SEARCH WARRANT HANDBOOK

Office of Chief Counsel
Criminal Tax Division

2009

PREFACE

Criminal Tax attorneys frequently provide legal advice to Criminal Investigation personnel with respect to search warrant applications. To assist in evaluating such applications, this handbook provides an overview of search warrant law. The overview provided herein is not intended to take the place of thorough legal research with respect to a particular search warrant application.

This handbook does not create or confer any rights, privileges, or benefits on any person. It is not intended to have the force of law or of a statement of Internal Revenue Service policy. *See United States v. Caceres*, 440 U.S. 741 (1979).

s/ Edward F. Cronin
EDWARD F. CRONIN
Division Counsel/Associate Chief Counsel
(Criminal Tax)
Internal Revenue Service

TABLE OF CONTENTS

search, threw her to the ground, and handcuffed her so tightly as to cause pain. Assuming these allegations to be true, the court concluded that the agent's conduct violated the Fourth Amendment, that a reasonable agent in his position would have known that it did, and that therefore the agent was not entitled to qualified immunity on those charges. 342 F.3d at 1059. However, with respect to the plaintiff's claim that detaining her in handcuffs during the search was unlawful, the court held that even though the agent had violated her constitutional rights, he was entitled to qualified immunity as to this portion of her claim. The court explained that, at the time of the search, the case law had not clearly established that this conduct violated the plaintiff's constitutional rights. *Id.* at 1065.

Qualified immunity was held not to apply with respect to any of the claims brought against IRS agents in *Tekle v. United States,* 511 F.3d 839 (9th Cir. 2007). In that case, the agents executed search and arrest warrants at the home of the plaintiff's parents, who were suspected of narcotics trafficking and tax-related offenses. During the search, the agents allegedly held a gun to the head of the eleven-year-old plaintiff, who was unarmed and barefoot, handcuffed him, pulled him up by the chain of the handcuffs, and detained him with the handcuffs on for approximately 15 minutes and then for an additional 10-15 minutes with guns still drawn. The plaintiff brought a *Bivens* action against the agents for the use of excessive force and for subjecting him to an unreasonable detention. The Ninth Circuit held that agents were not entitled to assert qualified immunity because "a reasonable officer should have known that it was constitutionally excessive to use such force and to use the handcuffs in the manner alleged against an unarmed eleven-year-old child who was fully complying with the officer's requests." 511 F.3d at 856.

C. Government Liability

In addition to claims against individual officials, the Federal Tort Claims Act ("F.T.C.A.") provides that a civil action alleging an illegal arrest, search, or seizure by a federal officer may be brought directly against the United States government. 28 U.S.C. § 2680(h). The relevant portion of § 2680(h) provides that the federal government is not immune to suit with regard to "acts or omissions of investigative or law enforcement officers of the United States Government" for "any claim arising ... out of assault, battery, false imprisonment, false arrest, abuse of process, or malicious prosecution." *Id.* The provision defines "investigative or law enforcement officer" as "any officer of the United States who is empowered by law to execute searches, to seize evidence, or to make arrests for violations of Federal law." *Id.*

VII. COMPUTER-RELATED SEARCHES AND SEIZURES

Computer-related searches and seizures are subject to the same Fourth Amendment requirements that apply to any search or seizure: a warrant is generally required if the target has a reasonable expectation of privacy in the computer to be searched, and the warrant application must be evaluated for probable cause and particularity. However, the legal analysis of these issues must take into account the unique characteristics of computers, which enable users to store vast amounts of

information and to share or restrict access to that information in various ways. Further, when searching computers, law enforcement agencies are subject to specific restrictions and obligations under the Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq.* and the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa *et seq.*

A. Reasonable Expectation of Privacy

The analysis of an individual's expectation of privacy with respect to a computer depends on the location and ownership of the computer and the extent to which it may be accessed by others. Courts have held that an individual generally has a reasonable expectation of privacy with respect to his or her home computer. *See United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004); *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001). Conversely, an employee may have a reduced expectation of privacy in his or her office computer, especially if that computer is subject to some level of monitoring by his or her employer. *See United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000).

When two or more individuals share a computer, or when an individual's computer has file-sharing software or is attached to a network, courts must engage in a fact-intensive analysis to determine whether Fourth Amendment protections apply. In such situations, if access to files is limited by a password or other means, there may be a reasonable expectation of privacy. *See Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001); *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007).

Like files shared over a network, emails and other transmissions generally lose their reasonable expectation of privacy and thus their Fourth Amendment protection once they have been sent from an individual's computer. *See United States v. Lifshitz*, 369 F.3d at 190; *Guest v. Leis*, 255 F.3d at 333. A similar principle applies to a computer user's subscriber information, which is shared with an internet service provider and is therefore not subject to Fourth Amendment protections. *See United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008).

B. Probable Cause

As with all searches, if there is a reasonable expectation of privacy and the warrant requirement applies, applications for computer-related warrants must be evaluated for probable cause. In general, the probable cause analysis for computer-related searches is no different from the analysis for other searches. *See United States v. Giberson*, 527 F.3d 882, 888-89 (9th Cir. 2008) (stating, with respect to a computer search for tax records and other documents, that "the potential intermingling of materials [on a computer] does not justify an exception or heightened procedural protections for computers beyond the Fourth Amendment's reasonableness requirement."). *But see United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (en banc) (imposing new procedural requirements with respect to the search and seizure of electronic data from a non-suspect third party). As with other types of searches, the connection between the place to be searched and the items to be seized may be inferred if that inference has "common sense appeal." *United States v. Perry*, 531 F.3d 662, 665 (8th Cir. 2008).

For example, in *United States v. Khanani*, a case involving immigration violations, money laundering conspiracy, and the evasion of federal employment and income taxes, the defendant contended that the seizure of his computers was without probable cause because the affidavit submitted with the warrant application provided no fact-specific reason to believe there were computers in his office, or that his computers had been used to facilitate the commission of any of the alleged criminal violations. 502 F.3d 1281, 1290 (11th Cir. 2007). The court disagreed, noting that the affidavit described the defendant as an accountant for one of the co-conspirators and that one of the tax returns for that individual had been found in the trash outside the defendant's office:

> While the Master Affidavit did not indicate that it was a computer-generated tax form, in reviewing the affidavit to ascertain whether it furnished probable cause for the warrant sought, the affidavit is given a "common sense and realistic" interpretation. ... Additionally, [a witness for the government] testified, that prior to the warrant application, he had entered [the defendant's] office and observed connected computers. The district court did not err in concluding that the allegations of the Master Affidavit were sufficient to provide probable cause for the seizure of computers from [the defendant's] accounting business.

Id. (citations omitted). As this quotation indicates, the same "common sense" standard that applies to probable cause determinations in general also applies in the context of computer-related searches and seizures. *See Illinois v. Gates*, 462 U.S. 213, 238 (1983) ("The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, ... there is a fair probability that contraband or evidence of a crime will be found in a particular place.").

C. Particularity

Computer technology poses unique challenges with respect to the particularity requirement. Because computers are capable of storing and intermingling a great deal of information, and because computer data may be mislabeled or otherwise concealed, it may be difficult to draft a computer search warrant that is comprehensive without being overbroad. This potential for overbreadth, however, underscores the importance of drafting computer search warrants with sufficient particularity. *See United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important.").

In *Otero*, a case involving charges of mail fraud and credit card theft against a postal carrier, the Tenth Circuit emphasized that "warrants for computer searches must *affirmatively limit* the search to evidence of specific federal crimes or specific types of

material." 563 F.3d at 1132 (citation omitted; emphasis in original). The court held that the warrant at issue lacked sufficient particularity on the following grounds:

> Attachment B is quite neatly divided into two subsections: "ITEMS TO BE SEIZED" and "COMPUTER ITEMS TO BE SEIZED." Each paragraph under the first section takes pains to limit the search to evidence of specific crimes or evidence pertaining to specific persons along Ms. Otero's delivery route. Each paragraph under the second section, in contrast, has no limiting instruction whatsoever. Read alone, they each authorize a search and seizure of "[a]ny and all" information, data, devices, programs, and other materials. There is no explicit or even implicit incorporation of the limitations of the first five paragraphs. The computer-related paragraphs do not even refer to the rest of the warrant. In fact, the presence of limitations in each of the first five paragraphs but absence in the second four suggests that the computer searches are *not* subject to those limitations. Even when read in the context of the overall warrant, therefore, the paragraphs authorizing the computer search were subject to no affirmative limitations.

Id. at 1132-33. The *Otero* holding indicates that explicit references to "affirmative limitations," such as a description of the specific crimes suspected, must be made in the computer section of a search warrant in order to satisfy the particularity requirement. *See also United States v. Adjani*, 452 F.3d 1140, 1149 (9th Cir. 2006) (holding that the warrant at issue satisfied the particularity requirement in part because "the government here did describe at some length both the nature of and the means of committing the crime.").

Although courts have emphasized the need for particularity in computer search warrants, they also recognize that the government may be unable to search for specific computer files during the execution of a warrant and may need to conduct a wholesale seizure of the computers themselves for subsequent searching. *See, e.g., Guest v. Leis*, 255 F.3d 325, 335 (6th Cir. 2001) ("Because of the technical difficulties of conducting a computer search in a suspect's home, the seizure of the computers, including their content, was reasonable in these cases to allow police to locate the offending files."); *Upham*, 168 F.3d at 535 ("it is no easy task to search a well-laden hard drive by going through all of the information it contains ... The record shows that the mechanics of the search for images later performed off site could not readily have been done on the spot."). It cannot be assumed, however, that the seizure of a computer for off-site searching is justified in every instance. Rather, to satisfy the particularity requirement, a search warrant affidavit must provide facts that support the need for an off-site search. *See United States v. Hill*, 459 F.3d 966, 975-76 (9th Cir. 2006) ("We do not approve of issuing warrants authorizing blanket removal of all computer storage media for later examination when there is no affidavit giving a reasonable explanation ... as to why a wholesale seizure is necessary.").

Consideration should also be given to the possibility of imaging a computer's hard drive rather than seizing the computer itself, because removal of the computer may make it impossible for the target to continue conducting business. *See, e.g., United States v. Rayburn House Office Building, Room 2113, Washington, D.C. 20515*, 497 F.3d 654, 670 (D.C. Cir. 2007) (noting that one of the ways in which FBI agents who searched a congressman's office minimized disruption was by "imaging computer hard drives rather than searching the computers").

D. Ninth Circuit Procedural Requirements

In a recent en banc opinion involving the search of a non-suspect third party's computers, the Ninth Circuit introduced new procedural requirements for computer-related searches. *See United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009). The court described these new guidelines as follows:

> 1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases. ...
>
> 2. Segregation and redaction must be either done by specialized personnel or an independent third party. ...
>
> 3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora. ...
>
> 4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents. ...
>
> 5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

579 F.3d at 1006.

E. Privacy Statutes that May Apply to Computer Searches

1. The Stored Communications Act

In general, the Fourth Amendment does not protect communications held in electronic storage, such as email messages stored on a server, because internet users do not have a reasonable expectation of privacy in such communications. Further, because the Fourth Amendment applies to government searches rather than searches by private actors, it does not appear to limit the ability of internet service providers ("ISPs") to obtain customer information and disclose it to the government. To fill this

gap, the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-11,[19] establishes certain protections for customer information in the possession of ISPs. *See* 18 U.S.C. § 2703. Specifically, if the government seeks to compel disclosure of the contents of electronic communications and other information without prior notice to customers or subscribers, the SCA requires that a valid search warrant be obtained. *See Guest v. Leis,* 255 F.3d 325, 339 (6th Cir. 2001).

2. The Privacy Protection Act

The Fourth Amendment also does not apply to searches and seizures of documentary evidence in the possession of innocent third parties, such as the press. *See Zurcher v. Stanford Daily,* 436 U.S. 547 (1978). However, the Privacy Protection Act of 1980 ("PPA"), 42 U.S.C. § 2000aa *et seq.*, makes it unlawful for a government employee to search for or seize documentary materials possessed by a person with a purpose to disseminate some form of public communication. 42 U.S.C. §§ 2000aa(a); (b). The PPA generally does not apply if the materials sought constitute contraband or the means of committing a criminal offense, or if there is probable cause to believe the person possessing the materials has committed a criminal offense to which the materials relate. 42 U.S.C. § 2000aa(a).

As the Sixth Circuit has observed, interpretation of the PPA presents particular challenges in the context of computer searches. *See Guest v. Leis,* 255 F.3d 325, 341 (6th Cir. 2001). These challenges stem from the difficulty of "separat[ing] the offending materials from other 'innocent' material on the computer." *Id.* at 341-42. In *Guest,* the court expressed concern that criminals might seek to insulate electronically-held criminal evidence from search and seizure by including PPA-protected materials on their computers. *See id.* at 342. Accordingly, the court held that "when protected materials are commingled on a criminal suspect's computer with criminal evidence that is unprotected by the act, we will not find liability under the PPA for seizure of the PPA-protected materials." *Id.* The court cautioned, however, that "police may not then search the PPA-protected materials that were seized incidentally to the criminal evidence." *Id.* In the case before it, the court declined to find the defendants liable under the PPA because the owner or operator of the computers at issue was a criminal suspect, and the PPA-protected materials were not searched. *Id.*

[19] The SCA is Title II of the Electronic Communications Privacy Act ("ECPA"), Pub. L. 99-508, 100 Stat. 1848.