during an investigation of suspected financial crime, child pornography, or other offense, a massive cache of unrelated data is inevitably caught in the net.

Although the Fourth Amendment demands that search warrants be particular as to the material sought and seized, prosecutors invariably argue — and courts often agree — that the requested search and its execution necessarily must be extremely broad. Many courts acknowledge Fourth Amendment concerns but nonetheless proceed to embrace, implicitly or explicitly, the following notion: Because investigators do not know in advance where any contraband is located, practical considerations allow them to examine every electronic folder and document seized, however briefly, to rule out the possibility that it contains evidence sought by the warrant.

A recent opinion by the 6th U.S. Circuit Court of Appeals, *United States v. Richards*, has continued this trend toward sanctioning broad searches and did so by citing heavily to an opinion issued earlier in 2011 by the 3rd Circuit, *United States v. Stabile*. These and similar opinions raise this question: once the government has obtained a search warrant regarding the contents of a hard drive or phone, whether there are any practical limits to what data may be accessed, viewed and ultimately used to convict.

Although these cases often arise in the context of child pornography investigations — when courts are presumably particularly reluctant to grant suppression — the general legal principles that they establish of course govern every kind of case, no matter how complex or esoteric the alleged wrongdoing.

A SHORT-LIVED FORAY INTO LIMITS ON SEARCHES

The *Richards* and *Stabile* opinions were not decided on a blank slate. In 2009, the en banc 9th Circuit breathed new life into this debate when it issued the initial opinion — later amended in a significant way — in *United States v. Comprehensive Drug Testing Inc.*, which imposed several procedural requirements on the government as to computer searches. The court upheld three orders granting Rule 41(g) motions for return of property filed as to searches of laboratories in a grand jury investigation of steroid use in major league baseball. In so doing, the 9th Circuit articulated some very broad concerns regarding searches of electronic records, which other courts have echoed:

"This pressing need of law enforcement for broad authorization to examine electronic records ... creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant. The problem can be stated very simply: There is no way to be sure exactly what an electronic file contains without somehow examining its contents — either by opening it and looking, using specialized forensic software, keyword searching or some other such technique. But electronic files are generally found on media that also contain thousands or millions of other files among which the sought-after data may be stored or concealed. By necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there. ... "

"We accept the reality that such over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures."

The *Comprehensive Drug Testing* court then addressed these concerns by setting forth several procedural requirements for computer-related searches. These included the categorical requirement of an independent "taint team" to examine and sort the seized data, and that magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.

However, after issuing the initial opinion, the 9th Circuit issued a new en banc opinion later in 2010. Now, the majority reached the same substantive results as the original opinion, but conspicuously omitted the discussion of the procedural requirements, which instead were set forth in a concurring opinion by Chief Judge Alex Kozinski. This procedural history highlights the ease with which courts can identify the risks posed by computer searches to the protections of the Fourth Amendment and the difficulty or reluctance that they have in fashioning a real-world solution to mitigate those risks.

RICHARDS AND *STABILE*

The 6th Circuit recently articulated the same concerns outlined in *Comprehensive Drug Testing* regarding overly broad searches — while simultaneously upholding a very broad search. On Oct. 24, the 6th Circuit decided *United States v. Richards*, in which the government obtained a search warrant allowing it to image the contents of an entire server maintained by a third-party company (a facility that maintained more than 2,000 servers). That server hosted two websites suspected of offering child pornography, along with five other websites controlled by the defendant. The individual defendant responsible for the content of the websites appealed the denial

PETER D. HARDY *(phardy@postschell.com)* and **ABRAHAM REIN** *(arein@postschell.com)* *are attorneys in the Philadelphia office of the law firm of Post & Schell, and are part of the firm's white-collar defense, internal investigations and corporate compliance practice, as well as its data protection group. Hardy previously served as an assistant U.S. attorney and is the author of "Criminal Tax, Money Laundering, and Bank Secrecy Act Litigation," a legal treatise published by BNA Books. Rein's experience with managing electronic information includes having co-founded and served as the managing partner of a Web-development and consulting firm.*

of his motion to suppress evidence obtained from the server on the basis that the warrant was overbroad under the Fourth Amendment, and because the search exceeded the scope of probable cause set forth in the warrant.

To describe the competing interests at stake, the 6th Circuit quoted language from an opinion issued by the 3rd Circuit earlier in 2011, *United States v. Stabile*, which had upheld the denial of a motion to suppress electronic evidence obtained in a bank fraud and child pornography case:

"On the one hand, it is clear that because criminals can — and often do — hide, mislabel, or manipulate files to conceal criminal activity, a broad, expansive search of the hard drive may be required. ... On the other hand, ... granting the government a carte blanche to search every file on the hard drive impermissibly transforms a limited search into a general one."

Continuing to cite *Stabile* throughout its opinion, the 6th Circuit stated that, in light of the practicalities of searching computers, federal courts have eschewed the use of a specific search protocol. Instead, they have applied a case-by-case reasonableness test and generally have rejected particularity challenges to warrants authorizing the search and seizure of entire computers.

Thus, and despite the acknowledged concern of electronic searches naturally devolving into impermissible general searches, the *Richards* court found that it is reasonable for executing officers to open the files within a hard drive and examine them in order to determine whether they contain evidence identified by the warrant, so long as the search is limited to evidence explicitly authorized by the warrant. Because the warrant at issue authorized the search and seizure of the entire server, the warrant was limited to a search for evidence of child pornography, and the government did not know when it obtained the warrant how the server was organized or held its information, neither the warrant nor its execution — a search of the entire contents of the server — was unconstitutionally overbroad.

In *United States v. Stabile*, the opinion cited by the *Richards* court, the 3rd Circuit upheld the denial of a motion to suppress electronic evidence obtained in a bank fraud and child pornography case with a complex procedural history. After seizing six hard drives during a bank fraud investigation through a warrantless search of the defendant's home obtained through the consent of another person, officers obtained a state court search warrant to search the hard drives.

Although the search of the home had found DVDs with labels that had led agents to believe (mistakenly) that they contained child pornography, and although the state search warrant authorized a search for evidence of both financial crimes and child pornography, the officer tasked with reviewing the data on the hard drives was instructed to search only for evidence of financial crimes. When the officer found child pornography in a file labeled "Kazvid," the defendant argued that the officer's decision to open that file represented an unreasonably broad search not limited to evidence of financial crimes.

Courts almost inevitably uphold very broad searches, using the logic that it is impossible to tell whether any document has been intentionally mislabeled until it is reviewed.

The 3rd Circuit observed that the competing principles of allowing a broad search to overcome any intentional mislabeling of files, versus avoiding an impermissible general search in every search of a computer, had led courts to suggest various strategies to limit the scope of a search. It cited *Comprehensive Drug Testing* for the principles that "law enforcement personnel trained in search and seizing computer data" should perform the initial review and segregation of data, as opposed to the case agents, and that the government should return any data not falling within the scope of the warrant.

The *Stabile* case also cited in part *United States v. Burgess*, issued by the 10th Circuit in 2009, for the propositions that a warrant need not set forth a particularized computer search strategy, but that it becomes more important for the government to tailor any search method that it uses as the warrant's description of places and things to be searched becomes more general. The *Burgess* court further recommended that computer searches begin by using search protocol to analyze file structure, followed by a search for suspicious file folders, followed by a review of files most likely to contain the objects of a search by doing keyword searches.

However, the 3rd Circuit observed that the *Burgess* court also stated that, ultimately, there may be no practical substitute for actually looking in many or all seized folders and documents. Turning to the case at hand, the *Stabile* court found that it was reasonable for the searching officer to open the "Kazvid" folder because, after determining whether any files had been corrupted or copied, he examined suspicious and out-of-place folders, including the "Kazvid" folder. The 3rd Circuit also found that the defendant had offered "no practical alternative methodology that would have protected his interests yet still permitted a thorough search for evidence of financial crimes"; further, the fact that the officer subjectively suspected that the "Kazvid" folder contained child pornography was irrelevant to whether a search fell within the scope of a warrant.

DWINDLING OPTIONS FOR DEFENDANTS

The line of cases discussed above appears to leave persons contesting the breadth of electronic searches with few real-world options. Despite repeated acknowledgements of the special risks of overbreadth posed by searches of electronic information, many courts almost inevitably uphold very broad searches, using the logic that it is impossible to tell whether any document has been intentionally mislabeled until it is reviewed. Of course, search warrant affidavits will dutifully include language that, in the affiant's experience, targets of investigations can and will mislabel files.

Even if the Fourth Amendment does not require that the warrant itself set forth a computer search protocol or strategy, the government invariably will employ such a search strategy — and that strategy still must reflect a reasonable execution of the warrant. As the 3rd Circuit suggested in *Stabile*, good procedures can include using only personnel trained in computer searches to perform the initial review and segregation of data, and returning any data that does not fall within the scope of the warrant.

However, these principles, although sound, do not appear to address or preclude the practical result that each opinion professes to deplore: a near-guarantee that the government will be empowered to examine every electronic document seized in just about every case, because it is impossible to rule out the potential, no matter how theoretical, that the document was intentionally mislabeled. It may be that the few scenarios left for a successful overbreadth claim include when the warrant simply fails to describe the offenses that are the basis of the search, when the warrant does not tie the electronic data to the offenses under investigation or when the government violates its own self-described search strategy. Although courts might be embracing this result as a marriage of necessity between the Fourth Amendment and modern technology, the recitations of concerns against electronic searches inevitably devolving into general searches appear to be eloquent but rarely material to case outcomes. •