Digital Investigation (2004) 1, 7–15

ELSEVIER

Digital Investigation

www.elsevier.com/locate/diin

Current issues confronting well-established computer-assisted child exploitation and computer crime task forces

Monique Mattei Ferraro[1], Andrew Russell[2]

Received 9 January 2004

Introduction

Over the past five years, a large number of agencies have developed specialized units to deal with high technology crimes and Internet crimes against children. The United States currently funds approximately 45 Internet Crimes Against Children Task Forces.[3] This article talks about some of the issues confronting established Internet crimes against children and high technology crime units and examines approaches to their resolution. First, the tension between forensics and investigations is discussed. With the first computer forensic laboratory being accredited by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB), pressure to split the functions is increasing attention to unit functions (Casey, 2004; Ferraro and Casey, 2004a). Next, the article addresses the continued confusion over obtaining information from Internet service providers.[4] The third issue discussed is the burgeoning problem of storing and returning evidence years after its seizure. In some cases the courts order return of evidence containing contraband, and often impose arduous duties on the unit personnel that are more akin to what a computer technician at a private shop would perform under contract than what law enforcement personnel should do to accommodate the owner of evidence to facilitate its return (Ferraro and Casey, 2004a).

The tension between forensic science and investigations

Issue 1: expert examination versus investigative review

Established computer crime units are beginning to feel pressure to become accredited. Accreditation schemes for laboratories parallel those used for hospitals, universities and police departments. There are general directives that apply to the entire laboratory and there are particular standards that apply to specific disciplines such as serology and document examination. Some of the standards are mandatory and some are elective. In order to maintain accreditation, labs must conform to a percentage of the essential standards and a certain level of important standards.

An emerging issue is the potential difficulty that some units that house both forensic examination and investigations have with accreditation standards. Generally, lab accreditation schemes require

E-mail address: mfer.ccu@snet.net (M.M. Ferraro).

[1] M.S., Northeastern University, J.D., University of Connecticut School of Law, Certified Information Systems Security Professional.

[2] J.D., Western New England School of Law.

[3] United States Department of Justice Office of Juvenile Justice and Delinquency Prevention. There are hopes that an additional four task forces will be added in the near future.

[4] Ferraro and Casey, Ferraro, Monique, "An Argument for Uniform State Long-Arm and Full Faith and Credit Provisions Regarding Compulsory Process for Information Held by Communication Service Providers" (tentative title) as yet unpublished, available from the author (2004).

1742-2876/$ - see front matter
doi:10.1016/j.diin.2004.01.004

a system of technical and administrative review of examination reports. Examiners must follow established procedures and document their findings. The lab must conduct proficiency testing of examiners. Testing can be internal as well as external and use blind and/or open samples with results that are unknown to the examiner but known to the test administrator. Additionally, examiners must pass competency examinations in each area in which they will perform examinations. With regard to computer forensic examiners, it means that they must be competent in each software and hardware tool they use. Finally, examiners must possess certain minimum academic credentials and training. The standards applicable to computer laboratory personnel require that examiners have at least a Bachelor's Degree with science courses (Ferraro and Casey, 2004b).

Established computer crime units and Internet crimes against children task forces have not received accreditation requirements enthusiastically. For many who work in this area, the requirement of a bachelor's degree could force them out of working in the computer crime field. Other objections go to the basics. First, many investigators believe that examining a computer system for evidence is not a matter for a "forensic scientist," but within the realm of an "investigative review of the evidence." It may seem like a minor distinction to some, but the entire future of this emerging field hinges on which direction the law enforcement community takes.

One does not have to be clairvoyant to predict that computers will be ubiquitous in nearly every sort of crime soon enough. If we set the standard such that we expect a forensic scientist to conduct an examination in every computer related crime, the demand for computer forensic scientists will be enormous. Every law enforcement agency will either have a laboratory of its own or rely upon a computer forensics laboratory to process its evidence. Unless the world is preparing to meet the demand for forensic science services that outstrip the meager resources we now have, some alternative will be necessary.

Full-blown forensic examinations are usually unnecessary. This is particularly so when the suspected criminal activity involves only a small portion of the storage media. For example, in child pornography possession, an examination looking for questionable images should be sufficient to obtain the necessary evidence to support a criminal investigation and possible prosecution. The lengthy process involved in a forensic examination, which requires duplicating all seized media, outlining the system setup and reviewing all of the files is more than what is necessary to prove that there were images of child pornography held in storage (see Casey, 2004 for details on the examination process).

Another example would be of a "traveler" who engages in online chat with the intended victim. When he travels to the prearranged spot, police arrest him. Some agencies conduct full forensic examinations of the suspect's hard drive, the victim's computer and execute search warrants for Internet service provider records as well. This practice expends resources on a misdemeanor or low-level felony that are typically used in a homicide investigation. Rather than expend the resources on the multiple forensic examinations, a printout of the chat logs together with the testimony of the investigating officer to authenticate it may be sufficient to prove that the communication took place. Of course, the scope of the forensic examination is an issue ultimately determined by the prosecutor (hopefully she will take into consideration the sound advice of forensic examiners and investigators).[5]

It is easier to train existing personnel than to recruit candidates who already possess the sought after skills. For that reason, law enforcement agencies have mostly opted for training existing personnel to perform computer forensic examinations. While this approach has been expedient, there are problems with it. One problem is that police officers have a relatively high turn over rate. Sworn officers often have to work only 20 years before they are eligible to retire, as opposed to civilian employees who usually need to work 30 or more years before they may retire. Civilians also are less likely to rotate out of the examination position because they make a commitment to being a forensic examiner rather than a police officer. In order to advance in rank, police officers usually cannot stay in one unit or division for long, due to a limited career ladder.

Another problem with training police officers to do forensic examinations of computer systems is that they may not possess the education and training necessary to qualify them as expert witnesses. The lack of formal university education is not a problem unless the examiners work in a laboratory seeking accreditation or the defense makes it a problem, but it is a factor. If the defense expects the computer forensic examiner to qualify

[5] For guidance in this area, see *United States vs. Tank*, 200 F.3d 627 (2000) and Cobb, J. Allen 39 Brandeis L.J. 785, 'ARTICLE: Evidentiary Issues Concerning Online "Sting" Operations: A Hypothetical Based Analysis Regarding Authentication, Identification, and Admissibility of Online Conversations—A Novel Test for the Application of Old Rules to New Crimes' (Summer 2001).

at the level that a DNA examiner presents, it would be nearly impossible for most examiners. However, the real issue is whether the computer forensic examiner needs to be qualified as an expert.

A primary reason to qualify a witness as an "expert" is so that she may offer her opinion in a court or other legal proceedings. Computer forensic examiners do not need to offer their opinions. Rather, they offer testimony as to the fact—what they did and what they found. They do not perform "tests." Either the evidence is there or it is not. There is nothing questioned for the technician to interpret.

Even when the evidence in question are digital images depicting what *appears* to be child pornography, the examiner testifies as to what he saw in fact. The examiner does not, nor should he, testify as to whether the images depict "child pornography." Child pornography is a legal determination. Only the finder of fact may decide the ultimate issue. In these cases, the ultimate issue is whether an image or set of images depict child pornography. The fact finder makes the legal conclusion by comparing the evidence presented to the elements of the crime.

Still another problem related to using police officers in a forensic science function is the expense of maintaining their police credentials and retirement. Often police officers must maintain their certification by attending in-service training and qualifying with a firearm. Police officers in many jurisdictions have specially equipped cars and other equipment like radios, bulletproof vests and similar items. If the officer performs forensic examinations of computer systems and does not exercise her law enforcement authority, the money expended on maintaining the police certification and equipping her for enforcement duties may be challenged as fiscally inefficient.

Another consideration is that new computer forensic tools are required as technology advances. Police officers cannot keep pace with the evolution of technology. Their role is reactive, not proactive. There is a great need for forensic scientists to develop tools and tactics to retrieve and preserve evidence from emerging and complex technologies. Networked environments require expertise that the average patrol officer or detective cannot maintain. Computer forensic experts should be responsible for obtaining data from networked environments. Intrusion investigations require sophisticated log analysis that one could not expect the average police officer to conduct. We need scientists to pioneer methods of extracting evidence and ensuring its stability and integrity.

This is a critical time for mature units. Some units have hired civilian examiners and have police officers working by their side. Still others maintain the forensic examination and active investigation functions within the same unit. One approach is to split the forensic and investigative duties in mature units.

Making the split: the lines of separation of responsibilities must be well planned

Mature computer crime units could split forensics from investigations. Units that have consolidated forensic duties find that the turnover time immediately improves. It makes duties more straightforward and physically separates the disciplines to facilitate record keeping. Many computer forensic laboratories limit their activities to retrieving and duplicating the evidence and returning it to the investigator for his review.

Where the investigative and forensic functions are split, it is essential to nurture a strong training component. New tools and techniques for seizing new technologies must be evaluated by forensic scientists, evaluated by the appropriate legal and policy personnel and passed to investigators quickly. Police officers both in computer crime and Internet crimes against children units require up-to-date training. Ideally, these police officers should pass their knowledge on to other police officers. Task forces serve the purpose of passing on valuable technology investigation techniques, protocols and best practices. Task forces foster mentoring, which encourages investigators to learn the proper way to search through evidence. In cases that require extensive forensics or network examination, lab personnel can preserve the evidence and turn it over for investigative review. Only a few most complicated examinations should require the expertise of a forensic examiner.

Participating in a task force would offer new computer crime investigators the experience of investigating other similar crimes and the benefit of the experience of his task force co-workers. Over time, search and seizure of computing devices will be as second nature to police officers as securing narcotics. Until that time comes, police with the necessary training and experience should conduct searches, and they should teach other officers how to do it.

The timing of the split of forensics and investigations is important. When a unit first begins, it is difficult to split the functions because personnel and expertise are limited. When the unit becomes more mature and the lines begin to split on their own, then administrators know it is time to make the split. The division will most likely be hastened

by professional and academic discussions and new policy directions explored by investigators. Whatever the impetus, where there is increasing tension between the disciplines, there is a message being communicated to administrators that should be heeded.

The Electronic Communications Privacy Act: clear as mud

Issue 2: continuing confusion over state jurisdiction and proper legal process in criminal matters under the Electronic Communications Privacy Act

One of the first issues computer crimes investigation units face is how to obtain information from Internet service providers (ISPs).[6] Information sought from ISPs falls into three categories: subscriber information, transaction data and content of communications. Working at the state level, training and reference materials prepared for generic use or for federal authorities do not address the needs of local officers. Investigators and prosecutors ultimately learn of the Electronic Communications Privacy Act (ECPA). The ECPA is the federal law that governs what information investigators may obtain from ISPs and what legal process they must use to get it. One might think that the federal law would help to simplify and streamline the process of obtaining information from ISPs. Unfortunately, this has not been the case. In fact, there is substantial confusion regarding how state and local authorities should properly obtain ISP information. This section briefly reviews the law, discusses the issue and offers a recommended solution.

Under ECPA, there are three levels of information held by ISPs.[7] Each level of information has a protected privacy interest. The more privacy afforded to the information, the higher the standard required for law enforcement officers to obtain the information. In order to obtain subscriber information, that is, the name, address and credit card information a person uses to establish an Internet access account, ECPA requires a subpoena. To compel disclosure of transaction information, such as the times and dates someone was logged onto his account, a government attorney must apply for a court order.[8] The government may only obtain the content of email with a search warrant.[9,10]

There are really two issues. The first is that some state and local jurisdictions misinterpret ECPA as creating long-arm jurisdiction where it clearly does not. The second issue is that police are not properly executing search warrants for Internet account information.

A state has jurisdiction over the people present within its boundaries. When a state must obtain jurisdiction over a person outside of its borders, it may do so only if authorized by a statute. Statutes that allow a state to reach beyond its borders are called "long-arm" statutes.[11] Most states have long-arm statutes that relate to civil jurisdiction and service of civil process. Quite often, the statutes provide that the courts "of this state may exercise jurisdiction on any basis not inconsistent with the Constitution of this state or of the United States."[12]

The United States Constitution restricts states from exercising unreasonable jurisdiction through the Due Process Clause (Scoles and Hay, 1992). The states may exercise jurisdiction over foreign corporations, such as ISPs, either with the corporation's consent or by virtue of the extent to which the corporation does business in the forum state.[13] If a state has a long-arm statute that allows it, and an ISP has sufficient contacts to the state or consents to the state's jurisdiction, the state is on solid constitutional ground when issuing

[6] For ease of reading, we refer to ISPs, but we also intend to include electronic communication services and remote computing services.

[7] In this section, we only address information held in storage for less than 180 days.

[8] As provided by 18 U.S.C. 2703(d).

[9] For a comprehensive discussion of ECPA and the issues detailed here, see Ferraro and Casey (2004a) and Ferraro, "An Argument for Uniform State Long-Arm and Full Faith and Credit Provisions Regarding Internet and Telephone Subscriber Subpoenas, Court Orders and Search Warrants" as yet unpublished, available from the author (2004).

[10] Contents of Electronic Communications in a Remote Computing Service. (1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or (ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

[11] The first long-arm statutes were enacted to enable civil suits against foreign corporations and out-of-state drivers who could not be personally served in the state (see Scoles and Hay, 1992).

[12] Calif. Code Civ Proc. Sec. 410.10 (2003).

[13] *International Shoe Co. vs. Washington*, 326 U.S. 310 (1945), *World Wide Volkswagen Corp. vs. Woodson*, 444 U.S. 286 (1980).

subpoenas or court orders compelling production of information from the ISP.

Search warrants differ from subpoenas and court orders compelling production of information in important respects. First, a search warrant is a judicial authorization for government agents to conduct a search. This concept is rooted in the common law and the United States Constitution. The Fourth Amendment of the Constitution provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, 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." State constitutions contain similar provisions, and in many states, the restrictions placed on government searches by states are stricter than the federal provisions.[14] When it comes to searching for ISP records belonging to a single subscriber, the "search" is nearly always conducted by ISP personnel—not police. This practice comports with the intent of Constitutional protections against unreasonable, overbroad searches, but state statutes generally require that only certain authorities enumerated by the statute conduct the search.

The proper procedure for one state to obtain and execute a search in another state is to solicit the assistance of the law enforcement agency with physical jurisdiction over the ISP. Using information from the requesting state, the state with jurisdiction applies for a search warrant and executes it at the ISP. Two factors complicate this process. First, three states—California, Minnesota and Florida—have statutes that recognize the validity of search warrants for ISP information. Second, police officers are not "executing" ISP searches.

California, Minnesota and Florida have statutes that recognize the validity of search warrants for information held by ISPs.[15] For many jurisdictions, this eases the burden of locating a contact in the police department with jurisdiction and clearing many administrative hurdles. A problem that has emerged is that some judges absolutely will not sign search warrants that will be executed outside of their jurisdiction. Even after the affiants produce the California, Minnesota or Florida statute, there are judges who continue to refuse to authorize the search. An officer faced with this usually has to let the investigation go because when he requests assistance from the state with jurisdiction, they tell him to get a search warrant from his state.

Of greater concern is that police are not executing ISP search warrants. Instead of actually executing the warrant, police routinely fax the warrant to the ISP, civilian personnel locate the records and fax them to the requesting officer. Many state statutes require that police officers execute search warrants.[16] The reasoning behind these statutes is to ensure that officers who have training in search and seizure and are bound by oath to uphold the law conduct searches. Of course, it is practically impossible for police to execute a search of an ISP for information. At the very least, officers would have to ask ISP personnel to assist them.

One might be tempted to argue that the search warrant is "executed" when the officer faxes it to the ISP. That is not intellectually or factually honest. A contract may be "executed" upon signing, but a search warrant is "executed" when police actually conduct the search. One may also be tempted to look to the language of the ECPA.

The ECPA states that "[a] governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—(A) *obtains* a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant."[17] Note that the statute explicitly refers to "obtaining" the search warrant, not "executing" the search warrant.

[14] Conn. Const. Art. I, § 7 (2003); *State vs. Kimbro*, 197 Conn. 219 (1985).

[15] Cal. Penal Code §1524.2 (2003), Fla. Stat. § 92.605 (2003) and Minn. Stat. § 626.18 (2003).

[16] See, for example, Connecticut's search warrant statute provides, "[t]he warrant shall be directed to any police officer of a regularly organized police department or any state policeman or to a conservation officer, special conservation officer or patrolman [ ]. The warrant shall state the date and time of its issuance and the grounds or probable cause for its issuance and shall command the officer to search within a reasonable time the person, place or thing named, for the property specified." C.G.S.§54-33a(c). New York's statute states [a] search warrant must contain: 1. the name of the issuing court and, except where the search warrant has been obtained on an oral application, the subscription of the issuing judge; 2. where the search warrant has been obtained on an oral application, it shall so indicate and shall state the name of the issuing judge and the time and date on which such judge directed its issuance; and 3. the name, department or classification of the police officer [ ] to whom it is addressed. "NY CLS CPL § 690.45 (2003). See also *U.S. vs. Bach*. 310 F.3d 1063; 2002 U.S. App. LEXIS 23726 (8th Cir. 2002); rehr den'd 2003 U.S. App. LEXIS 141 (2003); cert den'd, 123 S. Ct. 1817; 155 L. Ed. 2d 693; 2003 U.S. LEXIS 3174; 71 U.S.L.W. 3667 (2003).

[17] 18 U.S.C. § 2703(c) (2003).

Although the language is plain, the argument is flawed. If ISPs had to produce information upon obtaining search warrants, the whole process of serving the warrant or executing it would be unnecessary. Just because the statute does not state how police must execute the warrant does not mean that simply obtaining a warrant is sufficient.

The Eighth Circuit Court of Appeals dodged the issue when it decided *United States vs. Bach*.[18] The court avoided suppressing evidence obtained in violation of state and federal search warrant rules. Police faxed a Minnesota search warrant to Yahoo! in California seeking account information. Bach was party to an incriminating online conversation with a minor. After the Minnesota investigator faxed the search warrant to Yahoo!, Yahoo! personnel executed the search and returned the requested data to the Minnesota investigator. Under Minnesota law, police officers must execute a search warrant. In the Bach case, no law enforcement officer was present in California during the search. The court did not reach the question whether the Minnesota law requires that a *Minnesota* officer be present or actually execute the search. Pursuant to the information obtained in the first search, police executed a search warrant at Bach's home where they found child pornography and additional evidence of Bach's enticement of minors to engage in sexual activity. Bach moved to suppress evidence from both searches. The District Court suppressed evidence from the Yahoo! search because it held that the Minnesota officer violated the law governing execution of a search warrant but upheld the second search. The government appealed the District Court ruling and the Eighth Circuit Court of Appeals reversed.[19]

The court held that the federal search warrant statute does not codify the Fourth Amendment to the Constitution. If it had, the court would have suppressed the evidence. In dicta, the court cited that Congress created a privacy interest in email that under *Smith vs. Maryland* would probably otherwise not exist. The court upheld the Yahoo! Search's reasonableness, citing a number of state court holdings that approve civilian searches for bank records, software and other similar matters.[20] This holding works for this specific case, but it would not work in a jurisdiction that follows a *fruit of the poisonous tree* rule. A jurisdiction with a fruit of the poisonous tree rule would suppress all evidence obtained illegally. Some jurisdictions do not even allow a good faith exception. The court does not admit evidence obtained in violation of the law. The intent behind the strict suppression tactic is to deter cavalier search and seizure.

The information governed by ECPA is often essential to criminal investigations. The states must have settled methods for obtaining the information from out-of-state ISPs that is consistent with state and federal law as well as expedient for law enforcement investigators. After all, facilitating investigation of crimes is a most compelling state interest. If the states cannot obtain the information necessary to investigate crimes, we may as well surrender the Internet to lawlessness.

States could enact uniform ISP long-arm statutes

States should revisit their long-arm statutes to evaluate whether police have the ability to compel the production of information from ISPs using the least intrusive lawful method possible. The states should consider drafting a uniform law for each state to enact. Uniform long-arm statutes would help to ensure that the correct legal processes are used to obtain the sought after information. The states should consider entering into an Interstate compact regarding government access to stored electronic communications. Properly drafted Interstate compacts can facilitate relations among the states and smooth operations.

The states could enact uniform legislation that specifically authorizes courts to issue "warrants" supported by probable cause directed to civilian personnel to produce information held in electronic storage

As previously mentioned, some state courts have made exceptions to the strict requirement that police must execute search warrants, and have

[18] *U.S. vs. Bach*. 310 F.3d 1063.

[19] No. 02-1238 (8th Cir. 11/18/2002).

[20] Civilian searches are sometimes more reasonable than searches by officers. Harris vs. State, 401 S.E.2d 263, 266 (Ga. 1991) (stating that a dentist may execute a search warrant for dental X-rays and impressions); Schalk vs. State, 767 S.W.2d 441, 454 (Tex. App. 1988) (providing a search by a civilian software expert more reasonable than a search by an officer because the officer lacked knowledge to differentiate a trade secret from a legitimate computer software program), cert. denied, 503 U.S. 1006 (1992); State vs. Kern, 914 P.2d 114, 117—18 (Wash. Ct. App. 1996) (indicating that it is reasonable to delegate search of bank records to bank employees, even when a police officer was not present during the search). Civilian searches outside the presence of police may also increase the amount of privacy retained by the individual during the search. See Rodriques vs. Furtado, 575 N.E.2d 1124 (Mass. 1991) (body cavity search done outside presence of officers); Commonwealth vs. Sbordone, 678 N.E.2d 1184, 1190, n.11 (Mass. 1997).

allowed civilians to do so. This exception is sensible, but it is in derogation of the plain language of many state statutes. What happens in reality is that police justify the need to obtain stored communication content by detailing the probable cause to a judge who issues a search warrant. Instead of executing the search warrant, police fax or serve the warrant and the ISP does the searching. ISP personnel produce the records.

States need to explicitly authorize courts to issue a different type of warrant. Traditional search warrants require that police officers execute them. Subpoenas are ill suited to the task because the ECPA mandates the circumstances in which officers need a search warrant to compel production of information. The state legislatures could authorize the courts to issue a hybrid warrant that combines the essential elements of subpoena and search warrant while complying with the requirements of the ECPA. State legislation is required if the state does not already authorize a search warrant to be executed outside the state by non-sworn, non-government personnel.

Such action is not without precedent. The Privacy Protection Act serves as an example. In order to obtain records held by newspapers and publishers pursuant to the Privacy Protection Act (PPA) police must use a subpoena.[21] The reason Congress enacted the PPA was that police executed a search warrant at a California university student newspaper in search of information that would assist in identifying suspects in an investigation.[22] The newspaper objected to the search, but the courts upheld it, finding that the police did exactly what they should have. Congress enacted the PPA to ensure that instead of conducting a search of publishers' files, police give the publisher the opportunity to produce them. This practice protects the privacy of individuals who are not the subject of the investigation.

Dealing with large volumes of evidence and returning it pursuant to orders of the court

Issue 3: volume and disposition of evidence

Computer related crimes languish in the criminal justice system. From the point of evidence seizure to the moment the evidence is returned to a defendant is often between three and five years or even more. Depending on the number of cases processed by the particular unit, the amount of evidence accumulates quickly. Disposing of evidence is an arduous process, particularly for units that do not employ a full time evidence officer. The volume of evidence is mounting in those units that have been operating for a few years. When policy or statute requires that the government maintain the evidence until a case is finally adjudicated, the problem is increasingly worrisome given the length of time from inception to disposition in these cases.

Orders of the court that mandate either impossible or very time-consuming procedures further impede the effective handling of evidence. This phenomenon seems to be associated with the age of the computer crime or Internet crimes against children unit. When cases reach a certain stage in the criminal justice system, the court issues orders to deal with the evidence seized from the owner. Courts have ordered various approaches to dealing with digital evidence. Some examples include: return computer systems that likely contain contraband; destroy computer systems; excise contraband but keep other data intact on a computer system and return it to the owner of the system. While in most instances simply calling the prosecutor or court clerk and informing them about the difficulty of complying with the order resolves the matter favorably, in other cases it is not as simple.

Agencies should avoid returning property that contains contraband at all costs. When agencies return digital storage media that potentially or actually contains contraband, they facilitate the continuing commission of the crime of possessing child pornography (Ferraro and Casey, 2004a).[23] Of course, only a fact finder may make the legal determination of whether material alleged to contain child pornography is "contraband." This complicates matters because if the material is *not* child pornography, the owner of the material is entitled to its return unless forfeiture is part of his sentence or he consents to it.

Return of evidence that may contain contraband comes up in a number of different ways. Prior to even examining the evidence, the case may be dropped, nolled or dismissed. In those cases, the defendant is usually entitled to the return of the

[21] 42 U.S.C. §2000aa.

[22] *Zurcher vs. Stanford Daily*, 436 U.S. 547 (1978).

[23] We recognize that the issue of disseminating evidence prior to adjudication is a separate, though related and equally vexing a problem. California recently enacted a law that strictly limits the distribution of evidence containing contraband. Cal. Penal Code §1054.10.

evidence without any limitation. Because no examination of the evidence has yet been conducted, it is not possible to tell whether the agency is returning contraband. Next, as part of a negotiated plea agreement, the parties may agree to return the evidence. In this situation, the potential return of contraband is often simply overlooked. Finally, at the final disposition of a case a judge issues orders to return the evidence or otherwise dispose of it.

A favored approach is to encourage the court to issue orders favoring destruction rather than return of storage media. The best way to ensure that orders concerning the disposition of digital evidence are reasonable is through training. Judges, prosecutors, defense attorneys and law enforcement officers require training in fashioning effective orders regarding computer and digital evidence.

Whenever permissible, destroy media suspected of storing contraband

Destruction is the most cost-effective and secure method of ensuring that law enforcement does not contribute to continued criminal activity by returning contraband. There are alternatives, but they are not as acceptable. One alternative often ordered by judges is to "delete" the contraband and return what is left. This is the least attractive of the alternatives for a few reasons. First, personnel would have to conduct a complete forensic examination in order to identify the contraband. Next, the identified "contraband" would have to be "wiped." (We all know that simply "deleting" the files would not be effective because the defendant could simply "undelete" them.) Finally, to ensure that he effectively excised the contraband, the examiner would have to perform a second complete forensic examination of the media. All of this "evidence amelioration" takes quite a lot of valuable time. The human resource expense far outweighs the expense of buying a brand new hard drive or removable storage media.

Another alternative is to wipe the entire storage media. This is also popular among judges. Wiping media is almost as time consuming as excising contraband. In order to ensure that the contraband is completely eliminated, one must perform a second examination of the media.

Simply destroying the storage media is the most efficient and cost-effective approach. Hard drives and removable media are cheap. The inconvenience and expense to the defendant would be the cost of a new hard drive or media and the time spent to reinstall software. In jurisdictions that authorize it, the jurisdiction may reimburse the defendant for the cost of the lost media. We find that the biggest obstacle to getting judges to issue reasonable orders regarding evidence return is in accessing the judiciary, defense and prosecution for training in this area.

Develop and implement law enforcement, prosecutor, defense and judicial training concerning appropriate court orders regarding return of computer systems and digital evidence

Short of mandating that courts issue certain orders regarding evidence return, the most effective alternative is to introduce the issue and offer solutions in training. In-service programs, online tutorials and articles in professional publications should address appropriate orders and measures to take when returning evidence that may contain contraband. Just as a judge would hopefully never order the return of a woman's handbag that still contains an ounce of marijuana, a judge should not order the return of an individual's computer whose hard drive may contain images depicting child pornography.

Conclusion

This article explored three emerging issues facing established computer crime units. First, the tension between forensic science and investigations was discussed. Pressure to become accredited conflicts with practical considerations of investigators. This article examined splitting forensics from investigations and discussed some of the many considerations administrators should weigh when parsing out duties.

Second, the article examined jurisdictional and practical search and seizure issues spawned by the Electronic Communications Privacy Act. We explored the prospect of developing uniform long-arm statutes for states to enact. Further, we discussed the possibility that the states enter into an interstate compact to facilitate obtaining information from ISPs. The article talked about uniform state laws to allow a hybrid warrant that would allow judges to "warrants" that could be executed out-of-state by non-police officers who work for electronic communication providers.

Third, we discussed returning evidence that may contain contraband. Ill-informed orders to

dispatch the evidence often require personnel to perform functions that are beyond their government responsibilities. Judges, prosecutors, defense attorneys and law enforcement officers require training in the most expedient and fair methods of returning evidence that may contain contraband. The article described several approaches to dealing with digital evidence.

These three issues are the primary concerns seen by units with at least five years experience. The future is uncertain and holds challenges that we may not even anticipate. This inaugural issue of this Journal signals a beginning of a profession attempting to come together to solve our mutual problems. We have hope now, that this new medium will be an indispensable resource to us all in solving our current issues and the challenges yet to come.

References

Casey Eoghan. Digital evidence and computer crime. 2nd ed. Boston, MA: Academic Press; 2004.

Ferraro Monique, Casey Eoghan. Investigating child exploitation: the internet, the law and forensic science. Boston, MA: Academic Press; 2004a.

Ferraro Monique, Casey Eoghan. Investigating child exploitation: the internet, the law and forensic science. Boston, MA: Academic Press; 2004b.

Scoles Eugene, Hay Peter. Conflict of laws. 2nd ed. St. Paul, MN: West; 1992 [section 8.32].