**January**
**2014**
**Volume 62**
**Number 1**

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC
20530

H Marshall Jarrett
Director

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0 22(b)

The United States Attorneys' Bulletin is published bimonthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201

**Managing Editor**
Jim Donovan

**Associate Editor**
Carmel Matin

**Law Clerk**
Jennifer Jokerst

**Internet Address**
www usdoj gov/usao/
reading_room/foiamanuals
html

Send article submissions and address changes to Managing Editor, United States Attorneys' Bulletin, National Advocacy Center, Office of Legal Education, 1620 Pendleton Street, Columbia, SC 29201

# Cyber-Investigative Issues I

**In This Issue**

# Using the PIRL List to Get the Most out of Forensic Searches and to Draft Unassailable Search Warrants

*Michael L. Levy*
*Assistant United States Attorney*
*Eastern District of Pennsylvania*

*Timothy M. O'Shea*
*Assistant United States Attorney*
*Western District of Wisconsin*

## I. Introduction

The Prosecutor's Initial Reference List for Windows-based Computers (PIRL-Windows) is a plain English guide for an initial forensic analysis of Windows-based computers. A PIRL-Apple iOS guide, addressing the forensic review of iPhones, iPads, etc., that use the Apple iOS, is forthcoming. Experienced forensic analysts and line prosecutors created this guide and its companion, a Prosecutor's Initial Reference List for Cell Phones (PIRL Cell Phones). The original idea of the PIRL List was conceived by now retired Assistant U.S. Attorney Martin Littlefield of the Western District of New York. The two guides have repeatedly proved helpful in investigations and during trial preparation. The PIRL Lists have also proven helpful in drafting search warrants that allow the analysts to defeat future "some other dude did it" defenses and to collect evidence that proves the relevant mens rea. This article focuses on using the PIRL-Windows List as a guide when writing the application and warrant. However, its general discussion should be of value to all search warrants.

An application for a search warrant must show probable cause that a crime has been committed, that there is probable cause to believe that evidence of the crime will be found in the place to be searched, and that there is probable cause to seize the evidence. In addition, the things that the agent seeks authority to seize must be described with specificity. Agents and federal prosecutors are very proficient in drafting search warrants, applications, and supporting affidavits that demonstrate probable cause to believe both that a crime has been committed and that evidence of that crime will be found in the place to be searched. However, we often fail to draft a good "Items to be Seized" list. In addition, we sometimes fail to develop facts in the affidavit that justify seizing those items. This inadequacy results, in part, from a failure to recognize that a search warrant is not a grand jury subpoena. Probably more important is that by the time we finish writing (or reviewing) the affidavit for the first two items, we run out of energy. The purpose of this article is to give guidance on how we can do a better job in this third area, showing that there is probable cause to seize the evidence.

## II. General considerations: overbreadth and particularity

It is important to focus on key language in the Fourth Amendment: "*. . . and no Warrants shall issue, but upon probable cause*, supported by Oath or affirmation, and *particularly describing the* place to be searched, and the persons or *things to be seized*." U.S. CONST. amend. IV (emphasis added). These italicized phrases form the basis of two distinct problems of Fourth Amendment law: overbreadth and lack of particularity. An overbroad warrant is one that makes clear what the agents can seize, but the supporting affidavit does not provide probable cause to justify the seizure of some or all of those items.

*United States v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars and Fifty-Seven Cents ($92,422.57)*, 307 F.3d 137, 149 (3d Cir. 2002) ("We have contrasted a 'general warrant' with a warrant that is simply overly broad. An overly broad warrant describes in both specific and inclusive generic terms what is to be seized, but it authorizes the seizure of items as to which there is no probable cause.") (some internal quotations omitted). Justice Sotomayor succinctly stated, "the police must articulate an adequate reason to search for specific items related to specific crimes." *Messerschmidt v. Millender*, 132 S. Ct. 1235, 1253 (2012) (Sotomayor, J., dissenting).

A warrant that fails adequately to describe the things to be seized is often referred to as a general warrant. General warrants do not limit what can be seized and are the descendants of the colonial writs of assistance. *Sanford v. Texas*, 379 U.S. 476, 481 (1965). The Supreme Court described these warrants in *Andresen v. Maryland*:

> General warrants of course, are prohibited by the Fourth Amendment. "(T)he problem (posed by the general warrant) is not that of intrusion Per se, but of a general, exploratory rummaging in a person's belongings. . . . (The Fourth Amendment addresses the problem) by requiring a 'particular description' of the things to be seized."

*Andresen v. Maryland*, 427 U.S. 463, 479 (1976).

The Supreme Court further explained the nature of general warrants:

> The particularity requirement of the Fourth Amendment has a manifest purpose—to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search is carefully tailored to its justification, and does not resemble the wide-ranging general searches that the Framers intended to prohibit.

*United States v. Leon*, 468 U.S. 897, 963 (1984) (Stevens, J., concurring and dissenting).

## A. Overbreadth

As noted above, the overbreadth problem is caused when the affidavit does not spell out the probable cause to seize the specific items that are listed in the warrant. The warrant clearly delineates what the agents can seize, but the justification to seize those things is lacking. It is up to us to make certain that the affidavit spells out the reasons that support the seizure of the evidence in this area. Too often, we do not make that connection clear. We often work on these warrants for weeks, but even if we only have a few hours, it is more time than the magistrate judge has to consider it. It makes little sense to hope that the magistrate judge will figure out the inferences. We should spell out plainly the inferences that justify the seizure of the evidence.

*Messerschmidt v. Millender*, 132 S. Ct. 1235 (2012), is a good illustration of how to do that. *Messerschmidt* is a civil rights suit against police who executed a search warrant. The sole issue in the case was whether the officers acted in good faith in relying on the warrant. The Court's methodology, explaining why an officer could believe that there was probable cause to seize all the items listed, effectively demonstrates how we should set forth the inferences and reasoning that justify the seizure.

In *Messerschmidt*, Jerry Ray Bowen was a member of the Los Angeles street gang, the Crips. His girlfriend got tired of his physical abuse and decided to move out. She requested assistance from the Los Angeles County Sheriff's Department to protect her while she did so. Some Sheriff's deputies came to assist, but were called away to an emergency. Bowen then arrived. Enraged, he beat her and unsuccessfully attempted to throw her over the railing of the second floor landing. He screamed at her, "I told you never to call the cops on me, bitch!" *Id.* at 1241. When she started to get away in her car, he fired a sawed off shotgun at her fleeing vehicle. She reported the incident to the police.

The police obtained a warrant for Bowen's new residence in which they sought any type of firearm, not just the sawed-off shotgun, and evidence of his affiliation with the Crips gang. The warrant described the items with particularity. The issue before the Supreme Court was whether the warrant was overly broad, that is, whether there was probable cause to seize the items listed in the warrant.

The Court found that the police could reasonably believe that a warrant, which authorized the seizure of all firearms, was valid, given Bowen's background as a gang member with a criminal record for violence and who had just fired his weapon at his girlfriend because she had "called the cops." *Id.* at 1246–47. Furthermore, the Court found that Bowen's violent history made it reasonable for the officers to believe that it was necessary to remove all firearms to prevent further violence, rather than removing just the sawed off shotgun used in the incident. *Id.*

With respect to the search for indicia of gang membership, the Court concluded that it was reasonable for the officers to believe that this evidence would have been relevant in prosecuting the assault. *Id.* at 1247. The Court explained that the Fourth Amendment permits searches for evidence that "will aid in a particular apprehension or conviction." *Id.* at 1247–48 (citing *Warden v. Hayden*, 387 U.S. 294, 307 (1967)). It noted that Bowen tried to murder his girlfriend because she had "called the cops," thereby risking disclosure of his gang activity to the police. *Id.* at 1247. The Court went on to state that gang affiliation evidence could be useful in impeaching Bowen at a trial or in rebutting defenses. *Id.* at 1248. Finally, if evidence of gang affiliation were found during the search, it would provide evidence that he lived on the premises and, therefore, other evidence found at the residence could be attributed to him. *Id.*

This admittedly lengthy discussion of a gang case may seem a bit off track. However, how many of us put those types of justifications into the affidavits that we draft or approve? Why would we depend upon a magistrate judge to connect the dots or wait until the Supreme Court figures it out? With these explanations set forth, the probable cause to seize is clearer, and, if it is not enough, it bolsters the agent's good faith in relying on the warrant.

## B. Particularity

The particularity requirement prevents general rummaging through a person's belongings and gives assurance to the person whose property is being searched that the search is lawful and that the agents are acting within the scope of judicial authorization. *Id.* at 1252.

Particularity, however, does not mean that a description worthy of a photograph is always required. Special investigators in *Andresen v. Maryland*, 427 U.S. 463 (1976), obtained a search warrant after an investigation indicated that the defendant defrauded a purchaser of a lot. The search warrant listed numerous documents that were created in the real estate closing. However, after listing numerous specific items, the warrant included additional language authorizing the seizure of "other fruits, instrumentalities and evidence of crime at this time unknown." *Id.* at 479. The execution of the warrant resulted in the seizure of evidence of fraud relating to the original lot in the real estate closing, as well as similar frauds in the sale of other properties. The issue was whether the inclusion of the additional language invalidated the search warrant. The Supreme Court held that because the rest of the list dealt only with a fraud in relation to the sale of a particular lot, the clause was modified by that restriction and such description as a catchall phrase was constitutional.

The Court concluded that the executing "special investigators reasonably could have believed that the evidence specifically dealing with another lot . . . could be used to show [defendant's] intent with respect to the [original lot] transaction," in light of the fact that "they had been informed of a number of similar charges against [defendant] . . . and had become familiar with [his] method of operation." *Id.* at 483, 484. The Court also noted that such evidence of similar acts would be admissible to show intent and absence of mistake on the part of the defendant. *Id.* at 483. Therefore, the warrant could properly

authorize the seizure of this evidence, even though it did not relate directly to the crime under investigation. *Id.* at 484.

## III. Computer searches and the PIRL List

So, how does the need to show probable cause to seize evidence affect drafting computer search warrants? It is important to bear in mind that the search of a computer is much more than a search for documents because the computer is also a communications device. The analysis of the computer gives the prosecutor insight into the person's thought processes and allows the prosecutor to learn how and when the computer was used. Given how integrated the use of computers is into users' lives and the privacy concerns that result, judges are sensitive to the scope of a computer search warrant. It follows that the law of searching computers is often less favorable to the Government than the law for searching other items. Therefore, connecting the dots to show why there is probable cause to search for the items listed in the warrant may be more important when seeking authority to search a computer.

In addition to serving as filing cabinets, computers log a great deal of information that the user does not intentionally create. The PIRL List itemizes many of these things with an explanation of why you may find them useful, and it is a good tool for search planning. The Assistant U.S. Attorney and the agent should review the List to determine what should be put into the search warrant. It also gives them a tool for talking with a forensic examiner.

The most recent draft of the PIRL-Windows List now focuses on the evidentiary use that a prosecutor can make of many of these items. Specifically, the list addresses:

- User identity
- State of mind: knowledge, intent, consciousness of guilt, motive, absence of mistake
- Timeline
- Geographic location

### A. User identity

When drafting search warrants for physical locations (for example, a drug dealer's apartment), prosecutors routinely describe probable cause to search for and seize evidence of "indicia of use or control." They do so because evidence of who lived in the apartment where the drugs were found is as important as the drugs, guns, scales, etc., that were found in the apartment. Given the authority to seize evidence of use and control of the premises, agents take the suspect's mail and seize pictures depicting the suspect right off the apartment walls. Prosecutors, however, do not always apply the same mind set in the context of electronic evidence. As a result, the warrants do not give the analyst the necessary scope to search for indicia of use and control. For example, the warrant may direct the analyst to look for child pornography or stolen intellectual property, and for evidence of its transmission, but does not allow the analyst to figure out who was sitting behind the computer when the offending child pornography or stolen trade secret was viewed or transmitted. So, what is the analyst missing? When the warrant allows the analyst to search for indicia of use or control, the analyst can search the electronic information for evidence of identity by reviewing: the suspect's email (Did the suspect send an innocuous email to a friend just before viewing child pornography?), his Internet history (Did the suspect use the computer to pay his credit card bill?), all images on the computer (Are there pictures of the defendant, his friends, relatives, or pets?), and so on. Unnecessary litigation follows when analysts discover compelling evidence outside the scope of the warrant, too often with an unhappy result for the Government. *See, e.g.*, *United States v. Galpin*, 720 F.3d 436 (2d Cir. 2013) (explaining that heightened sensitivity to the particularity requirement is demanded in the context of digital searches).

## B. Mental state, timeline, and geographic location

As the limited examples above show, electronic evidence gives prosecutors multiple opportunities to prove the *identity* of the wrongdoer. The PIRL Lists, which delineate categories of information that can be found within computers and cell phones, help prosecutors understand that these devices also provide a unique view into: the suspect's *state of mind* (intent of the user, consciousness of guilt, motive, and knowledge that information—for example, child pornography or stolen trade secrets—is present on the device), the *timeline* of relevant events, and the *geographic location* of a user or device.

The PIRL-Windows List contains 36 "forensic requests" of electronic information within a Windows-based computer, which includes most computers. Adjacent to the request description, a "why this may be wanted" column describes how the evidence helps the prosecution establish identity, state of mind, timeline, and geographic location of the user or device. In a sense, this information is nothing new to prosecutors. These categories of relevant evidence are the bread and butter of how prosecutors have always proved the "who, what, when, and where" of a crime. We are simply applying the techniques of the physical world to electronic evidence. The forensic requests within the PIRL Lists are a good forensic starting point for many forensic reviews, and your analyst will likely have additional good ideas. The forensic ideas within the PIRL Lists, or that your analyst comes up with, however, cannot help prove your case if the warrant and affidavit do not allow the agent to search the electronic device for evidence of identity, state of mind, timeline, and geographic location.

In many cases, you will be looking for evidence that the subject intended to commit the crime or knew that certain facts existed. In other cases, a suspect may delete files or use counter-forensic tools such as Evidence Eliminator, which will show consciousness of guilt. Evidence Eliminator works by wiping files and making them not discoverable. In some cases, questions about whether the defendant knew something or when he did something may be critical. These are all things that you should have the warrant authorize the agents to "seize" when they search the computer.

Warrants that allow the analyst to look for "indicia of use or control" are nearly unassailable to defense challenges based on scope of the warrant. When the analyst is permitted to search for evidence of use and control, he or she can review all the emails, chats, Internet searches, images, videos, registry information, and more, to understand who has use and control of the computer. Moreover, when the affidavit contains facts justifying the search for other relevant evidence, such as *state of mind* (Did the suspect try to destroy electronic evidence?), *timeline* (Did the suspect make an online purchase just before accessing the contraband information?), and *geographic location* (Is there an image showing the defendant at a particular place relevant to the crime?), and this information is listed on the "Items to be Seized" list, then the warrant should be bulletproof from claims of overbreadth and lack of particularity.

## C. Practical tips

There is no need for prosecutors to reinvent the wheel. The Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) Web site has a sturdy computer search warrant go-by (Premises search warrant), that prosecutors can use and adapt for their own cases. The CCIPS go-by contains draft language, in both the affidavit and "Items to be Seized" list, supporting the search for "user attribution evidence," timeline, and, to a lesser degree, intent.

In drafting a warrant, you first need to explain in the affidavit why you want to look for items such as evidence of identity or state of mind. Do not put them into the "Items to be Seized" list without thinking about why you want them. You need to have probable cause to look for them. The facts of investigation will guide you here. Set forth in the affidavit why you want authority to search the computer for these types of items.

When drafting the "Items to be Seized" list, do not put down the particular place in the computer that one artifact might be found. If you do that, you will limit the forensic examiner's search ability. You

want to permit the search for generic things and let the examiner determine where to find them. Thus, you would usually want to list particular documents or information that you believe would be on the computer. You want the court to order the examiner to search for evidence that would tend to identify the person using the computer when those documents were created, read, or sent. You might want to look for evidence that would tend to show the knowledge of the defendant of certain facts or circumstances (for example, any evidence that would tend to show that the subject was aware of the contract requirements, the condition of the victim, etc.). These types of evidence could show that the subject created a "smoking gun" document, or read a document, which gave him knowledge of certain facts. In short, put into the "Items to be Seized" list the wish list of the kind of evidence that you need for a successful prosecution. Let the examiner find it for you.

Keep in mind that many of these things may be inculpatory or exculpatory, which is something that you want to know and almost any judge will let you look for. You can state in the affidavit that the absence of some evidence might be exculpatory and that is another reason to look for it.

## IV. Conclusion

Whether your warrant is for digital or physical evidence, drafting a detailed "Items to be Seized" list and having the affidavit justify the seizure of those items is critical. For computer searches, the PIRL-Windows List can help you perform this drafting. Consult with your office's Computer Hacking and Intellectual Property prosecutor(s) or with the CCIPS duty attorney for additional assistance with computer and electronic device searches or evidence.❖

**ABOUT THE AUTHORS**

❑**Michael L. Levy** is an Assistant U.S. Attorney for the Eastern District of Pennsylvania and is currently Chief of the Computer Crimes Section. He has previously served as the Interim U.S. Attorney, Deputy Chief of the Criminal Division, and First Assistant. Mr. Levy has been an AUSA since 1990, after previously serving in the same capacity from 1980 to 1983. Mr. Levy also has engaged in private practice and served as Special Attorney for the Philadelphia Strike Force. He is an Adjunct Professor of Law at the University of Pennsylvania Law School and has lectured frequently at the National Advocacy Center. ✠

❑**Timothy M. O'Shea** has been an Assistant U.S. Attorney for the Western District of Wisconsin since 1991, Senior Litigation Counsel since 2002, and his district's Computer Hacking and Intellectual Property prosecutor since the inception of the program. As a general crimes prosecutor, Mr. O'Shea currently chairs the PIRL working group, regularly lectures at the National Advocacy Center, and has contributed to three manuals published by the Office of Legal Education: Federal Grand Jury Practice in 2008, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations in 2009, and Federal Criminal Discovery in 2011. ✠

# Consensual Searches of Computers and Assumption of Online Identities

*Edward J. McAndrew*
*Assistant United States Attorney*
*District of Delaware*

Evidence, fruits, and instrumentalities of most crimes are often held in digital devices and online accounts of suspects, victims, and witnesses. Across the spectrum of criminal investigations, questions frequently arise about consensual searches of digital devices in homes, cars, and workplaces. In addition, the consensual assumption of a person's online identity has become an increasingly popular investigative technique in proactive investigations. This article will summarize some of the major principles concerning consensual searches of digital devices and the consensual assumption of an individual's online identity. In particular, this article will highlight relevant precedent developed since the publication of Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 15–26, 42–56 (Aug. 2009). Also included are suggested go-bys for obtaining and memorializing written consent for warrantless searches of digital devices and the assumption of online identities.

## I. General principles governing warrantless searches of digital devices conducted pursuant to consent

Fourth Amendment rights attach where a person has a reasonable expectation of privacy in their "person[], houses, papers, and effects." U.S. CONST. amend. IV; *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Under the "trespass" theory, the Fourth Amendment also is implicated where the Government "physically occupie[s] private property for the purpose of obtaining information." *Jones v. United States*, 132 S. Ct. 945, 949-50 (2012); *see also Florida v. Jardines*, 133 S. Ct. 1409, 1414

(2013).

### A. The *Jones* trespass theory

The applicability of the trespass theory to physical searches of digital devices appears to have not yet been examined in detail by any federal court. A number of courts, however, have rejected defense arguments based on the trespass theory in a variety of related contexts. *See, e.g.*, *United States v. Huart*, 735 F.3d 972, 974 (7th Cir. 2013) (no trespass by warrantless search of cellphone smuggled into BOP facility); *United States v. Cowan*, 674 F.3d 947, 955-56 (8th Cir. 2012) (no trespass by using key fob to identify car); *United States v. Alabi*, 943 F. Supp. 2d 1201, 1264 (D.N.M. 2013) (no trespass by warrantless scanning of bar codes on debit and credit cards).

*Jones* itself touches on what might be called remote, virtual, or "electronic" searches of digital devices—searches conducted where the device itself is not in the physical custody of the searching agent. *Jones*, 132 S. Ct. at 953 (majority opinion), 962 (Alito, J., concurring). In his concurring opinion, which was joined by three other justices, Justice Alito wrote:

> [T]he Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked. For example, suppose that the officers in the present case had followed respondent by surreptitiously activating a stolen vehicle detection system that came with the car when it was purchased. Would the sending of a radio signal to activate this system constitute a trespass to chattels? Trespass to chattels has traditionally required a physical touching of the property. *See* RESTATEMENT (SECOND) OF TORTS § 217 and Comment e (1963 and 1964); Dobbs, *supra*, at 123. In recent years, courts have wrestled with the application of this old tort in cases involving unwanted electronic contact with computer systems, and some have held that even the transmission of electrons that occurs when a communication is sent from one computer to another is enough. *See, e.g.*, *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997); *Thrifty–Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559, 1566, n.6, 54 Cal. Rptr. 2d 468 (1996). But may such decisions be followed in applying the Court's trespass theory? Assuming that what matters under the Court's theory is the law of trespass as it existed at the time of the adoption of the Fourth Amendment, do these recent decisions represent a change in the law or simply the application of the old tort to new situations?

*Id.* at 962. The majority had a clear, one-sentence answer to these questions: "Situations involving merely the transmission of electronic signals *without trespass* would *remain* subject to [the] *Katz* analysis." *Id.* at 953 (emphasis added as to "without trespass").

The majority's answer, of course, can be read to beg the concurrence's questions. What exactly "without trespass" means in the electronic context remains to be seen. As the law begins to develop under this theory, it is important to remember that the legislative history of the Computer Fraud and Abuse Act speaks of certain violations of § 1030 as "trespass[es]" into protected computers by hackers. *See, e.g.*, *United States v. Stratman*, No. 4:13-CR-3075, 2013 WL 5676874, at *2 (D. Neb. Oct. 18, 2013) (summarizing legislative history). For example, a 1996 Senate Report on the amendment of § 1030 under the Economic Espionage Act stated:

> [U]nder the bill, insiders, who are authorized to access a computer, face criminal liability only if they intend to cause damage to the computer, not for recklessly or negligently causing damage. By contrast, outside hackers who break into a computer could be punished for any intentional, reckless, or other damage they *cause by their trespass*.
>
> The rationale for this difference in treatment deserves explanation. Although those who

> intentionally damage a system, without authority, should be punished regardless of whether they are authorized users, it is equally clear that anyone who knowingly invades a system without authority and causes significant loss to the victim should be punished as well, even when the damage caused is not intentional. *In such cases, it is the intentional act of trespass that makes the conduct criminal . . . .*

S. Rep. No. 104-357, at 10-11 (1996) (emphasis added). Similarly, a 1986 House Report described § 1030(a)(5) as:

> a "malicious damage" felony violation involving a Federal interest computer. We have included an "intentional" standard for this felony and coverage is extended only to *outside trespassers* with a $1,000 threshold damage level.

H.R. Rep. No. 99-612, at 7 (1986), *quoted in United States v. Morris*, 928 F.2d 504, 508 (2d Cir. 1991); *see also Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 966 (D. Ariz. 2008) ("[L]egislative history confirms that the CFAA was intended to prohibit *electronic trespassing*, not the subsequent use or misuse of information.").

So far, courts have relied on the *Jones* majority's limiting statement regarding electronic surveillance to reject application of the trespass theory to remote, virtual, or electronic searches of digital files or electronic signals emanating from a device that is not in the physical custody of the searching agent. For instance, a number of district courts have rejected Fourth Amendment challenges based on the trespass theory where investigators have downloaded files shared over peer-to-peer networks. *See, e.g.*, *United States v. Brashear*, No. 4:11-CR-62, 2013 WL 6065326, at *3 (M.D. Pa. Nov. 18, 2013) (no trespass into defendant's computer by search of shared files via peer-to-peer network); *Russell v. United States*, No. 4:11CV1104, 2013 WL 5651358, at *7 (E.D. Mo. Oct. 16, 2013) (same); *United States v. Brooks*, No. 12-CR-166, 2012 WL 6562947, at *5 (E.D.N.Y. Dec. 17, 2012) (same as to "closed" network); *United States v. Nolan*, Crim. A. No. 11-82, 2012 WL 1192183, at *10–11 (E.D. Mo. Mar. 6, 2012) (similar). At least some courts also have declined to apply the trespass theory where investigators have "pinged" cell phones to locate suspects. *See, e.g.*, *United States v. Caraballo*, No. 5:12CR105, 2013 WL 4039028, at *10 (D. Vt. Aug. 7, 2013) (pinging cellphone does not constitute search under trespass theory); *United States v. Dooley*, No. 1:11-CR-255, 2013 WL 2548969, at *18 n.39 (N.D. Ga. June 10, 2013) (same).

### B. The *Katz* "reasonable expectation of privacy" theory

Putting aside the trespass theory, the Fourth Amendment is not infringed if the Government's conduct does not violate a person's reasonable expectation of privacy. *See, e.g.*, *Illinois v. Andreas*, 463 U.S. 765, 771 (1983); *United States v. Katzen*, 732 F.3d 187, 193, 197–98 (3d Cir. 2013); *United States v. Kastellanos*, 716 F.3d 828, 832–33 (4th Cir. 2013). Determining whether a reasonable expectation of privacy exists involves a two-step inquiry. *See, e.g.*, *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *United States v. Barrows*, 481 F.3d 1246, 1248 (10th Cir. 2007). First, the person must have an actual or subjective expectation of privacy. Second, that expectation must be one that society is prepared to recognize as objectively reasonable. *Katz*, 389 U.S. at 361; *Barrows*, 481 F.3d at 1248.

It is fairly well established that "individuals generally possess a reasonable expectation of privacy in their home computers." *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004); *see also United States v. Andrus*, 483 F.3d 711, 718 (10th Cir. 2007) ("[F]or most people, their computers are their most private spaces."); *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007); *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001). *But see United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009) (no reasonable expectation of privacy in files stored on computer but accessible through peer-to-peer sharing applications); *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008) (same); *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008) (same). This can be true whether the

person owns, leases, or otherwise uses a computer or account with authorization. *See, e.g.*, *United States v. Buckner*, 473 F.3d 551, 554 n.2 (4th Cir. 2007) (user of leased computer had reasonable expectation of privacy in password-protected files). Subject to the limitations discussed below, this expectation also can exist as to computers used at work, particularly if they hold personal information. *Compare Leventhal v. Knapek*, 266 F.3d 64, 75 (2d Cir. 2001) (reasonable expectation of privacy in work computer), *with Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2001) (no reasonable expectation of privacy in work computer).

Individuals also may possess a reasonable expectation of privacy in the contents of online accounts, particularly where they take steps to maintain the privacy of those accounts. *See, e.g.*, 18 U.S.C. §§ 2701–2712 (2013) (Stored Communications Act); *United States v. Lucas*, 640 F.3d 168, 178 (6th Cir. 2011) (email); *United States v. Warshak*, 631 F.3d 266, 283–88 (6th Cir. 2010) (email). *But see Chaney v. Fayette Cnty. Pub. Sch. Dist.*, No. 3:13-cv-89-TCB, 2013 WL 5486829, at *4–5 (N.D. Ga. Sept. 30, 2013) (plaintiff surrendered reasonable expectation of privacy in photograph posted on her "semi-private" Facebook profile, viewable by "friends and friends of friends"); *United States v. Bode*, No. ELH-12-158, 2013 WL 4501303, at *20–21 (D. Md. Aug. 21, 2013) (no reasonable expectation of privacy in chat logs conducted via social networking Web site where banners notified users that unlawful activity would be reported to law enforcement).

## C. The consent exception to the warrant requirement

Authorized and voluntary consent is a well-established exception to the requirement that probable cause exists and a warrant be obtained to conduct a search of a place or an effect in which a Fourth Amendment interest exists. *See, e.g.*, *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973) ("It is equally well settled that one of the specifically established exceptions to the requirements of both a warrant and probable cause is a search that is conducted pursuant to consent."). The "consent" exception applies to digital devices and computer networks, just as it applies to physical places and other containers. *See United States v. Stabile*, 633 F.3d 219, 230–31 (3d Cir. 2011); *United States v. King*, 604 F.3d 125, 137 (3d Cir. 2010); *United States v. Anderson*, No. 13-1003, 2013 WL 5498114, at *3-4 (7th Cir. Oct. 21, 2013) (consent to search for "documents" reasonably includes digital files contained on computers). Consent may be explicit or implicit, and the authority to consent may be actual or apparent. *See, e.g.*, *United States v. Buckner*, 473 F.3d 551, 555 (4th Cir. 2007); *United States v. Milian-Rodriguez*, 759 F.2d 1558, 1563–64 (11th Cir. 1985).

Two key concepts in the "consent" searches are the authority to provide consent and the scope of consent. Digital devices and networks may be owned or used by, or located within areas controlled by, multiple persons. Questions therefore often arise as to which persons have actual or apparent authority to consent to a search of a device or network. Devices are often located within places that are being searched for things beyond the devices themselves. Devices also often contain data about multitudes of subjects and aspects of the user's daily life. Questions therefore arise as to whether the device itself, and what data stored on a device, are encompassed within the scope of consent to search. Below is a summary of the general principles relating to authority and scope of consent, followed by sections outlining some of the recent precedent in the home and employment settings.

**Authority to consent:** It is common for more than one person to use a particular digital device. *See, e.g.*, *Stabile*, 633 F.3d at 232. In general, an owner or authorized user of a digital device can consent to a search of that device. *See, e.g.*, *id.*; *see also United States v. Tosti*, 733 F.3d 816, 818–19 (9th Cir. 2013) (wife had authority to consent to search of shared computers in shared home); *United States v. Mitchell*, No. 3:11-CR-248, 2013 WL 3808152, at *29–30 (M.D. Fla. July 22, 2013) (owner and possessor of iPhones and iPads used by another had at least apparent authority to consent to warrantless search). The owner has actual authority to provide such consent. Authorized users may have actual or apparent authority (or both) to do so. Thus, there is no Fourth Amendment violation where agents reasonably rely on the apparent authority of one who consents to a search. *See United States v. Morgan*,

435 F.3d 660, 663–64 (6th Cir. 2006) (agents reasonably relied on apparent authority of defendant's wife to consent to search of computer located in common room of home, even though wife maintained her own computer elsewhere); *United States v. Andrus*, 483 F.3d 711, 720–21 (10th Cir. 2007) (parent had apparent authority to consent to search of adult child's computer where parent had unrestricted access to bedroom and paid for Internet access).

Where there is "mutual use of the property by persons generally having joint access or control for most purposes," each user "has the right to permit the inspection in his own right and [ ] others have assumed the risk that one of their number might permit the common area to be searched." *United States v. Matlock*, 415 U.S. 164, 171 n.7 (1974); *Stabile*, 633 F.3d at 232–33. However, as to the search of dwellings at least, an authorized person cannot give valid consent in the presence of another authorized person who objects to a warrantless search. *See Georgia v. Randolph*, 547 U.S. 103, 121 (2006). Although police may not remove a potential objector simply "for the sake of avoiding a possible objection," the arrest and removal of a defendant will not invalidate the consent provided by a co-occupant. *See, e.g.*, *United States v. Hudspeth*, 518 F.3d 954 (8th Cir. 2008 ) (en banc) (wife could validly consent to residential search resulting in seizure of computer where defendant-husband was arrested at his workplace and voiced an objection to a warrantless residential search); *United States v. Trainor*, No. 4:09Cr066, 2011 WL 250431, at *4 (D.N.D. Jan. 26, 2011) (roommate could consent to search of desktop computer in living room that he occasionally used).

At least one circuit has held that *Randolph*'s rule regarding a present and objecting co-occupant simply does not apply to the consensual search of a computer during an otherwise lawful residential search. *See United States v. King*, 604 F. 3d 125, 134–37 (3d Cir. 2010). In *King*, the defendant installed his hard drive, which was later found to contain child pornography, in his girlfriend's laptop. After discovering that the defendant and his girlfriend were involved in the sexual exploitation of the girlfriend's daughter, agents arrived at the defendant and girlfriend's shared residence to execute an arrest warrant for the girlfriend relating to other conduct. During the execution of that arrest warrant, the girlfriend consented to the search of her laptop containing the defendant's hard drive, while the defendant objected to the search of his hard drive and asked to remove it from the laptop. Reading *Randolph* as limited to third party consent to search a dwelling, the Third Circuit denied the defendant's motion to suppress the evidence found on his hard drive. *Id.* at 135–37. Relying on *Matlock*, the Third Circuit reasoned that the defendant relinquished any expectation of privacy over the contents of the hard drive when he placed it in his girlfriend's laptop and permitted her full access to it without any password protection. *Id.* at 137. He thus assumed the risk that the girlfriend would consent to a search of the hard drive. *Id.*

**Scope of consent:** Where consent to search is given by an authorized person, a question still may arise as to the scope of that consent. As the Supreme Court has explained, "[t]he scope of a search is generally defined by its expressed object." *Florida v. Jimeno*, 500 U.S. 248, 251 (1991). In determining the scope of consent, courts apply a standard of "objective reasonableness—what would the typical reasonable person have understood by the exchange between the officer and the suspect?" *Id.*at 251.

As a general matter, the authority to access a given area may extend to individual items within that area, including digital devices. *See United States v. Suing*, 712 F.3d 1209 (8th Cir. 2013) (consent to search car included hard drive found in car); *United States v. Chappell*, No. 10CR531, 2011 WL 5352947, at *8 (N.D. Ga. Nov. 4, 2011) (general consent to search hotel room included search of computers, cell phones, and digital storage media). Where a defendant consents to a residential search and does not object to the seizure or accessing of computers located therein, courts generally construe the scope of consent to include digital devices located within the premises. *See, e.g.*, *United States v. Lucas*, 640 F.3d 168, 175–77 (6th Cir. 2011); *United States v. Lemmons*, 282 F.3d 920, 926 (7th Cir. 2002) (defendant's consent to search residence included computer he turned on after showing agents printed photographs). The same rule applies where a third person, such as a defendant's wife or girlfriend, grants consent to search a shared residence and has access to and control over computers found therein. *See, e.g.*,

*United States v. Politi*, No. IP 03-4-CR-1, 2003 WL 21078119, at *4 (S.D. Ind. May 1, 2003); *United States v. Smith*, 27 F. Supp. 2d 1111, 1115 (C.D. Ill. 1998) (girlfriend had actual and apparent authority to consent to search of residence that included computer located in open area of bedroom she shared with defendant, where children's games where found near the computer and defendant had attempted to teach girlfriend how to use the computer); *see also United States v. Mannion*, No. 02-4426, 2002 WL 31839377, at *3 (4th Cir. Dec. 19, 2002) (wife had access to computer and disk, was able to log on and access files, and evidence in vicinity suggested computer was used as family computer).

What happens when a suspect consents to a search of his computer for one type of evidence and searching officers locate another type of evidence? Courts generally deny suppression motions where the initial consent was objectively reasonable and the searching agent either reaffirms the consensual search upon locating evidence of a different crime or discontinues the search pending receipt of a search warrant for the newly discovered crime. Two good illustrations of this approach come from the Sixth and Eighth Circuits.

In *United States v. Lucas*, the Sixth Circuit upheld the denial of a motion to suppress child pornography found during a consensual search of a computer for evidence relating to narcotics. *Lucas*, 640 F.3d at 175–77. The defendant provided the officers with written consent to search his residence for "controlled substances, drug paraphernalia, and other material or records pertaining to narcotics." *Id.* at 177. During the search, an officer accessed a laptop and a thumb drive plugged into the laptop in the presence of the defendant, who did not object to the officer's actions. *Id.* In fact, the officer asked the defendant if the laptop was password protected, to which the non-objecting defendant responded in the negative. *Id.* at 177–78. The court noted that consent to search a residence does not necessarily equate to a "grant of broad authority to the police to open a suspect's non-secured computer and examine at will all the electronic files stored there." *Id.* at 178. Instead, there should be an objectively reasonable basis for concluding that the seizure and search of digital devices was within the scope of consent to search the residence. Under the facts in *Lucas*, the court easily concluded that the officer's initial search of the laptop and thumb drive for evidence pertaining to narcotics was consensual. *Id.*

The court went on to affirm the denial of the motion to suppress images of child pornography found on the devices during the consensual search for narcotics evidence. Upon discovering the images, the officer stopped searching the computer and thumb drive and obtained from the defendant a separate written consent form expressly authorizing the seizure and examination of the devices. *Id.* at 172. Before conducting a forensic examination of the devices, officers also obtained a warrant to search them for evidence of child pornography, just in case the defendant revoked his consent during the forensic examination process. *Id.* In upholding this approach, the court emphasized that there was "no evidence that [the officer] intentionally searched for child pornography and purposefully exceeded the scope of Lucas's consent to search for 'other material or records pertaining to narcotics.' " *Id.* at 179.

The Eighth Circuit reached a similar result in *United States v. Suing*, 712 F.3d 1209 (8th Cir. 2013). During a car stop, officers sought consent to search the defendant's vehicle for narcotics. The defendant signed a written consent form authorizing a search of the vehicle "to include luggage, containers and contents of all." *Id.* at 1210. The officers found an external hard drive in the front seat of the vehicle. Employing a review technique that should not be replicated for forensic reasons, the officers plugged the drive into a computer and began a manual search of the drive's contents. Almost immediately, the officers saw thumbnails of child pornography. They discontinued the search, pending receipt of a warrant authorizing a search for evidence of child pornography. *Id.* at 1211.

The Eighth Circuit rejected the defendant's argument that the child pornography evidence should be suppressed because the officers exceeded the scope of his consent to search the vehicle and the hard drive for narcotics evidence. *Id.* at 1212–13. The court concluded that the officers did not exceed the scope of consent, because they "did not abandon [the] drug search and continue a new, extended search for child pornography without judicial authority." *Id.* at 1212 (citing *United States v. Hudspeth*, 459 F.3d

922, 925–28, *rev'd in part on other grounds*, 518 F.3d 954 (8th Cir. 2008) (en banc)). Instead, they stopped and got a warrant covering child pornography crimes.

Courts have reached the opposite conclusion and suppressed evidence where the scope of a search was expanded to subjects beyond those consented to by the defendant. *See, e.g.*, *United States v. Parson*, 599 F. Supp. 2d 592, 611–12 (W.D. Pa. 2009) (suppression of child pornography ordered where defendant's written consent to search computer was invalid because agent led defendant to believe he was victim of identity theft); *United States v. Richardson*, 583 F. Supp. 2d 694, 724–25 (W.D. Pa. 2008) (similar). In *Parson* and *Richardson*, consent had been obtained solely on the basis of a factual misrepresentation as to whether the defendants were targets—as opposed to victims—of criminal conduct.

Another question concerns whether the scope of consent can be limited to certain files or portions of data contained on a hard drive. In *Stabile*, the Third Circuit rejected a Fourth Amendment challenge to the seizure of six hard drives with the consent of the defendant's putative wife. *Stabile*, 633 F.3d at 232–33. The court noted that a person may choose not to "relinquish[] his privacy in some files on a computer or in a subset of information," in which case "a third party would have no authority to consent to the search or seizure of [those files or subsets of information]." *Id.* Important factors in determining the scope of consent as to segregated data on a hard drive include the identity of the users, the circumstances of their use of the drive, and whether particular files have been password-protected or encrypted. *See id.*; *see also Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001) (defendant had not assumed risk that co-user of computer would consent to warrantless search of password-protected files). The consensual search was lawful, the court concluded, because Stabile had not password-protected his files on the shared drives.

Other circuits have reached the same conclusion in unpublished decisions, holding that certain portions of a hard drive may be protected against a third party's consent to a warrantless search. *See, e.g.*, *United States v. Trejo*, No. 10-2188, 2012 WL 975063, at *4 (6th Cir. Mar. 22, 2012) (defendant's parents had apparent authority to consent to search of files stored under defendant's personal profile, which was not password-protected, on family computer). In addition, the Eleventh Circuit has rejected a defense argument that a defendant's having password-protected certain files on a hard drive would invalidate the provision of consent by his girlfriend to search other, unprotected files on the drive to which she had access. *United States v. Hyatt*, No. 09-15285, 2010 WL 2490913, at *6 (11th Cir. June 18, 2010).

## II. Consensual searches of residences, cars, and personal devices

Whether a third person has authority to consent to the search of digital devices located within a residence or car is based on the totality of the circumstances. Important factors include joint use of the device, the presence or absence of a password permitting access to the device, and the location of the device within the residence or car. *See, e.g.*, *Stabile*, 633 F.3d at 232–33; *United States v. Aaron*, No. 00-6383, 2002 WL 511557, at *4 (6th Cir. Apr. 3, 2002) (defendant "did not protect his computer with a password or otherwise manifest an intention to restrict [his girlfriend's] access"); *United States v. Mitchell*, No. 3:11-CR-248, 2013 WL 3808152, at *29–30 (M.D. Fla. July 22, 2013) (owner and possessor of iPhones and iPads found in defendant's car had at least apparent authority to consent to warrantless search); *United States v. Politi*, No. IP 03-4-CR-1, 2003 WL 21078119, at *4 n.4 (S.D. Ind. May 1, 2003) (upholding consent search absent password on computer); *United States v. Smith*, 27 F. Supp. 2d 1111, 1113–14 (C.D. Ill. 1998) (denying suppression motion because computer was not password protected). *But see Trulock*, 275 F.3d at 403 (consent search invalid because defendant had reasonable expectation of privacy in password-protected files).

"As a general matter, one spouse has the authority to consent to a search of a premises jointly occupied by both spouses." *United States v. Duran*, 957 F.2d 499, 503 (7th Cir. 1992) (wife could consent to search of separate building to which she had access, but chose not to enter); *see also United States v.*

*Powers*, No 10-1206, 2011 WL 3805719, at *2 (2d Cir. Aug. 30, 2011); *United States v. Rowe*, No. CR-11-07-M, 2011 WL 2532407, at *3 (D. Mont. June 24, 2011) (wife had apparent authority to consent to search of computer located in common area of home to which she had full access); *United States v. Pollaro*, 733 F. Supp. 2d 364 (E.D.N.Y. 2010) (no suppression where wife consented to search of computers in dining room and office of home and present defendant did not object). The inquiry turns not on actual use of an area, but rather on the authority to access an area, regardless of whether that authority is exercised. *See, e.g.*, *Smith*, 27 F. Supp. 2d at 1115 (citing *Duran*, 957 F.2d at 505).

The Ninth Circuit recently upheld the consensual search of a computer provided to law enforcement agents by a defendant's estranged wife. *United States v. Tosti*, 733 F.3d 816 (9th Cir. 2013). Mr. Tosti's legal troubles began after a CompUSA computer technician discovered images of child pornography on a computer Mr. Tosti dropped off for service. *Id.* at 818–19. The technician alerted the police, who viewed only those images that the technician had viewed. A few days after Mr. Tosti's arrest, Mrs. Tosti signed a written consent form and gave the FBI documents, a computer, and several external hard drives and DVDs that she reported contained pornography. The Ninth Circuit held that Mrs. Tosti had apparent, if not actual, authority to consent to the search of this digital equipment. *Id.* at 823. The couple were married and had resided at their shared residence for over 20 years. Both the defendant and his wife used the computer and storage devices, none of which were password protected or encrypted. *Id.* Thus, the searching officers reasonably believed that she had authority to consent to the search of this equipment. *Id.*; *see also United States v. Klutter*, 674 F.3d 980, 984–85 (8th Cir. 2012) (father had apparent authority to consent to seizure of adult son's computers found in common areas and son's room in shared residence); *Stabile*, 633 F.3d at 232 (authority to consent to a search of computer derives "from 'mutual use of the property by persons generally having joint access or control for most purposes' ") (quoting *Matlock*, 415 U.S. at 171 n.7).

These concepts apply equally to smaller pieces of digital media. Apparent authority to consent to a search of loose digital media, such as a thumb drive, may exist where the drive is found in a room or furniture shared by defendants, one of whom consented to the search and seizure. *See United States v. Marchante*, Nos. 11-11906, 11-12568, 11-12441, 2013 WL 1223477, at *2 (11th Cir. Mar. 26, 2013). In this access device fraud and identity theft case, one defendant consented to the seizure of a thumb drive found in a nightstand she shared with a male defendant. Regardless of whether she ever actually used it, the court reasoned that the consenting female defendant had access to the thumb drive, which was not encrypted or otherwise "locked." *Id.*

## III. Consensual searches of employer-owned devices and networks

Evidence, fruits, and instrumentalities of crimes often exist on employer-provided devices and in employer-owned computer networks. The employee-users of these devices and networks may be criminal suspects, victims, or witnesses. The rules governing consent searches of such devices and networks can vary depending on the status of the employer and, in particular, on whether and to what extent an individual has a reasonable expectation of privacy in the device or network to be searched.

Private-sector employers have broad authority to consent to searches of their computer equipment and network. *See, e.g.*, *United States v. Ziegler*, 474 F.3d 1184, 1191 (9th Cir. 2007) (employer could consent to search of computer it provided to employee even if employee has stored personal information on it); *United States v. Williams*, No. 12-310, 2013 WL 2318144, at *17–19 (D. Minn. May 28, 2013) (employer could consent to search of employee's computer equipment and network files).

The issue is more complex as to public-sector employers. In general, public-employer searches of an employee's work-related areas and effects are governed by the "special needs" framework adopted in *O'Connor v. Ortega*, 480 U.S. 709 (1987). Under that test, a government employee may have a reasonable expectation of privacy in his workplace, and thus, in his workplace computer and network space. Employers nonetheless can conduct warrantless searches of such if the search is work-related,

justified at inception, and permissible in scope. *See id.* at 725–26. Should they find evidence of crime while doing so, they generally may provide that evidence to law enforcement agencies under a consent theory. *See, e.g.*, *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000).

Although it does not directly address the consent exception, the Supreme Court's decision in *City of Ontario, Calif. v. Quon*, 130 S. Ct. 2619 (2010), provides helpful guidance concerning public-employer searches of devices and networks used by employees. *Quon* presented a § 1983 challenge to a city police department's warrantless search of an officer's text messages sent via a city-provided pager. Prior to providing the pagers to SWAT officers it employed, the police department announced a "Computer Usage, Internet and E-Mail Policy" that specified that the department "reserves the right to monitor and log all network activity including email and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources." *Id*. at 2625. The department informed the officers that the policy applied to all usage of the pagers even though text messages via the pagers would be routed through the computer network of the service provider, not the police department. *Id.* The department obtained, from the service provider, text messages sent and received by Quon during his working hours after he repeatedly exceeded the text message limit. *Id.* at 2625–26. Most of the messages were non-work-related, and some were sexually explicit.

After he was disciplined for misuse of the pager, Quon sued the department, the city, and the text message service provider alleging violations of the Fourth Amendment and the Stored Communications Act (SCA). *Id.* at 2626. The district court granted summary judgment for the text message service provider under the SCA, and denied summary judgment to the public defendants after concluding that Quon had a reasonable expectation of privacy in the text messages he sent and received via the department-provided pager. *Id.* Following a trial focused on the department's search of the pager, the district court held that the department did not violate Quon's Fourth Amendment rights because its search of the text messages was reasonable in light of its employment-related objective of determining if the text messaging limit was too low. *Id.* at 2626–27. The Ninth Circuit reversed in part, agreeing that Quon had a reasonable expectation of privacy in the text messages, but concluding that the department's search of the messages was not reasonable, and therefore violated the Fourth Amendment. *Id.* at 2627. The Ninth Circuit also reversed the district court's grant of summary judgment for the service provider after concluding that the provider had violated the SCA by consensually providing text messages stored on its network to the department without a warrant. *Quon v. City of Ontario, Calif.*, 529 F.3d 892, 910–11 (9th Cir. 2008). The Supreme Court granted the public defendants' petition for certiorari on the Fourth Amendment issue, but denied the service provider's petition on the SCA issue.

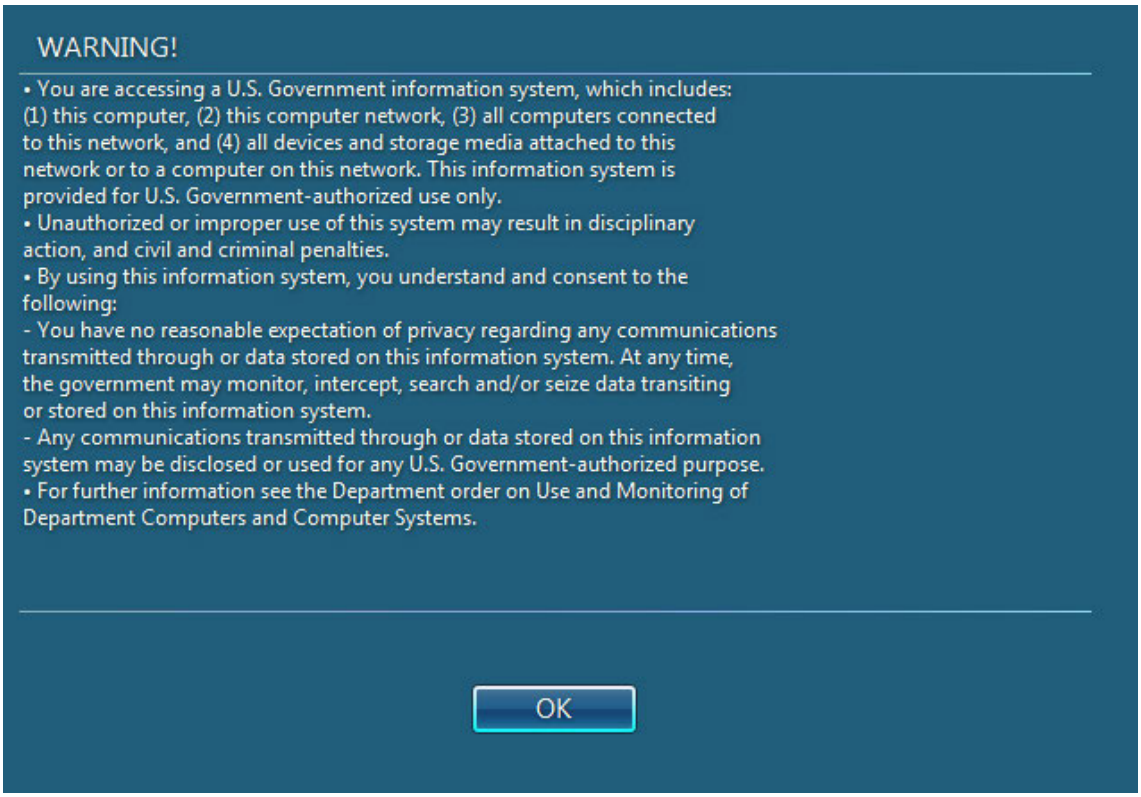
The Supreme Court assumed that the employee had a reasonable expectation of privacy in communications via the employer-provided pager, but held that the department's search of the text messages was reasonable. *Quon*, 130 S. Ct. at 2630–33. Even if such a privacy interest exists in employer-provided digital communications devices, the Court explained, warrantless searches of those devices by the employer for a " 'non-investigatory work related purpose or for the investigation of work related misconduct' is reasonable if it is 'justified at its inception' and if the 'measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of' the circumstances giving rise to the search." *Id.* at 2630 (quoting *O'Connor*, 480 U.S. at 725–26). This was so here, because the department reviewed the text messages not to search for evidence of misconduct, but to determine if the city's limit on text messaging was cost effective—a "noninvestigatory work-related purpose." *Id.* at 2631. Moreover, reviewing only a limited portion of messages transmitted while the officer was working was not "excessively intrusive." *Id.*

What ultimately may be more important are the Court's statements about employee expectations of privacy in the contents of digital data contained or transmitted via employer-provided digital devices or networks. *Id.* at 2629–32. The Court explained that "[p]rudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and the extent, of privacy expectations enjoyed by employees when using employer-provided communications devices." *Id.* at 2629.

"Many employers," the Court noted, "expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency." *Id.* In addition, "some States have recently passed statutes requiring employers to notify employees when monitoring their electronic communications." *Id.* at 2630 (citing Del. Code Ann., Tit. 19, § 705 (2005); Conn. Gen. Stat. Ann. § 31-48d (West 2003)). In what is likely to be an oft-quoted line, the Court stated that "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated." *Id.*

Future cases may find that both public and private employees have a diminished or no reasonable expectation of privacy in an employer-provided device or network account. This may prove particularly so where the employer explicitly retains the right to monitor the employee's use of the device or network. *See, e.g.*, *Zeigler*, 474 F.3d at 1191; *United States v. Thorn*, 375 F.3d 679, 683 (8th Cir. 2004); *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002); *Williams*, 2013 WL 2318144, at *19; *United States v. Bailey*, 272 F. Supp. 2d 822, 835–36 (D. Neb. 2003).

Computer banners and written usage policies serve as the primary means of notification and acknowledgement of limitations on expectations of privacy in work-related devices and networks. A good example of such a computer usage "banner" is the one that Department of Justice (DOJ) employees see and acknowledge before each log-in to the DOJ computer network:




Even if they do not entirely eliminate any reasonable expectation of privacy the employee may have in the device or computer network, such policies and banners make clear that the employer has retained actual authority to conduct a warrantless search of its devices or networks, and to provide any relevant information concerning crimes to law enforcement agents on a consensual basis. *See, e.g.*, *Thorn*, 375 F.3d at 683 (computer use policy eliminated employee's reasonable expectation of privacy in workplace computer); *United States v. Angevine*, 281 F.3d 1130, 1134–35 (10th Cir. 2002) (banner and computer usage policy eliminated any reasonable expectation of privacy employee had in data downloaded to government workplace computer over government computer network).

The Fourth Circuit's decision in *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000), is illustrative. In that case, the Fourth Circuit held that a CIA employee had no reasonable expectation of privacy in his work computer under agency's computer usage policy. That policy provided that CIA employees could access the Internet "for official government business only;" that accessing "unlawful material was specifically prohibited;" and that the CIA would "periodically audit, inspect, and/or monitor the user's Internet access as deemed appropriate." *Id.* at 395–96. Simons challenged remote warrantless searches of his work computer and the warrantless replacement of his hard drive following the discovery of images of child pornography. Because Simons had no reasonable expectation of privacy in the work computer or in his Internet activity through the CIA's computer network, the CIA could consensually provide the hard drive and records of Internet activity to law enforcement agents. *Id.*at 398.

Under the DOJ banner above, one court has held that users of DOJ devices have expressly consented to the warrantless monitoring of their activity on the device and network and to the provision of data relating to such to law enforcement agencies. *United States v. Linder*, No. 12-CR-22-1, 2012 WL 3264924, at *12 (N.D. Ill. Aug. 9, 2012). In *Linder*, a Deputy U.S. Marshal indicted for civil rights crimes challenged the Office of Inspector General's warrantless search of his DOJ-issued Blackberry and files stored on the DOJ network. The district court denied the defendant's suppression motion based on the DOJ computer usage policy and the banner quoted above, which appeared each time the defendant logged on to his government-issued computer or Blackberry. *See id.* at *4–5. The court also noted that the defendant was required to complete "Computer Security Awareness Training" each year, which reminded him that he had no reasonable expectation of privacy in his use of the DOJ computer equipment. *Id.* at *5. That the defendant chose to place personal photographs and other files on the DOJ computer network did not create an objectively reasonable expectation of privacy in those files. *Id.* at *8. Even if the defendant had a reasonable expectation of privacy in the contents of his DOJ-issued Blackberry and network files, the court continued, he expressly consented to the warrantless search of those devices and the data stored on them under the DOJ computer usage policy and log-on banner. *Id.* at *12.

The same rationale has been followed in the private employer context. *See Williams*, 2013 WL 2318144, at *17–19. Williams came under investigation for purchasing access to commercial child pornography Web sites. During a residential search and interview, Williams admitted accessing the Web sites from his home and work-issued laptop, which connected to his employer-owned network. Agents went to Williams' employer's office with a search warrant, but also obtained written consent to search and seize Williams' office computer and files from the employer's computer network. *Id.* at *5–6.

The district court denied Williams' motion to suppress the computer equipment and network data that his employer consensually provided to law enforcement agents. *Id.* at *17–19. Assuming that Williams may have had some reasonable expectation of privacy in the contents of the computer and network files, the court stated that "employer policies concerning communications 'shape the reasonable expectations of employees, especially to the extent that such policies are communicated.' " *Id.* at *17 (quoting *Quon*, 130 S. Ct. at 2630). Williams' employer "made it clear that the company had 'the right to view electronic mail, server and computer files or sites accessed via the Internet at any time, with our without reason, and examine the contents.' " *Id.* The policy, which Williams acknowledged by signature when he received his office computer equipment and network access, further prohibited the use of the computer equipment and network "to create, access or download any offensive or disruptive materials, including any materials which contain sexual implications [or] pornographic substance." *Id.* The court concluded that this policy authorized Williams' employer to monitor employee use of its devices and network and further authorized the employer to consent to a law enforcement search of such devices and network files. *Id.* at *18–19.

In decisions that may come to bear as BYOD ("bring your own device") policies and practices become more common, at least two courts have held that an employee may forfeit a reasonable expectation of privacy in a personal device that he uses for work-related purposes. In *United States v. Barrows*, 481 F.3d 1246 (10th Cir. 2007), the Tenth Circuit held that a government employee forfeited

any reasonable expectation of privacy in his personal computer that he brought to his office for work-related use. The court articulated factors that are important to evaluating whether the employee had a subjective and objective expectation of privacy in his personal device once he brought it to the office and connected to the office network. These factors include the employee's relationship to the device (ownership, etc.), whether the device was within the employee's immediate control when seized, and whether the employee attempted to maintain his privacy in the device while having it in the office. *Id.* at 1248. Barrows lacked an objectively reasonable expectation of privacy because he connected his personal computer to the city's network for file sharing, kept the computer turned on at all times, and failed to password protect or take any other steps to prevent third-party use of the computer, which was left in a public area. *See id.* at 1248–49; *see also United States v. Rankins*, No. ARMY 20100494, 2012 WL 5077656, at *1–2 (Army Ct. Crim. App. Oct. 16, 2012) (soldier who brought personal laptop to Forward Operating Base in Iraq and left it running in plain view had no objectively reasonable expectation of privacy in contents).

## IV. Consensual assumption of online identities

Criminal suspects, victims, or witnesses may have multiple computer network accounts that contain evidence, fruits, or instrumentalities of crimes. In addition to the employment-related accounts and devices discussed above, individuals almost certainly will have personal accounts with electronic communications and remote computing service providers that may contain relevant information. In certain online undercover situations, agents may wish to seek the consent of an account holder to assume control over the account and any related online identity.

As a threshold matter, it is important to distinguish between seeking consent from an account holder and from a network administrator or owner. An individual's reasonable expectation of privacy in personal online accounts is subject to both constitutional and statutory limitations that strictly curtail a *service administrator or network owner's* authority to consent to a governmental search of such accounts. *See, e.g.*, 18 U.S.C. §§ 2701–2712 (2013) (Stored Communications Act); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (email); *see also* Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Ch. 3 (Aug. 2009).

An individual who owns or legitimately controls and uses a personal online account may consent to the use of that account and the assumption of any related online identity by a law enforcement agent. *See, e.g.*, *United States v. Meek*, 366 F.3d 705, 711–12 (9th Cir. 2004); *United States v. Sawyer*, 786 F. Supp. 2d 1352, 1357 (N.D. Ohio 2011). Moreover, individuals generally have no objectively reasonable expectation of privacy in files or other electronic data that they knowingly and voluntarily share with third persons. *See, e.g.*, *Chaney v. Fayette Cnty. Pub. Sch. Dist.*, No. 3:13-cv-89-TCB, 2013 WL 5486829, at *4–5 (N.D. Ga. Sept. 30, 2013) (plaintiff surrendered reasonable expectation of privacy in photograph posted on her "semi-private" Facebook profile, viewable by "friends and friends of friends"); *United States v. Bode*, No. ELH-12-158, 2013 WL 4501303, at *20–21 (D. Md. Aug. 21, 2013) (no reasonable expectation of privacy in chat logs conducted with social networking Web site where banners notified users that unlawful activity would be reported to law enforcement); *United States v. Brooks*, No. 12-CR-166, 2012 WL 6562947, at * 2–3 (E.D.N.Y. Dec. 17, 2012) (no reasonable expectation of privacy in files shared through peer-to-peer network); *United States v. Soderholm*, No. 4:11-CR-3050, 2011 WL 5444053, at *6–7 (D. Neb. Nov. 9, 2011) (same). Instead, they assume the risk that the third person may consensually share their files or data with law enforcement agents. *See, e.g.*, *United States v. Ladeau*, No. 09-40021, 2010 WL 1427523, at *4–5 (D. Mass. Apr. 7, 2010). Thus, the target who communicates with a person whose online identity has been assumed by law enforcement, or who sends or receives data to/from the account of such person, is unlikely to succeed in challenging the use of such on Fourth Amendment grounds.

*United States v. Meek*, 366 F.3d 705, provides a good example of the "assumed online identity"

principle. In *Meek*, police officers identified and located a minor boy whose sexually explicit photographs were found online. With his father's consent, the minor provided one of the officers with authorization to assume his AOL identity and to take over control of the minor's AOL account. *Id.* at 709. The officer then began to communicate online with Meek, who appeared to have prior online contact about sexual encounters with the boy. Meek eventually was arrested after he arranged to meet "the boy" for sexual purposes. *Id.* at 710–11.

Meek moved to suppress a subsequent search of his AOL account, arguing that the officers violated his Fourth Amendment rights by monitoring his online communications with "the minor" without judicial authorization. The Ninth Circuit affirmed the district court's denial of Meek's suppression motion, concluding that "[l]ike private telephone conversations, either party to a chat room exchange has the power to surrender each other's privacy interest to a third party." *Id.* at 711 (citing *United States v. Karo*, 468 U.S. 705, 726 (1984)). The court characterized it as "a reality of the Internet that a person initiating an Internet-based conversation does not control [the recipient's subsequent use or disclosure of that conversation]." *Id.* (citing *Katz v. United States*, 389 U.S. 347 (1967)).

The same principle applies where a target has authorized a third person to access certain files via peer-to-peer networks. Even though such targets may have a subjective expectation of privacy in these accounts, they have no objectively reasonable expectation of such as to files or data they share with either third parties or the public at large. In *United States v. Sawyer*, 786 F. Supp. 2d 1352 (N.D. Ohio 2011), the defendant created a "closed" peer-to-peer network through which he shared specific files only with certain computer users he had "invited" into his "closed" network. During transit, the files were encrypted. One of the users the defendant had invited into his "closed" network authorized a law enforcement agent to assume his online identity on that network. By doing so, the agent was able to view and download the files that the defendant chose to share with his network "friends." *Id.* at 1354–55.

After being charged with distribution of child pornography, the defendant moved to suppress the files downloaded from his computer by the undercover agent, as well as all evidence subsequently seized during the investigation. The district court denied the motion after finding that the defendant had no objectively reasonable expectation of privacy in the files he made available to others via the "closed" peer-to-peer network. *Id.* at 1355–56; *see also Ladeau*, 2010 WL 1427523, at *1–5. Once he voluntarily shared these files with even a limited number of third persons, the defendant "bore the risk that those 'friends' might turn the files over to law enforcement." *Id.* at 1356; *see also Ladeau*, 2010 WL 1427523, at *4 ("No matter how strictly Ladeau controlled who accessed his computer files, he had no control over what those people did with information about the files once he granted them access."). Even if such a privacy interest existed, though, the court ruled that both the defendant and the user who consented to the assumption of his online identity authorized the agent to access the files contained in the defendant's "closed" network. *Sawyer*, 786 F. Supp. 2d at 1356–57. Because this third party had "authority or control over the property subject to [the] search" (that is, the defendant's "shared" folder(s) on the "closed network"), that third party could voluntarily consent to the use of his identity to access those files. *Id.* at 1357; *see also Brooks*, 2012 WL 6562947, at *2–3; *Soderholm*, 2011 WL 5444053, at *6–7. The same is true of file sharing on public networks. *See, e.g.*, *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009); *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008).

Courts have likewise rejected Fourth Amendment challenges to peer-to-peer undercover operations based on the *Jones* trespass theory. *See, e.g.*, *United States v. Brashear*, No. 4:11CR62, 2013 WL 6065326, at *3 (M.D. Pa. Nov. 18, 2013) (no trespass into defendant's computer by search of shared files via public peer-to-peer network); *Russell v. United States*, No. 4:11CV1104, 2013 WL 5651358, at *7 (E.D. Mo. Oct. 16, 2013) (same); *Brooks*, 2012 WL 6562947, at *5 (E.D.N.Y. Dec. 17, 2012) (same as to "closed" network); *United States v. Nolan*, Crim. A. No. 11-82, 2012 WL 1192183, at *10–11 (E.D. Mo. Mar. 6, 2012) (similar). In these cases, undercover agents assumed the identities of person's previously "invited" into semi-private or "closed" networks, or posed as an individual interested in obtaining contraband via a public network. In each scenario, the courts found that no trespass occurred, so

as to invoke the *Jones* rationale.

In *Brooks*, for instance, the district court reasoned that an agent who had consensually assumed a "friend's" online identity to download child pornography from the defendant's "closed" peer-to-peer network did not make "any physical intrusion on a constitutionally protected area." *Brooks*, 2012 WL 6562947, at *5. The agent "did not install any device or software on Brooks' computer to enable monitoring or tracking, did not physically enter Brooks' home, and did not physically access his computer." *Id.* (citing *Jones*, 132 S. Ct. at 950). Moreover, the agent's remote accessing of the defendant's files via the "closed" network occurred only after Brooks had consented to such access by a person who, in turn, consensually provided his online identity to the agent. The agent also accessed only those files to which Brooks had provided access to the person whose online identity had been consensually assumed. The court therefore concluded that the *Jones* trespass theory did not apply "because this situation involves 'merely the transmission of electronic signals without trespass.' " *Id.* (quoting *Jones*, 132 S. Ct. at 952–53).

## V. Conclusion

The daily investigation of many crimes has taken on a cyber-component. Digital devices and computer networks used by suspects, victims, and witnesses often hold some of the best evidence of a crime. The circumstances of digital investigations are often dynamic and quickly evolving, and the risk of loss of digital evidence is substantial. Consensual searches of devices and data from networks is therefore common and critically important in many cases. It is therefore essential that prosecutors and investigators understand the key principles concerning authority to, and scope of, consent to searches of devices and networks. Both authority and scope must be defined under the totality of the circumstances in which the search occurs. Many cyber-investigations also involve the assumption of a person's online identity. This person may be a victim, cooperator, or witness. Just as a person may consent to a search of their device, they also may consent to the use of their online identity and a search of their online accounts. Those who interact with those identities or accounts assume the risk of this consent.

## VI. Addendum: sample go-by consent forms

### A. Sample go-by providing consent to search computer/electronic equipment

**CONSENT TO SEARCH COMPUTER/ ELECTRONIC EQUIPMENT**

I, _____, have been asked to give my consent to a search. I have also been informed of my right to refuse to consent to such a search.

I hereby authorize _____ and any other person(s) designated by [insert Agency/Department] to search:

(check as many as apply)

- □ The premises at street address _____, and any storage media or other computer/electronic equipment located therein, including internal hard disk drive(s), floppy diskettes, compact disks, scanners, printers, other computer/ electronic hardware or software and related manuals; any other electronic storage devices, including but not limited to, personal digital assistants, cellular telephones, and electronic pagers; and any other media or materials necessary to assist in accessing the stored electronic data.
- □ The following storage media or electronic devices:

---

Description of computer, data storage device, cellular telephone, or other device (make, model and serial number, if available)

---

I consent that search may be for any purpose, and that the search may include the examination of computer data and the use of forensic review techniques. I consent to the search occurring at any time, for any length of time, and at any location.

If any of the devices described above are protected with a password and/or encrypted, I consent to the use of my passwords and/or encryption keys to access the data. The password(s) and/or encryption keys are: _____.

I certify that I have a right to access or use these devices and all information found in them. I understand that any contraband or evidence on these devices may be used against me in a court of law.

I relinquish any constitutional right to privacy in these electronic devices and any information stored on them. I authorize [insert Agency/Department] to make and keep a copy of any information stored on these devices. I understand that any such copy will not be my property and that I will have no privacy or possessory interest in the copy.

This written permission is given by me voluntarily. I have not been threatened, placed under duress, or promised anything in exchange for my consent. I have read this form, or it has been read to me, and I understand it. I understand the [English] language and have been able to communicate with the agents/officers.

I understand that I have the right to withdraw my consent to the [agency's] search of my original physical storage media or electronic devices. I understand that I may ask for a receipt for all things turned over.

Signature _____ Date and time _____

Name (printed) _____

Signature of Witnesses: _____

_____

**B. Sample go-by providing consent to assume online presence**

**CONSENT TO ASSUME ONLINE IDENITY**

I, _____, hereby voluntarily provide consent to the United States to take over control of and use my "online presence." This online presence includes the following screen name(s), nickname(s), account(s), Web site(s), and/or e-mail address(es) as well as the password(s) associated with these account(s):

| Account Name | Password |
|---|---|
| | |
| | |
| | |
| | |

My online presence may be used by the United States for any official purpose, including (but not limited to) sending and receiving e-mail, instant messages, or any other sort of communication; accessing stored communications or information; changing account settings; conducting any other activities related to the above account(s); and using or disclosing any information related to these account(s).

I understand that the United States may change the password(s) to these account(s) so that I will no longer have access. I understand and acknowledge that by signing the consent form, I relinquish all present and future claims to the use of these account(s).

I give this consent freely and voluntarily, without fear, threats, or coercion. Moreover, I have not received any promise or representation of any kind concerning what sentence I may receive for any criminal violations that I may have committed. I have been advised of my right to refuse to allow the assumption of my online presence, and I hereby voluntarily waive this right.

Signature: _____ Witness: _____
Name (printed): _____ Name (printed): _____
Date: _____ ❖

**ABOUT THE AUTHOR**

❑**Edward J. McAndrew** is an Assistant United States Attorney in the District of Delaware, where he focuses on Internet-based and technology facilitated crimes. He previously served in the Cyber Crime Unit of the Eastern District of Virginia and in the Criminal Division's Child Exploitation and Obscenity Section. Prior to joining the Department in 2006, he was a litigation partner at Reed Smith LLP, in Washington, D.C. ✠

# Seizing and Operating Criminal Computer Networks

*Edward Chang*
*Assistant United States Attorney*
*District of Connecticut*

Recent cases demonstrate that it may be inadequate to simply seize and disable computers and computer networks used by cyber criminals because of potential adverse consequences to innocent victims. In the "Rove Digital" prosecution, for example, cyber criminals infected over four million computers with malicious software that re-routed the victims' Internet browsers through computer servers controlled by the criminals. A simple takedown of those servers would have prevented millions of innocent victims from being able to browse the Internet.

As a result, prosecutors have begun seeking judicial authorization—not to seize and disable criminal computer networks (takedown), but to seize and continue operating those networks, appropriately modified (takeover)—in order to protect crime victims and advance other significant law-enforcement objectives. To do so, prosecutors have appealed to district courts' powers in equity, either to impose a receivership, as in Rove Digital, or to issue an injunction, as in the takeover of the Coreflood "botnet." This article describes the legal framework on which those cases relied and sets forth some of the prudential considerations that may arise when government prosecutors seize and continue to operate a criminal computer network.

## I. The traditional takedown model

Before describing a takeover, it will help first to describe a traditional takedown of a criminal computer network. Criminal computer networks take many different forms, ranging from a "bulletin board," which may consist of a single, centralized server used by criminals to share contraband or instrumentalities of crime, to a "botnet," consisting of multiple, hierarchical computer servers used by criminals to control and exploit thousands or millions of compromised computers. A takedown, broadly speaking, focuses on seizing or disabling enough of the assets of a criminal computer network to render it inoperable.

Depending on the specific network in question, those assets typically include:

- Computer servers
- Internet domain names, such as "whitehouse.gov"
- IP addresses, such as 192.0.0.1

Tangible assets in the United States, such as computer servers, are typically seized using a Rule 41 search warrant or a forfeiture seizure warrant. *See generally* Office of Legal Education, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Ch. 2 (2009). One advantage of using a forfeiture warrant rather than a Rule 41 warrant is that a forfeiture warrant need not be issued in the district where the computer server is located, which can simplify matters considerably if there are multiple computer servers around the country to be seized. *See* 21 U.S.C. § 853(j) (2013). Finally, it is often the case that a compromised computer, owned by a legitimate entity, is used as part of a criminal computer network. In that case, it may be possible to obtain or disable the computer server by consent of the legitimate owner.

Tangible assets outside the United States are more difficult to address. The preferred approach is to work with the Office of International Affairs and the legal attachés of the investigating agencies to obtain the assistance of foreign authorities in seizing the foreign assets. If the assistance of foreign authorities is not forthcoming, however, the investigating agents must determine whether the foreign assets really need to be seized in order to execute a successful takedown. For example, it may be possible to execute a takedown by isolating the foreign assets from the rest of the criminal computer network or to execute only a partial takedown of the network. Unfortunately, some criminal computer networks are sufficiently resilient that they cannot be taken down at all without assistance from foreign authorities.

Intangible assets, such as Internet domain names and IP addresses, are typically seized using a forfeiture seizure warrant or a forfeiture restraining order under 21 U.S.C. § 853(e). It is not always easy, however, to identify the entity on whom the warrant or order should be served. With respect to an IP address, which is assigned by a regional Internet registry (RIR) to an Internet service provider (ISP), *see generally Regional Internet Registry*, WIKIPEDIA, http://en.wikipedia.org/wiki/Regional_internet_registry, the warrant or order should be served on both the RIR and the ISP. Because an IP address can be sold or sub-leased, it may also be prudent to serve more than one Internet service provider in order to ensure that the IP address is not inadvertently reassigned and seized back by the criminals. Likewise, an Internet domain name must be registered by a commercial domain name "registrar," recorded on an Internet domain "registry," and associated with an IP address by a DNS (domain name system) service provider. *See generally Domain Name Registrar*, WIKIPEDIA, http://en.wikipedia.org/wiki/Domain_name_registrar. Therefore, to effectuate the seizure of a domain name, the warrant or restraining order should be served on the registrar, the registry, and the DNS service provider.

The warrant or order should instruct the appropriate entities to lock the accounts associated with the seized IP address or domain name to prevent any changes to the accounts unless authorized in writing by the prosecutors or investigating agents. Also, if the computer associated with the seized IP address or domain was previously accessible on the Internet (as opposed to a hidden or otherwise inaccessible part of the criminal computer network), it may be appropriate for the warrant or order to direct the service providers to route Internet traffic addressed to the seized IP address or domain to a computer server that is controlled by the investigating agency, in order to display a banner providing public notice of the seizure.

Before using a forfeiture warrant or restraining order, however, it is necessary to establish statutory authority for the forfeiture. Not all criminal violations are associated with forfeiture provisions and not all forfeiture provisions permit the forfeiture of instrumentalities of crime. *See, e.g.*, 18 U.S.C. § 982(a)(2) (2013) (authorizing only forfeiture of proceeds from mail, wire, and bank fraud and other offenses). Of course, a forfeiture provision that only permits forfeiture of proceeds will suffice if there is probable cause to believe that the assets to be forfeited are traceable to the proceeds. Fortunately, most cybercrimes are associated with forfeiture provisions that permit the seizure of instrumentalities such as IP addresses and domain names. *See, e.g.*, 18 U.S.C. §§ 1029(c)(1)(C) (access device fraud), 1030(i) and (j) (computer intrusion), 1037(c) (spamming), 2253 (child exploitation), 2323 (2013) (copyright and trademark infringement); *see also* 18 U.S.C. § 2513 (2013) and 28 U.S.C. § 2461(c) (2013) (violating the Wiretap Act).

The recent takedown of "Megaupload.com," though unusually complex, is an example of a traditional takedown. As alleged in the indictment, the defendants used the site to engage in criminal copyright infringement and money laundering on a massive scale. *See United States v. Kim Dotcom et al.*, No. 1:12 Cr. 3 (LO) (E.D. Va. filed Jan. 5, 2012).

To execute the takedown, the prosecutors used criminal forfeiture warrants to seize 18 Internet domain names. The forfeiture warrants authorized the Government to post an online banner that notified users of Megaupload.com that the site had been seized and that criminal charges had been filed. The prosecutors also obtained Rule 41 warrants to image portions of the 1,103 computer servers operated by the defendants at an ISP in Virginia. Finally, the prosecutors took steps to freeze the defendants' financial

assets around the world and worked with foreign law enforcement agencies to execute arrest warrants and search warrants overseas. Notably, the takedown was successful even though the Government did not actually seize all of the computer servers used by Megaupload.com.

## II. A takeover using criminal authorities: Rove Digital

Rove Digital presents a perfect example where the traditional takedown model is inadequate. In Rove Digital, the defendants allegedly infected over four million computers around the world with malicious software that re-routed the Internet traffic of the victims' computers through computer servers controlled by the defendants. *See United States v. Vladimir Tsastsin et al.*, No. 1:11 Cr. 878 (LAK) (S.D.N.Y. filed Nov. 9, 2011). As a result, a takedown of those computer servers would have effectively prevented millions of innocent victims from accessing the Internet.

Specifically, the malicious software used by the defendants modified the victims' computers to use the wrong DNS servers, which are the computer servers used to translate Internet domain names into IP addresses. By modifying the victims' computers to use the rogue DNS servers controlled by the defendants, the defendants were able to selectively re-route Internet traffic from the victims' computers. In particular, the defendants re-routed the victims' Internet browsing activity (that is, clicks) to unwanted online advertisements, for which the defendants received payment from third parties—a type of fraud known as "click hijacking."

The criminal computer network in Rove Digital included over 18,000 IP addresses and numerous computer servers at data centers in New York, Chicago, Houston, Kansas City, Las Vegas, Atlanta, and elsewhere. In lieu of a traditional takedown, however, the prosecutors and agents executed a takeover of the network, proceeding in three stages:

1. Seizing control of the criminal computer network
2. Continuing to operate portions of the network to minimize further injury to crime victims
3. Coordinating with private sector entities to notify victims and remediate infected computers

The seizure of the computer network was accomplished in the traditional manner, using forfeiture warrants and a protective order. The protective order prohibited the pertinent RIRs and ISPs from making any changes to the ownership, registration, or Internet routing of the defendants' IP addresses, including the IP addresses used by the defendants' rogue DNS servers.

The next phase of the takeover—continued operation of the seized network—required extraordinary authority, because the forfeiture of the network had not been finalized. Absent a final order of forfeiture (or a declaration of administrative forfeiture), the Government does not have title to seized property, and its use of seized property can present potential issues of liability or create an appearance of impropriety. *See* Asset Forfeiture Policy Manual, Ch. 5, Sec. II.A (2013). Accordingly, government agents generally may not use seized property pending forfeiture, absent (1) consultation with the U.S. Marshals Service (or other appropriate property guardian), and (2) judicial authorization procured on the ground that such use is necessary in order to maintain the property. *See id.* Sec. II.B.

In Rove Digital, the judicial authorization to continue operating the seized network was founded on the district court's powers in equity, specifically its power to appoint a receivership over the seized property. *See generally id.* Ch. 10. The prosecutors relied on 18 U.S.C. § 1956(b)(4), which provides specific statutory authority to create a receivership in money laundering cases, as well as 21 U.S.C. § 853(e)(1), which more generally authorizes the district court to issue "a restraining order or injunction . . . or take any other action" to preserve property that is subject to criminal forfeiture. Although 21 U.S.C. § 853(e)(1) does not refer to receiverships *in haec verba*, a district court has inherent authority to create a receivership when its powers in equity are properly invoked. *See FTC v. U.S. Oil & Gas Corp.*, 748 F.2d 1431, 1432 (11th Cir. 1984) (per curiam) (holding that authority to appoint receiver

inhered in statutory authority to issue injunction); *see also In re McGaughey*, 24 F.3d 904, 907 (7th Cir. 1994) (recognizing "inherent equitable power to appoint a receiver"). The appointment of a receiver is an "extraordinary remedy," so the Government must demonstrate that less drastic measures would be inadequate. *See, e.g.*, *Netsphere, Inc. v. Baron*, 703 F.3d 296, 305 (5th Cir. 2012).

The district court in Rove Digital reasonably concluded that the extraordinary remedy of a receivership was warranted in order to prevent millions of victims from losing effective access to the Internet. Accordingly, the district court appointed a third party receiver with authority to operate replacement DNS servers, using the same IP addresses that had been used by the defendants' DNS servers. It was necessary to use the same IP addresses, that is, to continue operating part of the criminal computer network seized by the Government, because the victims' computers had been modified to use those IP addresses to make DNS queries (translate domain names into IP addresses).

The final stage of the takeover operation was to notify victims and to remediate the compromised computers. Notification of victims, of course, is mandated by statute. *See* 18 U.S.C. § 3771(c)(1) (2013). It is often impracticable to notify every victim in a large cybercrime investigation, however, because the information known about each victim is usually incomplete. In Rove Digital, for example, most victims were known only by the IP address of the victim computer contacting the rogue DNS servers (and later, the replacement DNS servers). In order to identify each victim, it would have been necessary to trace each of the millions of IP addresses through one or more ISPs. In such cases, a district court may authorize victim notification by any "reasonable procedure . . . that does not unduly complicate or prolong the proceedings." *Id.* § 3771(d)(2).

Remediating the harm caused by a criminal defendant is not a traditional law enforcement responsibility and can be a difficult goal to accomplish, especially in light of privacy and civil liberty concerns that are implicated when government actions—however well intended—affect privately owned computers. Remediation is nonetheless a worthwhile endeavor, particularly as to compromised computers, because a computer infected with malicious software is often used to infect other computers or as an instrumentality to commit other crimes. In addition, the fact that the Government is attempting to assist crime victims can be a significant consideration in persuading a court to invoke its equitable authority.

Accordingly, the prosecutors in Rove Digital obtained authority to provide notice of the case by publication on the Internet sites of the U.S. Attorney's office and the FBI. In addition to providing notice, the Internet sites offered technical information about repairing the DNS configuration on compromised computers. The prosecutors also obtained authority for the third party receiver to track the IP addresses of the victim computers, that is, any computers making DNS queries to the replacement DNS servers, and for the Government to provide the IP addresses of the victim computers to the ISPs on whose networks the victim computers were located. By working with private-sector entities, notifying ISPs, and helping them identify victim computers, the Government accomplished its goals of victim notification and remediation as part of the successful takeover in Rove Digital.

## III. A takeover using civil authorities: Coreflood

The takeover of the Coreflood botnet, though similar in many respects, differed from the takeover in Rove Digital in one significant way—there was no underlying criminal prosecution in Coreflood, so the Government's continued operation of the seized computer network was based on civil legal authorities rather than on criminal forfeiture. The ability to use civil legal authorities to take over a criminal computer network may be significant if there is no viable defendant to charge or if the need to interdict the criminal activity is so urgent that there is no time to conduct a full criminal investigation. *See United States v. Am. Heart Research Found., Inc.*, 996 F.2d 7, 11 (1st Cir. 1993) ("Congress authorized this expedited action [for a civil injunction against fraud] precisely because 'the investigation of

fraudulent schemes often takes months, if not years, before the case is ready for criminal prosecution' and in the meantime 'innocent people continue to be victimized.' ").

In Coreflood, over 2 million computers were, or had been, infected with the Coreflood virus. *See United States v. John Doe*, No. 3:11CV561 (VLB) (D. Conn. filed Apr. 11, 2011). The Coreflood virus allowed infected computers to be controlled remotely by another computer, known as a "command and control" server. Thus, each infected computer was potentially a software robot, or "bot," and the collection of infected computers was known as the "Coreflood botnet." Each bot would periodically communicate with a command-and-control server in order to receive updates or commands, a process known as "beaconing."

Botnets, in general, can be used for a range of criminal enterprises, including financial fraud, spamming, and denial-of-service attacks. The Coreflood botnet was used primarily to commit financial fraud. Specifically, infected computers in the Coreflood botnet automatically recorded the keystrokes and Internet communications of unsuspecting users, including online banking credentials and passwords. The stolen data was then transmitted to and stored on one or more command-and-control servers. The perpetrators used the stolen data to direct fraudulent wire transfers from the bank accounts of their victims.

The criminal computer network in Coreflood included command-and-control servers in Arizona, Georgia, Texas, Ohio, California, and the Republic of Estonia, together with 30 Internet domain names. Because the malicious software in Coreflood used those Internet domain names, rather than IP addresses, to communicate with the command-and-control servers, it was not necessary to seize the IP addresses used by Coreflood. The harm caused by Coreflood, however, could not be stopped by simply seizing its command-and-control servers and Internet domain names because the Coreflood virus on the infected computers would have remained active, stealing data and leaving the infected computers vulnerable to reacquisition by the perpetrators. Accordingly, a takeover of the Coreflood botnet was executed, using the same three-stage approach: (1) seizing the network, (2) continuing operating portions of the network, and (3) providing victim notification and remediation.

To accomplish the takeover, the prosecutors secured a temporary restraining order (later followed by preliminary and final injunctions), under 18 U.S.C. §§ 1345 and 2521. Section 1345 provides, in pertinent part, that the Government may file a civil suit and obtain an injunction to stop or prevent certain types of fraud, including mail fraud, wire fraud, and bank fraud. 18 U.S.C. §§ 1345 (2013). Section 2521 provides comparable authority with respect to violations of the Wiretap Act. *See* 18 U.S.C. § 2521 (2013). Thus, §§ 1345 and 2521, when applicable, offer explicit authority for invoking a district court's powers in equity to continue operating a criminal computer network in order to prevent harm to innocent victims.

In order to obtain an injunction under §§ 1345 and 2521, or similar statutes, *see, e.g.*, 18 U.S.C. § 1964(a) (authority to enjoin RICO violations), it is sufficient for the Government to show past criminal violations and a "reasonable likelihood" that the violations will continue. The less stringent "reasonable likelihood" standard applies where the Government has express statutory authority to seek an injunction against future criminal conduct. *See, e.g.*, *United States v. Philip Morris USA Inc.*, 566 F.3d 1095, 1131 (D.C. Cir. 2009) (injunction against RICO violations under 18 U.S.C. § 1964(a)); *SEC v. Sargent*, 329 F.3d 34, 39 (1st Cir. 2003) (injunction against securities law violations under 15 U.S.C. § 78u(d)); *United States v. Kaun*, 827 F.2d 1144, 1148 (7th Cir. 1987) (injunction against illegal tax shelters under 26 U.S.C. § 7408). The Government does not need to prove irreparable injury, which can be presumed from the past criminal violations. *See generally City of New York v. Golden Feather Smoke Shop, Inc.*, 597 F.3d 115, 120 (2d Cir. 2010). Before filing a civil suit for an injunction, prosecutors who are unfamiliar with civil practice and procedure may benefit from consulting with civil division Assistant U.S. Attorneys on issues that do not routinely arise in criminal proceedings, such as personal jurisdiction, venue, and service of process.

The civil suit in Coreflood was brought against the 13 "John Doe" defendants who had registered the Internet domain names (the Coreflood Domains) used by infected computers to communicate with the command-and-control servers. In the temporary restraining order, the defendants were prohibited from using the Coreflood botnet to continue engaging in fraud. In order to execute and enforce the order, the U.S. Marshals Service was directed to operate, through an independent third party, two substitute command-and-control servers that would respond when infected computers "beaconed" to the Coreflood Domains. *Cf.* 28 U.S.C. § 566(a) (2013) (providing that primary role of U.S. Marshals Service is, inter alia, to execute and enforce court orders). Specifically, the substitute command-and-control servers issued "exit" commands that caused the Coreflood virus to stop running on the infected computers. It was necessary to use the Coreflood Domains, that is, to continue operating part of the criminal computer network, because the infected computers used those domain names to communicate with the command-and-control servers.

At the Government's request, the temporary restraining order provided that the substitute command-and-control servers would only issue "exit" commands to infected computers that, based on IP addresses, were located in the United States. The limitation was requested to avoid the appearance that government-controlled computers in the United States were exercising any degree of control, via the Coreflood virus, over computers in foreign countries.

Finally, the prosecutors and investigating agents worked closely with private-sector entities, including ISPs and anti-virus vendors, to notify victims and to provide a means for removing Coreflood from infected computers. In addition, the Government obtained the consent of numerous institutional victims to remove Coreflood using Coreflood's own command-and-control mechanism. In other words, when given written consent by a victim, the Government issued commands from the substitute command-and-control servers that caused the Coreflood virus to be removed directly from the victim's computers without any further action by the victim. During the approximately ten-week period that the Government was operating the substitute command-and-control servers, the number of infected computers in the Coreflood botnet was reduced by over 95 percent.

## IV. Conclusions

The takeover of the criminal computer networks in Rove Digital and Coreflood demonstrate that there are effective tools that prosecutors can use to attack sophisticated cybercrimes. Considering how difficult it can be to identify the perpetrators of these crimes and to extradite them when they are located overseas (as they so often are), it may make sense to focus on dismantling the criminal computer networks that are being used when the perpetrators themselves cannot be easily prosecuted.

Rove Digital relied on criminal forfeiture and Coreflood relied on a civil injunction. A natural extension of those cases would be to take over a criminal computer network using civil forfeiture. Using civil forfeiture, the Government would not have to identify the perpetrators at all, because a civil forfeiture proceeding is brought in rem, meaning the defendant of the suit would be the criminal computer network itself. *See generally* Craig Gaumer, *A Prosecutor's Secret Weapon: Federal Civil Forfeiture Law*, 55 U.S. ATTORNEYS' BULLETIN 6, 59–73 (Nov. 2007), *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab5506.pdf. As with criminal forfeiture, any district court with venue over the action would have nationwide jurisdiction to issue a seizure warrant, *see* 18 U.S.C. § 981(b)(3) (2013), and the court would have express statutory authority to create a receivership over the seized network, *see id.* § 983(j). Although some criminal statutes only permit criminal, not civil, forfeiture of instrumentalities, *see, e.g.*, 18 U.S.C. § 1030(i) (2013) (computer intrusion); § 1037(c) (2013) (spamming), many criminal computer networks are likely used to violate at least one criminal statute that would support civil forfeiture of instrumentalities, *see, e.g.*, 18 U.S.C. § 2254 (2013) (child exploitation); § 2323(a) (2013) (copyright and trademark infringement); § 2513 (2013) (violations of Wiretap Act).

Prosecutors should be cautious, however, about initiating a civil proceeding if criminal charges are anticipated, in order to avoid problems that can arise with parallel civil and criminal proceedings.

Identifying the appropriate legal authority is only one step, however, in executing a successful takeover. There are significant prudential considerations that a prosecutor must weigh in determining how a seized criminal computer network can and should be used, and those considerations can be highly specific to the underlying technology in each case. For example, consider the question of whether public notice of a takedown or takeover should be made using the criminal computer network itself—for example, whether an online banner should be published on a seized computer server or Internet domain. This was done in Megaupload, and indeed, it is routinely done in takedowns of illegal Internet sites. It was not, however, done in Coreflood, even though there was no technical obstacle to doing so. In fact, using an online banner would have enormously simplified the task of victim notification. Using an online banner in Coreflood, however, would have required using the Coreflood virus to execute code on victims' computers—a technical approach that might be deemed more intrusive than posting a banner at Megaupload.com, even though the practical effect would have been the same.

As another example, consider the question of how to handle foreign computers. In Rove Digital, the replacement DNS servers responded to requests from foreign computers, but in Coreflood, the substitute command-and-control servers simply ignored communications from foreign computers. The reason for the distinction is that, in Rove Digital, the replacement DNS servers were responding to legitimate DNS queries generated by the Internet activity of legitimate computer users. In Coreflood, however, the substitute command-and-control servers were receiving communications generated by the Coreflood virus, so the communications were ignored (even though it would arguably have been better to respond with an "exit" command to the foreign computers as well as the U.S.-based computers). Obviously, prosecutors involved in the operation of seized criminal computer networks must be careful not to take actions with respect to foreign computers—no matter how innocuous or well-intentioned—that might be considered illegal under foreign law.

Rove Digital and Coreflood demonstrate that there are criminal and civil legal authorities available for prosecutors to use in attacking criminal computer networks on the Internet, even when it is necessary to takeover, and not merely takedown, those networks. ❖

## ABOUT THE AUTHOR

❑ **Edward Chang** has been an Assistant U.S. Attorney since 2000, first in the Southern District of New York and presently in the District of Connecticut. He currently serves as Deputy Chief of Appeals. ✠

# *Say Hello to My Little Friend*: The New and Improved Cyberstalking Statute

*Edward J. McAndrew*
*Assistant United States Attorney*
*District of Delaware*

New instances of technology-facilitated stalking continue to arise as the digital world assumes an increasingly vital role in our daily lives. Some of the many ways these instances manifest themselves include: cyberbullying at school, the office, or even a professional sports locker room; threatening a romantic rival via email or text message; extorting or coercing a victim to self-produce explicit or embarrassing images, provide money or other things of value; disseminating sexually explicit images of a person to others without the depicted person's consent; witness intimidation; and digital surveillance and harassment leading to murder. Through the Internet, this behavior can be directed at a victim from an ocean away or just down the hall. And its consequences can range from emotional and psychological distress to death.

There are a variety of federal statutes that may apply to any particular "stalking" scenario. *See, e.g.*, Jeff Breinholt, *Threats*, 60 UNITED STATES ATTORNEYS' BULLETIN 52, 63–66 (Jan. 2012) (discussing various threat crimes), *available at* http://dojnet.doj.gov/usao/eousa/ole/usabook/usab/1201/1201bu07.htm; C.J. Williams, *Making a Federal Case out of a Death Investigation*, 60 UNITED STATES ATTORNEYS' BULLETIN 1, 1–4 (Jan. 2012), *available at* http://dojnet.doj.gov/usao/eousa/ole/usabook/usab/1201/1201bu01.htm#III; Darcy Katzin et al., *Social Networking Sites: Breeding Grounds for "Sextortion" Prosecutions*, 59 UNITED STATES ATTORNEYS' BULLETIN 54, 54–55 (Sept. 2011), *available at* http://dojnet.doj.gov/usao/eousa/ole/usabook/usab/1109/1109bu06.htm#III.B; Margaret S. Groban & Leslie A. Hagen, *Domestic Violence Crimes in Indian Country*, 58 UNITED STATES ATTORNEYS' BULLETIN 2, 4–5 (July 2010), *available at* http://dojnet.doj.gov/usao/eousa/ole/usabook/usab/1007/1007bu01.htm.

This article surveys the recently revised and more expansive federal cyberstalking statute, 18 U.S.C. § 2261A(2). This newest iteration of § 2261A(2) sprung into effect as the Federal Government shutdown on October 1, 2013.

This article will compare the old and the new versions of § 2261A(2) and will highlight how the new changes broaden and sharpen the cyberstalking statute into a formidable tool for combating various forms of online abuse. This article will then touch on some of the key points to bear in mind as you consider charging and prosecuting a cyberstalking case under § 2261A(2).

## I. The old words and the new

### A. Prior versions of the cyberstalking statute

The interstate stalking statute was originally passed in 1996, as part of the Violence Against Women Act. *See* National Defense Authorization Act for Fiscal Year 1997, Pub. L. No. 104-201, 110 Stat. 2422, 2655 (1996). It is codified at 18 U.S.C. § 2261A. From September 23, 1996 to October 27, 2000, § 2261A only proscribed stalking based on interstate travel "with intent to injure or harass another person." 18 U.S.C. § 2261A (1996). Since October 28, 2000, § 2261A has included two provisions:

Subsection 1 (the interstate stalking provision), and Subsection 2 (the cyberstalking provision). This article will focus on the cyberstalking provision.

Prior to January 2006, § 2261A(2) proscribed the use of "the mail or any facility of interstate or foreign commerce to engage in a course of conduct that places [a] person in reasonable fear of the death of, or serious bodily injury to, [that person, an immediate family member of that person, or the spouse/intimate partner of that person]." 18 U.S.C. § 2261A(2) note (2006 Amendments) (2013). The statute further required that the defendant have acted with the intent "to kill or injure," *id.* § 2261A(2)(A), or to place a person in reasonable fear of the death of, or serious bodily injury to, that person, an immediate family member, or a spouse/intimate partner. *Id.*§ 2261A(2)(B). Finally, the statute required that the victim be located "in another State or tribal jurisdiction, or within the special maritime and territorial jurisdiction of the United States." *Id.*

Thus, this original version of § 2261A(2) was limited as to the criminal intent (that is, "to kill or injure" or "to place a person in another State . . . in reasonable fear of the death of, or serious bodily injury to [that person, an immediate family member of that person, or the spouse/intimate partner of that person]"). *Id.* § 2261A(2)(A) & (B). It also did not protect against any harm other than fear of death or physical injury. Both subsections (A) and (B) further required that the perpetrator and the victim be located across certain geographical boundaries (that is, state jurisdiction, tribal jurisdiction, or special maritime and territorial jurisdiction).

From January 5, 2006 to September 30, 2013, § 2261A(2) read:

> Whoever--
>
> * * *
>
> **(2)** with the intent--
>
> **(A)** to kill, injure, harass, or place under surveillance with intent to kill, injure, *harass, or intimidate, or cause substantial emotional distress to* a person in another State or tribal jurisdiction or within the special maritime and territorial jurisdiction of the United States; or
>
> **(B)** to place a person in another State or tribal jurisdiction, or within the special maritime and territorial jurisdiction of the United States, in reasonable fear of the death of, or serious bodily injury to--
>
> > **(i)** that person;
> >
> > **(ii)** a member of the immediate family (as defined in section 115) of that person; or
> >
> > **(iii)** a spouse or intimate partner of that person;
>
> uses the mail, *any interactive computer service*, or any facility of interstate or foreign commerce to engage in a course of conduct that causes substantial emotional distress to that person or places that person in reasonable fear of the death of, or serious bodily injury to, any of the persons described in clauses (i) through (iii) of subparagraph (B);
>
> shall be punished as provided in section 2261(b) of this title.

18 U.S.C. § 2261A(2) note (2013 Amendments) (2013) (emphasis on added language).

This version of § 2261A(2) substantially expanded the statute's coverage in a number of ways. First, the mens rea element was broadened to include an intent "to . . . harass, or place under surveillance with intent to kill, injure, harass, or intimidate, or cause substantial emotional distress to" the intended victim. *Id.*

Second, the instrumentalities of the crime were expanded to include "any interactive computer service." *Id.* Although not defined in §§ 2261A or 2266, "interactive computer service" is defined elsewhere in the United State Code to mean "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 15 U.S.C. § 1637(c) (2013); 18 U.S.C. § 1462 (cross referencing 47 U.S.C. § 230(f)); 47 U.S.C. § 230(f) (2013).

Third, in terms of the requisite harm, causing "substantial emotional distress" to the victim was added to the prior requisite harm of placing a person "in reasonable fear of the death of, or serious bodily injury to" the victim or related persons. 18 U.S.C. § 2261A(2) note (2013 Amendments) (2013). This significantly expanded the protection of victims who could be harassed, embarrassed, or defamed to the point of suffering severe, non-physical injury, even if the perpetrator did not place them in fear of injury or death to themselves or a loved one.

Though much broader than its prior iteration, this version of § 2261A(2) still required the perpetrator and the victim to be located in different jurisdictions when the proscribed "course of conduct" occurred. Thus, the stalker who used a social networking application or email/instant message service from another state could be prosecuted under § 2261A(2), but the stalker who did the same from across the university campus, down the office corridor, or elsewhere within a state could not. As a result, the statute offered no protection to victims of cyberbullying, extortion, harassment, or threats perpetrated by those geographically close to them. *See, e.g.*, *United States v. Borker*, 2011 WL 1630344, at * 1 (S.D.N.Y. Apr. 28, 2011) (dismissing cyberstalking count "because 18 U.S.C. § 2261A 'requires that the perpetrator and the victim be situated in different states' "); *United States v. Jordan*, 591 F. Supp. 2d 686, 707 n.28 (S.D.N.Y. 2008) (The Government agreed to narrow the scope of cyberstalking indictment to the time when defendant and victim were in separate states in order to meet the statute's requirement.).

## B. The new cyberstalking statute

The newly revised cyberstalking statute is a much broader and more powerful tool than its predecessors. Regardless of the location of the defendant or the victim, it can be used against cyberbullying, extortion, defamation, threats, spying, and even murder, death or serious bodily injury resulting from digital harassment, intimidation, or surveillance.

The new § 2261A(2), which became effective on October 1, 2013 and which has been substantially rewritten, provides:

> Whoever--
>
> * * *
>
> **(2)** with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that--
>
> **(A)** places that person in reasonable fear of the death of or serious bodily injury to a person described in clause (i), (ii), or (iii) of paragraph (1)(A); or
>
> **(B)** causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of paragraph (1)(A),
>
> shall be punished as provided in section 2261(b) of this title.

18 U.S.C. § 2261A(2) (2013).

The new § 2261A(2) improves upon its predecessor in three key ways. First, and most significantly, it eliminates the requirement that the perpetrator and the victim be located in separate jurisdictions. Section 2261A(2) now enables the Government to prosecute a wide range of stalking conduct where the perpetrator and victim are in relatively close proximity. Such cases could range from those resulting in harassment causing emotional distress or fear of death or injury, to those involving the use of digital technology to commit premeditated murder.

Second, the new § 2261A(2) further expands the types of instrumentalities that may be used to violate the statute. In particular, § 2261A(2) adds two new types of technologies to those that are covered: "electronic communication service[s]" and "electronic communication system[s] of interstate commerce." Although the term is not defined in §§ 2261A or 2266, an "electronic communication service" is defined in the Wiretap Act as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (2013). The Wiretap Act also defines an "electronic communications system" as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." *Id.* § 2510(14). Although the Wiretap Act definition includes an "s" on "communication" that is missing from § 2261A, the definition should nonetheless apply. *Cf. Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 899–901 (9th Cir. 2008) (using the Wiretap Act definition of "electronic communications system" to determine whether the defendant violated the Stored Communications Act), *rev'd sub nom. on other grounds, City of Ontario, Cal.* v. *Quon*, 130 S. Ct. 2619, 2633 (2010).

Third, the new § 2261A(2) expressly applies to conduct that "attempts to cause, or would be reasonably expected to cause" substantial emotional distress. When proceeding under an emotional distress theory, proof that a victim actually suffers substantial emotional distress is no longer required. This change should allow law enforcement to act more quickly on cyberstalking allegations without having to wait for a victim to actually suffer severe emotional distress or worse.

One area that remains unchanged is that of cyberstalking conspiracies. Section 2261A still does not contain an express conspiracy provision. Therefore, prosecutors should continue to charge conspiracies to cyberstalk under 18 U.S.C. § 371. *See, e.g., United States v. Fullmer*, 584 F.3d 132, 163 (3d Cir. 2009). It will often be the case that such a conspiracy count would accompany substantive cyberstalking counts against each defendant. *See, e.g.*, Press Release, Federal Bureau of Investigation, Three Members of Matusiewicz Family Indicted for Federal Stalking Crimes Resulting in Courthouse Murders (Aug. 8, 2013) (indictment charging conspiracy, aiding and abetting, and substantive interstate and cyberstalking resulting in death against three co-conspirators), *available at* http://www.fbi.gov/baltimore/press-releases/2013/three-members-of-matusiewicz-family-indicted-for-federal-stalking-crimes-resulting-in-courthouse-murders.

## II. Key points in utilizing the new § 2261A

Key issues commonly arise with each element of a cyberstalking charge. Although courts have articulated them differently depending on the type of stalking conduct at issue, those elements can be broadly characterized as:

1. Criminal intent
2. Use of a prescribed medium to engage in a "course of conduct"
3. A qualifying effect (actual or intended) on the victim.

*See* 18 U.S.C. § 2261A(2) (2013); *United States v. Petrovic*, 701 F.3d 849, 859–60 (8th Cir. 2012); *United States v. Shrader*, 675 F.3d 300, 309–10 (4th Cir. 2012); *United States v. Fullmer*, 584 F.3d 132, 163 (3d Cir. 2009); *United States v. Bowker*, 372 F.3d 365, 388 (6th Cir. 2004), *vacated on other grounds*, 543 U.S. 1182 (2005).

## A. Criminal intent

The required criminal intent is now expressed entirely and more clearly in § 2261A(2), without resort to subsections (A) or (B). The prior version of § 2261A(2) listed alternate criminal intents in subsections (A) and (B). To establish the necessary mens rea for a cyberstalking violation, the Government must prove that the defendant acted with the intent to do one or more of the following:

1. To kill
2. To injure
3. To harass
4. To intimidate
5. To place under surveillance with the intent to kill, injure, harass, or intimidate

18 U.S.C. § 2261A(2) (2013). These acts obviously cover a wide range of intentions, ranging from harassment and intimidation to murder.

Reported cases often deal with the intent to harass, intimidate, and to place under surveillance. The terms "harass" and "intimidate" are to be given their ordinary meanings, which "can be ascertained fairly by reference to judicial decisions, common law, dictionaries, and the words themselves because they possess a common and generally accepted meaning." *United States v. Bowker*, 372 F.3d 365, 381 (6th Cir. 2004) (quoting *Staley v. Jones*, 239 F.3d 769, 791–92 (6th Cir. 2001)). To "harass" can be defined as "to disturb persistently; torment." WEBSTER'S ENCYCLOPEDIC UNABRIDGED DICTIONARY 870 (2d ed.1996). To "intimidate" can be defined as "to make timid; fill with fear." *Id.* at 1000. Courts generally do not labor to find sufficient evidence of intent to harass or intimidate. *See, e.g.*, *United States v. Petrovic*, 701 F.3d 849, 860 (8th Cir. 2012) (finding intent to harass and intimidate where defendant posted a Web site displaying sexually explicit images of victim taken during their relationship and sent postcards to her ex-husband, employer, family members, and local businesses regarding the Web site); *United States v. Shrader*, 675 F.3d 300, 312 (4th Cir. 2012) (finding intent to harass and intimidate where defendant left messages citing a need to talk before victim's death, wrote a "manifesto" asking God to take victim's child's life, etc.); *United States v. Al-Zubaidy*, 283 F.3d 804, 809 (6th Cir. 2002) (intent may be inferred from totality of circumstances).

Despite the broad meaning of these terms, some courts have overly scrutinized allegations that a defendant acted with intent to harass. An Arizona district court, for instance, dismissed a stalking complaint after concluding that the Government failed to establish intent to harass the victim. *United States v. Infante*, 782 F. Supp. 2d 815, 823 (D. Ariz. 2010). Infante met a woman while they attended a class together at Arizona State University. After a coffee date, she informed Infante " 'she was not interested in communicating with [him] any longer' and 'on several occasions to leave her alone and to stop bothering her.' " *Id.* at 820–21. She then returned to her home state of New Jersey and later to college in Rochester, New York. Infante contacted the woman by Facebook, email, and text message. He also traveled to Rochester, sent her flowers from a local flower shop, and tried to obtain information about her from a professor. He saw her in person, but did not attempt to approach her or to make eye contact. He thereafter continued to email her, writing that "he could not live with just a 'platonic love' because he had a 'powerful longing' for [her]." *Id.* at 821.

After beginning his opinion with a quote from Oscar Wilde about stupidity and nobility, the magistrate judge concluded that the " 'intent-to-harass' element of [§ 2261A] requires that a defendant act with the purpose to harass." *Id.* at 820. The magistrate judge quoted a New Hampshire district court opinion that also rejected a charge under the Telephone Harassment Statute (47 U.S.C. § 223(a)(1)(D)) after finding insufficient evidence of intent to harass:

> In other words, it is not enough merely to foresee that emotional upset is a likely consequence of repeated calls. Instead, the actor must purposely seek to cause, or must desire to cause an adverse emotional reaction in a person . . . .

*Id.* (quoting *United States v. Tobin*, 545 F. Supp. 2d 189, 193 (D.N.H. 2008)). The magistrate reasoned that Infante acted only "in the misguided hope to renew their relationship" and had not threatened the victim. *Id.* at 821–22. Thus, in his view, Infante lacked the necessary intent to harass the victim.

Any concern over such scrutiny should be alleviated by the new cyberstalking statute. One of the most potentially significant changes under new § 2261A(2) is the elimination of two areas of intent that generated a fair amount of litigation: (1) the intent to cause substantial emotional distress; and (2) the intent to cause reasonable fear of death or serious bodily injury. Although defendants are generally unsuccessful, sufficiency challenges to proof of intent to cause emotional distress or to cause fear of death/injury are a common ground for legal challenge. *See, e.g.*, *Shrader*, 675 F.3d at 312–13 (holding that defendant's communications to victim evinced clear intent to cause fear and emotional distress); *Bowker*, 372 F.3d at 388–89 (defendant unsuccessfully argued that district court failed to dismiss his cyberstalking count for lack of intent); *United States v. Clement*, 2010 WL 1812395, at *1 (W.D. La. May 3, 2010) (defendant unsuccessfully argued that Government failed to prove he acted with the requisite intent); *United States v. Jordan*, 591 F. Supp. 2d 686, 707 (S.D.N.Y. 2008) (defendant unsuccessfully claimed he acted to convince victim to rekindle relationship, not to cause her emotional distress or fear of death/injury).

In addition, the intent elements relating to emotional distress and reasonable fear of death/injury were sometimes conflated to the point of reversible error. For example, the Ninth Circuit recently reversed a cyberstalking conviction by bench trial, after the district court judge failed to specify whether the defendant violated § 2261A(2)(A) or (B). *See United States v. Cook*, 2013 WL 5718210, at *1 (9th Cir. Oct. 22, 2013). In particular, the *Cook* court found reversible error in the trial judge's failure to clearly explain whether the defendant acted with an intent "to kill, injure, harass, or intimidate, or cause substantial emotional distress," in violation of § 2261A(2)(A), or whether the defendant acted with the intent to place the victim "in reasonable fear of death or serious injury to herself" or other protected class members, in violation of § 2261A(2)(B).

While they have been removed from the mens rea element, the concepts of emotional distress and fear of death/injury have not been removed from the statute. They are now expressed only in the element of the crime focused on the effect on the victim. *See* 18 U.S.C. § 2261A(2)(A), (B) (2013). These new requirements relating to fear of death/injury or emotional distress are discussed below.

### B. The use of mediums to engage in a "course of conduct"

The defendant also must use one or more of the following to engage in a "course of conduct" with at least one of the types of criminal intent outlined above:

1. The mail
2. An interactive computer service
3. An electronic communication service
4. An electronic communication system of interstate commerce
5. Any facility of interstate or foreign commerce

18 U.S.C. § 2261A(2). Without cataloguing the scope of items, it should suffice to say that any cell phone, computer, Web site, electronic messaging service, or digital device capable of connecting to the Internet will qualify.

Special consideration should be given to defining the "course of conduct" in which the defendant engages. Section 2266 expressly defines a "course of conduct" as "a pattern of conduct composed of 2 or more acts, evidencing a continuity of purpose." 18 U.S.C. § 2266(2) (2013). The Government is not required to prove, however, that "each act was intended in isolation to cause serious distress or fear of bodily injury to the victim." *Shrader*, 675 F.3d at 311. It is enough for the Government to show that "the totality of the defendant's conduct 'evidenced a continuity of purpose' to achieve the criminal end." *Id.* Thus, the proper focus is on "persistent or repetitive conduct" by the defendant. *Id.* at 312 ("The cumulative effect of a course of stalking conduct may be greater than the sum of its individual parts.").

### C. Fear of death/injury or actual, intended or possible emotional distress

The Government has a new, much lighter burden as to the final element of the crime—the effect of the defendant's actions on the victim. Under § 2261A(2)(A) and (B), the defendant's course of conduct must either:

1. Place the targeted victim in reasonable fear of death or serious bodily injury, or
2. Cause, attempt to cause, or would reasonably be expected to cause substantial emotional distress

to the targeted victim or to an immediate family member, spouse, or intimate partner of the victim. *See id.* § 2261A(2)(A),(B).

There is no longer a requirement to prove that the defendant *intended* for the victim to experience fear of death/injury or substantial emotional distress, with the possible exception of an allegation that the defendant acted only in an attempt to cause such distress. As noted above, a fair number of the decisions under § 2261A(2) focused on the sufficiency of evidence to support this erstwhile element.

Under the new statute, the Government still can prove that reasonable fear of death/injury resulted from the defendant's actions. Alternatively, and even more broadly, the Government can prove that the defendant's actions:

1. Actually caused
2. Attempted to cause, or
3. Would reasonably be expected to cause

substantial emotional distress. Unlike under prior law, whether the defendant tries or succeeds in causing emotional distress is no longer determinative, so long as a reasonable person would have been expected to suffer such. This is a substantial lightening of the Government's burden. *See, e.g.*, *United States v. Petrovic*, 701 F.3d 849, 860 (8th Cir. 2012) (challenging sufficiency of evidence to establish that victim suffered substantial emotional distress); *United States v. Clement*, 2010 WL 1812395, at *2 (W.D. La. May 3, 2010) (similar). This issue will be a quintessential jury question that may allow the Government to avoid, or at least limit, testimony of victims or other witnesses at trial.

## III. Penalties for cyberstalking

The penalties for violating both the cyberstalking and interstate stalking subsections of § 2261A remain unchanged under the new legislation. The available penalties, which are contained in § 2261(b), are tied to the effect that the cyberstalking has on the victim. The maximum penalties range from five years to life, and there is a mandatory minimum penalty of one year for those who commit a stalking offense in violation of certain types of court orders.

Section 2261(b) provides:

> (b) Penalties.--A person who violates this section or section 2261A shall be fined under this title, imprisoned--

(1) for life or any term of years, if death of the victim results;

(2) for not more than 20 years if permanent disfigurement or life threatening bodily injury to the victim results;

(3) for not more than 10 years, if serious bodily injury to the victim results or if the offender uses a dangerous weapon during the offense;

(4) as provided for the applicable conduct under chapter 109A if the offense would constitute an offense under chapter 109A (without regard to whether the offense was committed in the special maritime and territorial jurisdiction of the United States or in a Federal prison); and

(5) for not more than 5 years, in any other case,

(6) Whoever commits the crime of stalking in violation of a temporary or permanent civil or criminal injunction, restraining order, no-contact order, or other order described in section 2266 of title 18, United States Code, shall be punished by imprisonment for not less than 1 year.

or both fined and imprisoned.

*Id.*

In addition to these penalty provisions, § 2265A also contains an enhanced penalty for recidivist domestic violence or stalking offenders. In particular, § 2265A provides:

**(a) Maximum term of imprisonment.**--The maximum term of imprisonment for a violation of this chapter after a prior domestic violence or stalking offense shall be twice the term otherwise provided under this chapter.

**(b) Definition.**--For purposes of this section--

**(1)** the term "prior domestic violence or stalking offense" means a conviction for an offense--

**(A)** under section 2261, 2261A, or 2262 of this chapter; or

**(B)** under State or tribal law for an offense consisting of conduct that would have been an offense under a section referred to in subparagraph (A) if the conduct had occurred within the special maritime and territorial jurisdiction of the United States, or in interstate or foreign commerce; and

**(2)** the term "State" means a State of the United States, the District of Columbia, or any commonwealth, territory, or possession of the United States.

18 U.S.C. § 2265A (2013).

When viewed in light of the myriad types of conduct covered by § 2261A(2), § 2265A is a very broad and powerful sentencing provision.

Two important issues arise regarding the connection between the cyberstalking conduct and the resulting harm to the victim. First, is there a mens rea requirement relating to the injury suffered by the victim? Second, what causal connection must exist between the course of conduct and the injury? There appear to be no reported cases addressing these issues in the context of interstate stalking or cyberstalking resulting in injury or death under § 2261A. We may find guidance, however, from the interpretation of other statutes that contain similar "resulting in death/injury" penalty provisions.

In interpreting other statutes containing "resulting in death/injury" provisions, courts have consistently held that there is no mens rea requirement as to the victim's injury. That is, the Government

need not prove that the defendant intended the death or injury of the victim for the enhanced penalty provision to apply. For example, courts have held that the Government need not prove that a defendant charged with federal kidnapping under 18 U.S.C. § 1201 "voluntarily and intentionally caused the resulting death[]." *United States v. Barraza*, 576 F.3d 798, 807 (8th Cir. 2009) (quoting 18 U.S.C. § 1201 ("the death of any person results")); *cf. United States v. Matus-Leva*, 311 F.3d 1214, 1219 (9th Cir. 2002) (no mens rea requirement as to enhanced penalty for transportation of aliens resulting in death under 8 U.S.C. § 1324(a)(1)(B)(iv)).

Similarly, under the federal felony-murder statute, 18 U.S.C. § 1111(a), the Government need not prove that the defendant who commits an underlying felony also intended to kill the victim. *See, e.g.*, *United States v. Tham*, 118 F.3d 1501, 1508 (11th Cir. 1997). Instead, the "fact that the death, even if accidental, resulted from the commission of the enumerated felony is sufficient . . . ." *United States v. Parks*, 411 F. Supp. 2d 846, 852 (S.D. Ohio 2005). As the district court in *Parks* noted in finding that the penalty provision of the federal bank robbery statute (18 U.S.C. § 2113(e)) contained no mens rea provision:

> Congress has enacted numerous statutes that impose penalties of death or life imprisonment "if death results" from the commission of a felony. Like § 2113(e), none of these statutes contains an express mens rea requirement.

*Id.*

Although there are no cases directly on point under the cyberstalking statute, the causation analysis will likely follow that applicable to other statutes that include sentencing enhancements where the criminal conduct "results" in death. The most recent Supreme Court pronouncement on this issue came just days ago in *Burrage v. United States*, No. 12-7515, 2014 WL 273243 (Jan. 27, 2014), where the Court reversed a defendant's conviction for distribution of heroin resulting in a user's death, in violation of 21 U.S.C. § 841(a)(1) and (b)(1)(C). Two medical experts testified that the taking of the heroin contributed to the user's death. Due to other narcotics taken by the deceased user, neither expert could say whether the user would have lived had he not taken the heroin. *Id.* at *2. The Court concluded that such testimony was insufficient to establish that the defendant's distribution of heroin resulted in the user's death. *Id.* at *9.

The Supreme Court began by stating that "[w]hen a crime requires 'not merely conduct but also a specified result of conduct,' a defendant generally may not be convicted unless his conduct is 'both (1) the actual cause, and (2) the legal cause (often called the proximate cause) of the result.' " *Id.* at *4 (quoting 1 W. LaFave, SUBSTANTIVE CRIMINAL LAW § 6.4(a), pp. 464–66 (2d ed. 2003); ALI, MODEL PENAL CODE § 2.03, p. 25 (1985)). The Court expressly limited its analysis to the concept of "actual cause." *Id.* Its opinion does not address the second constituent part of causation: "proximate cause." *Id.*

As to the "actual cause" component, the Court read the statutory phrase "results from" to "require[] proof 'that the harm would not have occurred' in the absence of – that is, but for – the defendant's conduct.' " *Id.* (quoting *Univ. of Tex. Sw. Med. Ctr. v. Nassar*, 133 S. Ct. 2517, 2525 (2013) (quoting RESTATEMENT OF TORTS § 431, cmt. A (1934))). Under the facts in *Burrage*, this "actual cause" standard required the government to prove that "the use of the drug distributed by the defendant [was] an independently sufficient cause of the victim's death." *Burrage*, 2014 WL 273243, at *9.

Meeting this "actual cause" standard in the context of a cyberstalking case will be fact intensive, but should not prove difficult. It is critical to articulate to the court that cyberstalking involves a "course of conduct," not an isolated act of the type at issue in *Burrage*, that is, the distribution of heroin to a particular user who dies after taking it. The government is not required to prove that "each act was intended in isolation to cause [death]." *United States v. Shrader*, 675 F.3d 300, 309–10 (4th Cir. 2012). Instead, prosecutors must develop facts to show that "the totality of the defendant's conduct" was a "but for" cause of the victim's death. *Id.* To use the language of *Burrage*, the government must prove that the

victim's death "would not have occurred in the absence of" the cyberstalking course of conduct. *Burrage*, 2014 WL 273243, at *4.

Although it does not analyze the issue, *Burrage* makes clear that "death results" sentencing enhancements also create a proximate cause requirement. *Id.* Thus, in addition to proving that the victim's death or injury would not have occurred but for the cyberstalking, the Government also must prove that the defendant's cyberstalking conduct proximately caused the victim's death or injury. Again, there appear to be no reported decisions addressing this issue under §§ 2261(b) or 2261A, but the requirement is clear in light of *Burrage*.

Even prior to *Burrage*, most courts had held that the Government must prove that the defendant's conduct proximately caused death or injury under statutes employing the "results in death/injury" language. As the Ninth Circuit explained, a "basic tenet of criminal law is that, when a criminal statute requires that the defendant's conduct has resulted in an injury, the government must prove that the defendant's conduct was the legal or proximate cause of the resulting injury." *United States v. Pineda-Doval*, 614 F.3d 1019, 1026 (9th Cir. 2010) (imposing proximate cause requirement for transportation of aliens resulting in death) (quoting *United States v. Spinney*, 795 F.2d 1410, 1415 (9th Cir. 1986)).

Other circuits have stated likewise as to various federal statutes containing enhanced penalties for conduct resulting in death/injury. *See id.* at 1027 n.4 (collecting cases). The Sixth Circuit, for instance, has held that the Government must establish conduct proximately causing death in a health care fraud case under 18 U.S.C. § 1347(a)(2). *See United States v. Hancock*, 2012 WL 1058422, at *2 (6th Cir. Mar. 29, 2012). The Sixth Circuit explained:

> "The concept of proximate cause incorporates the notion that an accused may be charged with a criminal offense even though his acts were not the immediate cause of the victim's death or injury." *Guillette*, 547 F.2d at 749. "In many situations giving rise to criminal liability," the harm "is not directly caused by the acts of the defendant but rather results from intervening forces or events." *Id.* "Where such intervening events are foreseeable and naturally result from [the defendant]'s criminal conduct," the defendant is "criminally responsible for the resulting harm." *Id.*; *see also Hoopengarner v. United States*, 270 F.2d 465, 469 (6th Cir. 1959) (holding defendant culpable for the "natural and probable consequence [ ]" of his conduct). Therefore, even if [the defendant] did not intend for his two patients to die, he can be held responsible for their deaths if there was sufficient evidence that it "reasonably might or should have been foreseen . . . that [his fraudulent conduct] would be likely to create a situation which would expose another to the danger of . . . death." *Id.*; *see also Harris*, 701 F.2d at 1102 (holding that "if death results" requirement under § 241 [was] satisfied because death was "a foreseeable and natural result" of defendant's actions).

*Id.* (quoting *United States v. Martinez*, 588 F.3d 301, 319 (6th Cir. 2009) (quoting various cases)); *see also United States v. Ouedraogo*, 2013 WL 4792928, at *13 (6th Cir. Sept. 10, 2013) (Government must prove kidnapping proximately caused death for enhanced penalty to apply); *Parks*, 411 F. Supp. 2d at 856 ("The Court agrees that Defendants cannot be held criminally liable for Williams' death, or be subjected to the increased penalties set forth in § 2113(e), unless the Government proves that their conduct during the high speed chase proximately caused Williams' death.").

A final point about enhanced penalties bears noting. Other than proof of a prior conviction, facts triggering an enhanced penalty must be found by the jury. *See, e.g.*, *Burrage*, 2014 WL 273243, at *3 ("Because the 'death results' enhancement increased the minimum and maximum sentences to which Burrage was exposed, it is an element that must be submitted to the jury and found beyond a reasonable doubt."). The Supreme Court has explained, "When a finding of fact alters the legally prescribed punishment so as to aggravate it, the fact necessarily forms a constituent part of a new offense and must be submitted to the jury." *Alleyne v. United States*, 133 S. Ct. 2151, 2162 (2013); *United States v. Lake*,

2013 WL 4017293, at *1 (10th Cir. Aug. 8, 2013) (vacating sentence where "resulted in death" finding was not made by jury in narcotics trafficking conspiracy case); *United States v. Hancock*, 2012 WL 1058422, at *2 (6th Cir. Mar. 29, 2012) (jury must find facts for enhanced penalty on charge of health care fraud resulting in death).

## IV. First Amendment issues

As a general matter, speech engaged in as part of a cyberstalking "course of conduct" is not protected by the First Amendment. *See, e.g.*, *United States v. Petrovic*, 701 F.3d 849, 854–56 (8th Cir. 2012); *United States v. Sayer*, 2012 WL 1714746, at *2–9 (D. Me. May 15, 2012); *but see United States v. Cassidy*, 814 F. Supp. 2d 574, 583–88 (D. Md. 2011) (§ 2261A(2) violated First Amendment as applied to statements posed online about religious views of well-known religious figure).

There are certain "well-defined and narrowly limited classes of speech" that are not protected by the First Amendment. *United States v. Stevens*, 559 U.S. 460, 468–69 (2010) (quoting *Chaplinsky v. New Hampshire*, 315 U.S. 568, 571–72 (1942)). They include:

- Defamation—*Beauharnais v. Illinois*, 343 U.S. 250, 254–255 (1952)
- Fraud—*Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748, 771 (1976)
- Incitement—*Brandenburg v. Ohio*, 395 U.S. 444, 447–449 (1969)
- Obscenity—*Roth v. United States*, 354 U.S. 476, 483 (1957)
- Speech integral to criminal conduct—*Giboney v. Empire Storage & Ice Co.*, 336 U.S. 490, 498 (1949)
- True threats—*Watts v. United States*, 394 U.S. 705, 708 (1969)

Speech that is part of a cyberstalking course of conduct generally falls into one or more of these categories.

In *Petrovic*, for instance, the defendant disseminated sexually explicit images and false and defamatory statements relating to promiscuity of a former spouse, both online and through the mail. *See Petrovic*, 701 F.3d at 852–53. Prior to doing so, he had threatened the victim with such acts if she did not continue their relationship. The Eighth Circuit easily concluded that these communications "were integral to [his] criminal conduct as they constituted the means of carrying out his extortionate threats." *Id.* at 855. The court also noted that the victim was a private individual, and the information that the defendant disseminated was "intensely private information." *Id.*

A Maine district court reached the same conclusion in a case where the defendants used Web sites and email services to create fictitious Internet advertisements and social media profiles portraying the victim as promiscuous and inviting men for sexual encounters. *See United States v. Sayer*, 2012 WL 1714746, at *1–2 (D. Me. May 15, 2012). One defendant also sent letters to various people falsely accusing a victim of being a "serial rapist, child molester and murderer" and claiming that the victim "makes child pornography." *Id.* at *3. The district court found that none of these communications were protected by the First Amendment. Instead, they were "integral to criminal conduct" and defamatory. *Id.* at *2–4; *see also Snyder v. Phelps*, 131 S. Ct. 1207, 1215 (2011) ("[W]here matters of purely private significance are at issue, First Amendment protections are often less rigorous . . . because restricting speech on purely private matters does not implicate the same constitutional concerns as limiting speech on matters of public interest.").

The analysis is more complex where the victim of the cyberstalking is a public figure and speech comprising the alleged course of conduct concerns public issues. In *United States v. Cassidy*, 814 F. Supp. 2d 574 (D. Md. 2011), the district court held that Twitter and blog posts were protected speech

even though they caused the victim emotional distress. *Id.* at 585–86. Unlike the private victims and information at issue in the cases noted above, the victim in *Cassidy* was a well-known public figure, and the defendant's posts only criticized her character and qualifications as a religious leader. *See id.* at 583. The vast majority of cyberstalking scenarios will be easily distinguishable from *Cassidy*. Prosecutors simply need to be mindful of the differing standards that may apply where the course of conduct involves speech about public issues involving a victim who is a public figure.

## V. Conclusion

The newly revised, federal cyberstalking statute is a flexible and powerful tool now available to combat many forms of online abuse. From simple harassment to premeditated murder, § 2261A(2) provides a statutory net for investigating and prosecuting online abuses that may have fallen through prior gaps in the federal criminal code. By using Internet-based conduct and digital technology as federal jurisdictional hooks, § 2262A(2) now enables federal prosecutors to pursue cases that may be wholly intrastate in nature. Thus, the cyberstalker or cyberbully next door is no longer immune from criminal prosecution under federal stalking law. In addition, the lighter evidentiary burden the government bears should enable federal prosecutors to investigate and charge cyberstalking cases earlier in the cycle of online abuse, with the hope of preventing at least some of the tragedies that too often result from this relatively new form of criminal conduct.❖

### ABOUT THE AUTHOR

❑ **Edward J. McAndrew** is an Assistant United States Attorney in the District of Delaware, where he focuses on Internet-based and technology facilitated crimes. He previously served in the Cyber Crime Unit of the Eastern District of Virginia and in the Criminal Division's Child Exploitation and Obscenity Section. Prior to joining the Department in 2006, he was a litigation partner at Reed Smith LLP, in Washington, D.C. ✠