Bloomberg BNA

Electronic Commerce & Law Report™

ELECTRONIC EVIDENCE

Courts have applied the plain view doctrine and the need for ex ante search warrants for computer and e-mail searches inconsistently, leading to uncertainty for law enforcement, prosecutors and defense attorneys alike. The authors propose using wiretap protocols as a model for consistent procedures and judicial oversight.

Public Safety, Privacy, and Particularity: A New Approach to Search Warrants for Digital Evidence

By Jason Weinstein and William Drake

Federal agents enter a company's offices armed with a search warrant for documents and other evidence of a financial fraud scheme. In executing their search, the agents look anywhere the documents might reasonably be found – in every file folder, in every drawer, in every desk and file cabinet. And since participants in criminal activity tend not to label their files ''Evidence of Crime,'' the agents look in every file, regardless of how it is labeled. Along the way, in ''plain view,'' the agents find evidence of some other crime they were not even investigating – say, for example, money laundering or child pornography – and use that evidence to build a case regarding that other crime.[1]

Across the country, a different team of agents goes to a storage facility to execute a search warrant for a storage unit rented by a suspected drug dealer. The agents enter the storage unit – doing the search themselves, rather than asking the manager of the facility to do it for them – and look through every item that might reasonably contain the evidence of drug trafficking covered by the warrant. Again, they find evidence of some other, unrelated crime while executing their search, and use that evidence to develop charges for that other crime.

Jason Weinstein is a partner in the Washington office of Steptoe & Johnson LLP. He is a former federal prosecutor and most recently served as deputy assistant attorney general in the U.S. Department of Justice's Criminal Division, where he oversaw the Computer Crime and Intellectual Property Section.

Will Drake is an associate in Steptoe's white-collar crime group, who focuses his practice on fraud and public corruption. He is a 2009 graduate of the Georgetown University Law Center.

[1] The authors gratefully acknowledge the assistance of future Steptoe associate Nick Silverman, Georgetown University Law Center Class of 2014.

Everything we just described is accepted as legitimate and reasonable conduct in executing a search warrant. The same is true if the search warrant is for a subject's home – perhaps the most sacred of constitutionally protected private spaces.

But what if the search is for a subject's computer – whether in a home or office? Or for the subject's e-mails, stored by a webmail provider? Do the rules change when agents are perusing digital files stored on a hard drive, as opposed to papers in a physical file cabinet? Or when agents are searching e-mails stored on a server owned by a third party, as opposed to possessions stored in a physical locker owned by a third party? More generally, should the same rules that govern searches in the ''physical'' world also apply in the digital world?

Today, the answers to these questions depend on which judge you ask or which courthouse you are standing in. And the answers have significant consequences for both public safety and privacy.

Even before anyone had heard of Edward Snowden, the country was in the midst of a growing debate over how to balance public safety and privacy in the digital age. Since Snowden became a household name, that debate has tended to focus on the NSA and the gathering of foreign intelligence. But much closer to home, on an almost daily basis, judges in criminal cases are struggling with the real-world implications of this debate in the context of search warrants for computers, digital devices, and e-mail accounts.

Since 2009, when the Ninth Circuit issued its first en banc opinion in *United States v. Comprehensive Drug Testing, Inc. (CDT)* (14 ECLR 1247, 9/2/09), there has been a growing disagreement among courts in different circuits over what, if any, special rules should govern searches of computers and other digital devices. For some courts, searches of digital devices present unique privacy challenges because of the sheer volume of personal information contained, for example, on a smartphone or laptop. These judges have imposed protocols and rules to constrain law enforcement agents in executing such searches. Other judges view digital searches as essentially the same as physical searches, and believe the privacy issues involved are just part and parcel of criminal investigations in the digital age.

Over the past year or so, the unresolved debate has expanded to include search warrants for e-mail accounts, with a similar split emerging among courts over whether special rules are needed to limit the scope of such searches. Indeed, over the past year, several federal magistrate judges have refused to approve searches of e-mail accounts in the absence of protocols requiring that an independent third party or separate group of agents – or even the e-mail provider itself – screen out non-responsive material before turning over evidence to investigators.

Commentators disagree as well. Some embrace the use of search protocols, arguing that they are essential to avoid turning a warrant to search for evidence of a particular crime into an unfettered license to search for evidence of any crime. Others contend that these protocols place undue and unwarranted burdens on the ability of law enforcement officers to do their jobs, arguing instead that the courts should define what is ''reasonable'' in the context of digital searches through decisions on motions to suppress.

Circuit Split Over Search Protocols

Ninth Circuit	Elsewhere
The Ninth Circuit originally required search protocols for magistrates including government waiver of plain view doctrine. A subsequent opinion changed magistrates' use of search protocols to advisory.	Courts in the First, Third, Fourth, Sixth, Seventh, Eighth, Tenth, and Eleventh Circuits have rejected ex ante search protocols or requirements forswearing use of plain view doctrine.

With e-mail and digital evidence playing an increasing role in investigations of just about every crime on the books – from white collar, to cyber, to violent crime, and everything in between – the question of what constitutes a reasonable digital search is of critical, and growing, importance.

In the interests of full disclosure, one of the authors of this article was a longtime federal prosecutor who oversaw the Computer Crime and Intellectual Property Section (CCIPS) at DOJ's Criminal Division, which led DOJ's efforts to guide prosecutors in the wake of *CDT*. He now deals with these issues from ''the other side of the v.'' as a defense attorney. Based on those dual perspectives, this article suggests that the best way to balance law enforcement's ability to function effectively with the privacy interests of subjects of investigations lies somewhere between the extremes described above: neither a one-size-fits-all protocol established before a warrant issues, nor an after-the-fact examination of the reasonableness of a search, but rather a greater oversight role for judges *during* the execution of digital search warrants.

CDT and the Circuit Split on Computer Search Warrants

The BALCO investigation is generally credited with contributing to the reduction in the use of performance-enhancing drugs in baseball. But whatever its impact on baseball, its impact off the diamond has been even greater, because the BALCO investigation produced the Ninth Circuit's series of opinions in *CDT*, which were a seminal moment in the evolution of the law governing searches of digital media.

In *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1000 (9th Cir. 2009) (en banc) (*CDT II*), the majority – in dicta – instructed magistrate judges in the Ninth Circuit to impose search protocols as a condition for approving future applications for search warrants for computers. The Court required that these protocols include:

- a government waiver of the use of the ''plain view'' doctrine;
- the use of an independent third party or specialized personnel to segregate and redact all non-responsive information;
- a disclosure in applications and subpoenas detailing the actual risks of destruction of information specific to the case at hand, rather than mere allusion to general risks that devices will be booby-trapped to automatically delete information upon unauthorized entry

   ISSN 1098-5190

(also noting any prior efforts to seize the information in other judicial fora);

- a search procedure to uncover only responsive information; and

- a requirement that the government destroy or return all non-responsive data and file a return as soon as practicable detailing what has been kept.

The Ninth Circuit later downshifted its proposed search protocols from mandatory to advisory for magistrate judges in the Circuit, as *CDT II* was replaced by a per curiam opinion, with the proposed search protocols relegated to a concurrence. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1178 (9th Cir. 2010) (en banc) (per curiam) (hereinafter *CDT III*) (15 ECLR 1434, 9/22/10).

While some magistrates within the Ninth Circuit have embraced the *CDT* protocols, others have not, opting to exercise their own discretion. The result has been inconsistency and confusion within the Ninth Circuit among law enforcement, government attorneys, and defense counsel over what rules govern digital searches. And that inconsistency and confusion extends to other parts of the country as well.

The vast majority of other circuits – including the First, Third, Fourth, Sixth, Seventh, Eighth, Tenth, and Eleventh – have rejected the use of either ex ante search protocols or government agreements to forswear reliance on plain view as a condition of approving search warrants for computers. See, e.g., *United States v. Richards*, 659 F.3d 527, 538, 542 (6th Cir. 2011); *United States v. Stabile*, 633 F.3d 219, 237–38, 240–41 (3d Cir. 2011) (16 ECLR 268, 2/23/11); *United States v. Mann*, 592 F.3d 779, 785 (7th Cir. 2010) (15 ECLR 240, 2/17/10); *United States v. Williams*, 592 F.3d 511, 522 (4th Cir. 2010); *United States v. Burgess*, 576 F.3d 1078, 1094 (10th Cir. 2009); *United States v. Cartier*, 543 F.3d 442, 447–48 (8th Cir. 2008); *United States v. Khanani*, 502 F.3d 1281, 1290-91 (11th Cir. 2007); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (4 ECLR 183, 2/24/99).

Several of those courts have expressly acknowledged that officers executing search warrants for computers are permitted to open and review every computer file where evidence of the crime under investigation might reasonably be found, recognizing that file names and extensions can be manipulated, enabling a criminal to conceal illegal materials by labeling them something mundane and misleading. See, e.g., *Williams*, 592 F.3d at 522; *Upham*, 168 F.3d at 535. Other courts have encouraged officers to use caution and develop methods to tailor their searches as narrowly as possible, observing that decisions on motions to suppress will allow the contours of the plain view doctrine and the definition of ''reasonableness'' to take shape on a case-by-case basis. See, e.g., *Richards*, 659 F.3d at 538, 542; *Mann*, 592 F.3d at 785-86. At least one court has held that searches of computers must be targeted at evidence of the crime covered by the warrant and has suggested that to the extent that officers' *subjective* intent is to seek information outside the scope of the warrant, plain view would be unavailable. *United States v. Galpin*, 720 F.3d 436, 451-52 (2d Cir. 2013) (18 ECLR 2174, 7/17/13).

Emerging Split on E-mail Searches

The different approaches to computer search warrants reflect the challenge faced by courts in ''reconcil[ing] [the] competing aims'' of finding inculpatory hidden files while avoiding a general search. *Stabile*, 633 F.3d at 237-38.

More recently, this conflict has played out in the context of search warrants for e-mail accounts. Typically, when law enforcement agents serve a search warrant on an e-mail provider for evidence of a crime under investigation, the provider does not screen the e-mails for relevance. On the contrary, the provider sends a copy of all of the e-mails in the account to the agents, who then review them for responsiveness to the warrant.

In August 2013, a federal district judge in Kansas became one of the first, if not the first, federal judge to reject a search warrant application for an e-mail account based on the possible scope of the search (18 ECLR 2495, 9/11/13). In that case, the court rejected five applications for warrants that would have required Google, GoDaddy, Verizon, Yahoo, and Skype to disclose, among other things, the contents of all e-mails, IMs, and chat logs associated with the target accounts as part of an investigation into the theft of computer equipment.

The court concluded that the proposed warrants suffered from two primary defects: first, they required the providers to turn over all content, as opposed to restricting the providers to disclosing only content related to the crimes under investigation; and second, they failed to include any sorting or filtering procedures that would require the government to separate relevant evidence from either irrelevant or privileged material. The court found that the warrants gave the government ''virtual carte blanche'' to review the entire e-mail account of the target, observing that ''the breadth of the information sought by the government's search warrant . . . is best analogized to a warrant asking the post office to provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the mail to find out whether it [contains evidence].'' *In the Matter of Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts*, 2013 WL 4647554, at *8, 9 (D. Kan. Aug. 27, 2013). Accordingly, the court found that the warrants failed to describe the scope of the material to be collected with sufficient particularity.

The Kansas court declared that warrants for Internet communications must contain sufficient limits or boundaries so that law enforcement can determine which e-mail communications and information are within the scope of the warrant. The court stopped short of imposing a particular search protocol – instead leaving the choice of a procedural safeguard up to the government – but suggested that one of the following methods would be acceptable: asking the provider to disclose only content that contained certain key words or that was sent to or from certain parties, appointing a special master with authority to hire an independent vendor to use computerized search techniques, or setting up a ''filter group'' or ''taint team'' within the investigating agency.

More recently, a magistrate judge in the District of Columbia went further, rejecting a series of applications for search warrants for e-mails or digital devices, all on essentially the same grounds: the failure to adopt search protocols to prevent the government from seizing or searching e-mails or other data outside the scope of the warrants, and the failure to provide any timetable for when, if ever, the government intended to return the

devices. In an earlier case the judge had warned the government that failure to adopt strict protocols – such as keyword searches, use of an independent special master to conduct initial searches/screening, or use of a separate taint team of agents to do that initial screening – would result in the rejection of future warrant applications. The judge followed through with his threat, rejecting a total of 11 search warrant applications in a two-month period. See, e.g., *In the Matter of the Search of Black iPhone 4*, 2014 WL 1045812 (D.D.C. Mar. 11, 2014); *In the Matter of the Search of ODYS LOOX Plus Tablet*, 2014 WL 1063996 (D.D.C. Mar. 20, 2014).

Federal district judges in Maine and Tennessee, and a different district judge in Kansas, are among the courts that disagree. Each approved the issuance of, or denied motions to suppress evidence from, warrants that required providers to turn over all e-mails sent to or from target accounts, even in the absence of search protocols or other indications from the government about how the searches would be conducted or what would be done with non-responsive e-mails after the search. *United States v. Ayache*, 2014 WL 923340 (M.D. Tenn. Mar. 10, 2014); *United States v. Deppish*, 2014 WL 349735 (D. Kan. Jan. 31, 2014); *United States v. Taylor*, 764 F. Supp.2d 230 (D. Me. 2011). As the court in Tennessee noted, searches of electronic communications create '' 'practical difficulties' that require a flexible approach to the application of the particularity requirement.'' *Ayache*, 2014 WL 923340, at *2.

The Problem with Protocols

When it comes to the Fourth Amendment, confusion and lack of clarity are not good – not for citizens, not for law enforcement officers, and – in the case of e-mail – not for providers. But as much as they appeal to our desire for certainty, search protocols of the type proposed by the Ninth Circuit in *CDT* are both unworkable and unwise.

The Internet and modern communication technologies are used to facilitate virtually every type of crime imaginable. Because criminals of all types use cell phones, mobile devices, and Internet-based means of communication more than ever, electronic evidence is ubiquitous in criminal investigations, whether involving terrorism, espionage, white collar crime, violent crime, drug trafficking, organized crime, kidnapping, cybercrime, or crimes against children. It is the rare investigation these days that does not involve a search warrant for a digital device or an e-mail account.

For that reason, it is not practical to require law enforcement officers to utilize a ''taint team'' for every warrant in every case. It is even less workable to engage a special master, or other independent entity, to prescreen evidence. Investigations would come to a standstill, and law enforcement would not be able to do its job efficiently or effectively.

But at the same time, it is unfair – to both the public and the providers – for e-mail providers to be required to perform this pre-screening function. To do so would impose a time-consuming and expensive burden on these providers that they should not have to bear. Moreover, no one's privacy interests are served by having private citizens, who are not sworn law enforcement officers, engage in investigative functions. As one district judge recently wrote, ''[N]othing in the Fourth Amendment requires law enforcement to cede to non-law enforcement their power to search and determine which matters are subject to seizure.'' *Deppish*, 2014 WL 349735, at *6.

Moreover, with due respect to those judges who have suggested it, requiring law enforcement officers to forswear reliance on plain view is absurd, and is detrimental to public safety. If a law enforcement officer conducting a search pursuant to a validly issued warrant comes across evidence of a crime against a child, or some other serious offense, how is public safety served if the officer is precluded from using that evidence? And provided that the officer comes across that evidence only because he or she has a warrant to conduct the search in the first place, there can be no concern of law enforcement overreaching that would require the suppression of lawfully obtained evidence.

On the other hand, waiting until cases reach the motion to suppress stage and allowing case-by-case determinations to guide an understanding of what is ''reasonable'' neither satisfies the need for clarity nor protects citizens' privacy interests. If officers act in accordance with a warrant, only to have evidence suppressed because a court later decides that the manner of execution was unreasonable, the result is a waste of resources – for agents, prosecutors, defense lawyers, and the courts. And by the time a motion to suppress is heard, any privacy violation suffered by the subject of the investigation has already occurred.

With search warrants for electronic evidence becoming more and more common, it has never been more important for magistrate and district judges to have a good grasp of the realities of a forensic examination. As a practical matter – and contrary to what you might see on ''CSI'' or ''24'' – minimization or filtering takes place of necessity in every forensic exam. Because the volume of electronically stored information on the average hard drive has increased so dramatically – not to mention the increase in the type and number of other digital devices in use today – and because forensic examinations are a critical part of so many criminal cases, it is impractical, if not impossible, for forensic investigators to examine every document in every file in every part of a hard drive. Instead, forensic investigators employ techniques to filter seized data to try to isolate the most relevant material to the crimes under investigation.

Author Suggestion: Treat Warrants Like Wiretaps

- Require minimization procedures, to avoid interception of innocent communications as much as possible.
- Provide reports to the issuing judge of the warrant's progress.
- Allow ongoing monitoring by the judge to address concerns in real time.
- Incentivize efficient searches.

In fact, the methodology used by today's digital forensic investigators typically consists of a series of dynamic filtering techniques, including key word searches; triage based on the type of file (e.g., operat-

   ISSN 1098-5190

ing system files, executables, databases, spreadsheets, etc.) and the file name; and further triage by looking at the 5-10 words before and after a key word hit. Typically, it is only after multiple layers of dynamic filtering that the examiner looks at the contents of a file. Moreover, because it is not practical to do a ''full'' forensic analysis, forensic examiners typically conduct just that level of analysis sufficient to address the allegations that are the focus of the investigation; indeed, once they have identified enough evidence to prove or disprove the allegations at issue, the forensic investigator will typically suspend the analysis unless necessary to address questions raised by the agents or prosecutors or arguments likely to be raised by the defense.

But if the cases requiring the use of search protocols for computers – and the expansion of those protocols to search warrants for e-mails – tell us anything, it is this: there is a growing unease among judges that digital searches are not conducted in a reasonable manner, and that judges lack the tools to control or supervise the manner in which these warrants, once issued, are executed.

So is there a way for courts to exercise greater oversight over digital search warrants and place appropriate and workable limits on the manner of their execution, while also allowing law enforcement officers to do their jobs? And is there a way for courts to exercise this oversight even before a case ever gets to the indictment stage, let alone a motion to suppress? Is there way to protect privacy interests in a new, and ever-changing, digital world? We suggest that the answer to all of these questions is yes, and that courts need not look very far to find a model that works.

Treating Warrants Like Wiretaps

Federal judges already have a workable, effective framework for overseeing the execution of warrants for electronic communications and other data: the rules governing wiretaps.

Wiretap orders are essentially search warrants authorizing the interception of communications over telephones or e-mail. But unlike search warrants for stored e-mails or other data, wiretaps are search warrants for phone conversations or e-mails executed *in real time*. As such, they present special privacy challenges, and judges have special procedures for addressing those challenges, including:

■ **Minimization procedures:** When applying for a wiretap order, the government must affirm to the judge that it has instituted procedures for minimizing the interception of innocent, non-criminal conversations. The government need not specify in the application what those procedures are, just that they are in place and that the agents have been instructed to follow them. The minimization procedures used by federal prosecutors and agents tend to be fairly standardized, although there may be variations based on the facts and circumstances of each case.

■ **Reporting requirements:** With a typical federal search warrant, the issuing judge receives a ''return'' – a report listing what was seized – within 14 days after issuance of the warrant. In the case of a computer or e-mail search warrant, that return describes the computers or other devices seized or the e-mail account disclosed by the provider, but the judge gets no further report regarding the actual search of the contents of the computer or e-mail account, which may not occur for months after the initial seizure. By contrast, federal wiretap orders are good for only 30 days each, and the government is required to provide reports to the court on or about the 10^{th}, 20^{th}, and 30^{th} day after issuance. Those reports typically include examples of criminal conversations being intercepted over the target phone or e-mail account. They also include data demonstrating that agents are properly minimizing interception of non-criminal communications. If new targets are identified, the government advises the court that they are being added to the list of target subjects. And if the wiretap reveals that the targets are committing new or different crimes than those specified in the wiretap order – essentially, the equivalent of finding evidence of other crimes in ''plain view'' – the government does not seek a new wiretap, but rather informs the court of the new crimes and advises the court of its intention to intercept communications relating to those crimes as well.

■ **Ongoing monitoring by the judge:** The issuing judge does not sign a wiretap and then wait months to find out what happened. Instead, periodic reports allow the issuing judge to take an active role in monitoring the execution of the warrant and ensuring that it is done in a reasonable manner. If the judge is not satisfied with the agents' efforts to minimize interception of non-criminal communications, or objects to the government's plan to intercept communications about a newly discovered offense, or is otherwise unhappy about any aspect of the execution of the wiretap warrant, those concerns can be addressed in real time while the execution is still ongoing.

These procedures, which are set forth in the wiretap statute, exist in part because wiretaps have traditionally been viewed as one of the most intrusive investigative techniques available to law enforcement. A search warrant for stored electronic communications is certainly no *more* intrusive than a wiretap permitting the ongoing interception of such communications. Thus, if judges have heightened privacy concerns about such warrants, they can adopt procedures modeled after those used in wiretaps to address these concerns. For example:

■ **Minimization procedures:** The court could require the government to attest that it will adopt procedures designed to tailor its initial review of the seized material to the extent possible. That could mean the use of search terms or hash values where appropriate to narrow the amount of reviewed information, but the particular techniques would depend on the facts of the case, and the government need not be required to specify any particular techniques in advance.

■ **Reporting requirement:** The court could require the government to provide a report after 90 days regarding the manner and progress of its search of the seized digital devices or e-mails. This report – in effect, a supplemental return – would allow the court to evaluate the reasonableness with which the search is being conducted. If the government has discovered evidence of other crimes in plain view, it would report that to the court as well. The court could require a further report, perhaps after another 90 days, as appropriate.

■ **Ongoing monitoring by the judge:** As a result of the 90-day report, the issuing judge would no longer be

in the dark about the manner in which the search authority was carried out. On the contrary, the court would have an ongoing oversight role, much like in the wiretap context. If a judge had concerns about the manner in which the search was being conducted, those concerns could be addressed, in close to real time, rather than waiting until the motion to suppress stage. The judge would also be in position to monitor the return of seized property in a timely manner.

■ **Incentive to conduct searches more efficiently:** The 90-day report and ongoing role for the court would have the added benefit of maximizing the incentive for the government to get these searches done more quickly. To say that federal forensic investigative resources are strapped would be a significant understatement. The forensic examiners at DOJ and other federal law enforcement agencies are overworked and underpaid, and there are not nearly enough of them. As a result, there are often significant backlogs and delays in conducting forensic examinations of seized digital devices, with prosecutors and investigators waiting months and months for the results. But no prosecutor wants to be in the position of reporting to a court that the search of computers seized months earlier has not yet taken place because of forensic backlogs. Judicially-imposed deadlines have a way of inspiring action and affecting resource allocation. Perhaps the pressure created by this reporting requirement will inspire DOJ to supplement, and make smarter use of, its digital forensics resources.

Authority to adopt these procedures arguably exists under the All Writs Act, 28 U.S.C. § 1651, although statutory changes and changes to Rule 41 would be needed to make this authority more explicit and to ensure uniformity. But in the absence of changes to Rule 41, it is critically important that judges within a circuit – if not across circuits – attempt to develop a consistent set of practices regarding the timing and format of reports and the nature of judicial oversight. The goal here should be to develop more uniform procedures, not to replace one set of inconsistent practices with another.

Conclusion

Balancing public safety and privacy in the digital world means ensuring that law enforcement can do its job effectively while preserving a meaningful role for the courts to prevent overreaching or excessive intrusion. Luckily, a framework already exists for achieving this balance. Applying procedures modeled on those found in the federal wiretap statute will protect both public safety and privacy, giving courts greater oversight over the execution of computer and e-mail search warrants without resorting to impractical and unworkable protocols.

  ECLR ISSN 1098-5190