PAPER:

CAUGHT IN THE MIDDLE: WHETHER TO SEEK HELP WHEN THE ORGANIZATION IS THE SUBJECT OF AN INFORMATION TECHNOLOGY ATTACK

By **Joseph J. Schwerha IV,** M.S., J.D.

Information technology is utilized in almost every facet of the modern business enterprise.[1] Unfortunately, when so many assets of a business are solely in electronic form, businesses sometimes find themselves trying to recover when someone within their organization has abused information technology to the detriment of the enterprise.[2]

When put in such a situation, businesses in the United States are faced with a multitude of laws and regulations that affect the discovery and acquisition of digital evidence to support its cause. Indeed, the victims of cybercrime will probably have the choice of pursuing remedies through the public or private sectors, or both. This choice usually is presented practically in the form of whether to request a law enforcement agency to provide assistance, or whether to employ alternative specialist assistance to gather digital evidence and pursue private remedies through the civil courts.[3] There are great differences and implications associated with deciding which choice to make.

This paper provides a simple discussion of the various methodologies that may be used to gather digital evidence through civil or criminal procedure under United States law. To facilitate this discussion, a common scenario is offered to help delineate the differences between seeking digital evidence by way of criminal versus civil procedures. An overview of the basic methodologies that can be used to gather digital evidence under criminal and civil procedures will follow the sample scenario. Finally, an analysis will be provided of the choices faced in the sample problem, together with some general conclusions.[4]

The sample case

Imagine that you are the regional manager of a high tech company. You have a substantial sales force, which you depend upon to solicit your customers. Late one afternoon, you receive a report from Jim Smith, your East Coast Sales Manager, that Lou Cipher, your West Coast Sales Manager, is possibly stealing company information. Jim observed Louis copying customer databases on to a 'thumb drive'.[5] Simultaneously, you receive an e-mail from Louis, resigning with immediate effect, and going to work for Bad Guys, Inc., a direct

[1] *Please note that this article is basic in nature and not meant for the experienced American practitioner.*

[2] *While not all information technology abuse is cybercrime, it is suggested that all cybercrime is information technology abuse by its very nature. For instance, an employee may extensively surf the internet at work and therefore abuse technology to his own benefit. However, that is not generally considered to be a cybercrime. However, all cybercrimes would generally be considered an abuse of information technology. Thus, reference may sometimes be made to cybercrime instead of information technology abuse. When such a reference is made, the reference will include information technology abuse.*

[3] *For example, 18 U.S.C. Section 1030 provides both a civil and criminal cause of action. Thus, someone could seek criminal remedies by reporting the incident to a law enforcement agency. Alternatively, they might not report it to a law enforcement agency, but pursue a remedy through the civil courts.*

[4] *A sample case is used in large part to provide a practical backdrop upon which to view the choices that a cybercrime victim might make under the circumstances set out. However, it is useful to outline a particular case, because it is impossible to discuss all the permeations in cases where someone is seeking digital evidence. This paper does not seek to discuss all possible situations and provide concrete answers as to involve law enforcement or to not involve law enforcement. Rather, the discussion focuses upon tools that are available under both criminal and civil procedures to illustrate the major differences between the two types of remedy.*

[5] *A thumb drive is also known as a flash drive. They are sometimes referred to as 'thumb drives' because they are about the size of a person's thumb.*

competitor. Your sales on the West Coast are dependent upon your customer list and the specialized pricing system that your company has developed over the past five years. If Louis had copied them and left to go to work for a competitor, it would take years for your company to recover, if it was possible to recover. In this situation, there are several possible criminal and civil violations. Thus, it is possible to pursue a remedy though the civil courts and to report the incident to a law enforcement agency. The options available and the general arguments that apply to each are discussed below.

Pursuit of remedies by reporting the incident to law enforcement

In the United States, criminal charges may generally only be pursued by a public official, acting on behalf of the public.[6] Crimes are basic societal rules, the breach of which makes society the victim. The end result is that the tools available to law enforcement, be it Federal, State or locally based, may not be used by private parties. This means that where a decision is made to call in a law enforcement agency in the United States, the agency will have specialized tools available to them, and they may only be used under the rules of criminal procedure.[7]

Under criminal procedure, the methodologies used will depend upon who possess the evidence sought. If the target of the investigation (the suspect) possesses the evidence, then there are a number of legal mechanisms available to law enforcement investigators that can be used to gather evidence from them. However, if the evidence is in the possession of third party, then other procedures must be utilized.

If the evidence is held by a third party, a law enforcement investigator can use the following during the investigation: the subpoena;[10] a 'd' order;[11] a search warrant;[12] and a general investigation. Each one will be discussed in turn.

Under the Federal Rules of Criminal Procedure, the party may subpoena digital evidence held by third parties in certain situations.[13] Precisely what digital evidence a law enforcement agency may subpoena and legally require the respondent to provide, is greatly dependent upon how the particular evidence is viewed within the provisions of the Electronic Communication Privacy Act (ECPA).[14] For instance, it may not be necessary to request a subpoena in respect of the content of an e-mail, so much as to know the name of the party who had registered the nickname within a particular ISP system, a subpoena can be used.[15]

One of the more under-used methodologies for obtaining physical evidence from third parties is by a court order issued pursuant to 18 U.S.C. Sec. 2703(d). To obtain such an order, a law enforcement official must offer 'specific and articulable facts showing that there are reasonable grounds' to believe the information sought is 'relevant and material to an ongoing criminal investigation.'[16] In order to obtain an order for digital information under this section,[17] the applicant merely has to show that the required information comes within the scope of ECPA, and that pursuant to the language therein, can be obtained pursuant to a 2703(d) order, and is relevant and material to the investigation at hand. While this order is under-used in general, digital evidence specialists routinely utilize this order within the federal system because it enables the holder of the order to obtain digital evidence, such as subscriber information, without having to show probable cause, as with a search warrant.

Law enforcement agencies may also use search warrants to obtain digital evidence held by third parties. Generally, a search warrant can be obtained if there is a fair probability under the circumstances that either evidence of a crime or contraband may be found at the person or place to be searched at that time.[18] At the Federal level, this is sometimes a challenge, and federal prosecutors are usually less likely to pursue search warrants because their actions tend to be obtrusive on a practical level. However, at state level, a search warrant

[6] *At the Federal Level, it is the United States Attorney General, generally through one of his or her assistants. At the State level, that public official is the State Attorney General. At the local level, that official is the District Attorney for that particular political subdivision.*

[7] *The laws and rules under Federal law will be referred to, since these laws generally apply across the United States. However, there are usually State equivalents, and these will be referred to as well. However, the reader should not assume that a particular law or rule is only available at the Federal level if the state equivalent is not mentioned.*

[10] *Fed. R. Crim. P. 17.*

[11] *18 U.S.C. § 2703(d).*

[12] *Fed. R. Crim. P. 41.*

[13] *Fed. R. Crim. P. 17(c)(1).*

[14] *ECPA is a Federal statute that sets forth rules for disclosure of certain electronic information held in the possession of third parties, such as internet service providers. See 18 U.S.C. § 2510 and following.*

[15] *Please note this comment reflects the Federal law in the United States, and the Federal law is only be available to federal law enforcement agencies. In the vast majority of cases, the state or local law enforcement agencies would be involved, and they might only operate under their particular state law, and may or may not have power to issue a subpoena. This would be evident by looking at each individual state law to determine whether or not the state has the power. For instance, in Pennsylvania it is questionable whether or not law enforcement agencies have subpoena power prior to the filing of an action to obtain individual evidence in any particular investigation. See Pa. R. Crim. P. 107.*

[16] *See 18 U.S.C. § 2703(d).*

[17] *The scope information obtainable under 18 U.S.C. § 2703(d) is set forth in sections 'b' and 'c' of section 2703.*

[18] *See Comm. v. Lloyd, -- A.2d. --, 2008 WL 2043199 (Pa. Super. 2008) and Com. v. Otterson --- A.2d ----, 2008 WL 1874567 (Pa.Super., 2008) for examples of defining probable cause and the standard for the issuance of search warrants under Pennsylvania state law.*

is readily obtainable.[19]

Alternatively, if the evidence is not held by a third party, but instead is held by the suspect (Louis Cipher in the sample case), then a search warrant is appropriate. Where a search warrant is issued, it is possible to search for and seize whatever evidence is listed in the search warrant itself. In the sample case, it might be possible to obtain a search warrant for all digital storage devices owned or possessed by Louis Cipher. If successful in obtaining a search warrant, it is possible to search for and forcibly seize the evidence described in the warrant immediately. This mechanism can be much more effective than any other means of obtaining digital evidence that might be difficult to obtain.

The general investigation is the last method to examine. For instance, if a third party that holds information is *not* open to the public, but holds e-mails or stores digital documents, the requirements of ECPA do not apply to that entity.[20] Therefore, the third party could provide the information to law enforcement voluntarily, should they desire to do so. Sometimes, it is also possible to by-pass the provisions of the ECPA by the terms of service that people may use. For instance, eBay has terms of service that allow for investigations by law enforcement agencies and agree to provide information to law enforcement agencies without the use of a formal court process to support such a request.[21] Such provisions can be a very valuable part of the acquisition and discovery of digital evidence.

While not a methodology to actually force someone to provide evidence to a law enforcement agency, another option that is available to law enforcement agencies is a notice to preserve under 18 U.S.C. § 2703(f), which reads as follows:

> (f) Requirement To Preserve Evidence.—
>
> (1) In general.— A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.
>
> (2) Period of retention.— Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

Under this provision, a law enforcement agency may notify the possessor of electronically stored information[22] to preserve that information in their possession for a period up to 90 days.[23] This is the typical procedure that a law enforcement agency would use to obtain subscriber information from an internet service provider.[24] It also allows for 90-day extension of the preservation, if is necessary. A law enforcement agency can use this procedure immediately to force the recipient to provide the electronically stored information, even though it might take time to obtain the relevant papers. This is an important power that is available to law enforcement agencies, and has no corollary in civil procedure.[26]

Benefits and detriments of utilizing criminal procedures

The best and clearest advantage of going to a law enforcement agency for help is that it is possible to obtain the most evidence in the quickest way by using the methods available under criminal procedure.[27] If third parties hold the electronically stored information, then it is likely that the provisions of 18 U.S.C. § 2703(f) can be used to preserve the data, and then legally force the respondent to provide such information through use of a subpoena, 'd' order, or search warrant.[28] Further, it is not necessary to consider the individual privacy

[19] *The only real value in obtaining a search warrant is the information the might be found, and, if it is good evidence for the prosecution, it will undoubtedly be challenged by the defendant, who will require the prosecution to show probable cause.*

[20] *See 18 U.S.C. § 2703.*

[21] *See http://pages.ebay.com/help/policies/privacy-policy.html#Disclosure.*

[22] *Please note that the target possessor of electronically stored information must be an electronic communication service or a remote computing service, as defined by ECPA, in order for 18 U.S.C. § 2703(f) to apply. 18 U.S.C. § 2703(f).*

[23] *18 U.S.C. § 2703(f).*

[24] *The United States Internet Service Provider Association provides the following summary of the general procedure utilized to obtain this sort of information from Internet Service Providers:*

'1. A law enforcement agent contacts the appropriate legal official at an Internet Service Provider (ISP), and requests in writing that the ISP preserve identified records or communications related to a particular person. (records or communications refers to subscriber information, credit card information, IP Addresses, and e-mails).

2. An ISP then preserves the identified records or communications that the ISP has in its possession on the date of the request that were requested by the law enforcement agent, and makes sure the information is not deleted for 90 days.

3. The law enforcement agent then obtains the proper legal process to gain access to the preserved records or communications within 90 days, and serves the legal process on the ISP.

4. The ISP then gives the law enforcement agent the records and communications requested to be preserved.' http://www.usispa.org/pdf/DataPreservationSystem.pdf.

[26] *It can be argued that sending out a notice to preserve ESI might be an equivalent. However, it is debatable. First, the notice to preserve only reminds the defendant of a duty that they already have. It does not, in and of itself, create a duty to preserve anything. Second, the notice does not carry the direct penalties that that a notice issued under 2703(f) possesses. Third, the 2703(f) notice is applicable to anyone who receives it, not just defendants.*

[27] *For example, even a search of the contents of a mobile telephone at a traffic stop was held to be lawful. U.S. v. Fierros-Alaverez, --F.Supp.2d.--, 2008 WL 1826188 (D. Kan. April 23, 2008).*

[28] *Joseph Schwerha, Cybercrime: Legal Standards Governing the Collection of Digital Evidence, (Kluwer Academic Publishers, June, 2004), Information Systems Frontiers 6:2, 133-151.*

interests of the custodian of such records, but rather the evidence can be obtained wherever it may be found within the powers provided by criminal procedure.[29] Finally, there is no additional cost, because law enforcement agencies do not charge for their services.

However, there are considerations that ought to be taken into account when deciding whether to approach a law enforcement agency. First, the investigation is conducted by the agency. Once a report is made to a law enforcement agency, the agency controls the progression of the investigation and prosecution. Second, the complainant loses control over the evidence. Once the police have the evidence in their possession, it cannot be used in civil proceedings until after the criminal prosecution is over. Nevertheless, the attractiveness of this option will ultimately be determined by comparison to the alternative: pursuit via civil litigation.

Pursuit of remedies through the civil courts

There are various methods that are available for obtaining digital evidence by way of civil proceedings under United States law. A summary of the most available and effective methodologies are set out below.

In seeking a remedy solely through civil proceedings in the United States, it will be necessary to hire people to investigate the evidence and take legal action. This would normally involve hiring a digital evidence specialist, as well as an attorney to file the action. The digital evidence specialist will be responsible for preserving and acquiring the evidence, whilst also attempting to preserve and acquire evidence held by a third parties. The preservation of physical evidence held either by the suspect (i.e. Louis Cipher) or by third parties can only be achieved by initiating action.[30]

Obtaining information quickly

Civil proceedings are often filed along with motions for a preliminary injunction, temporary restraining order and for expedited discovery. The motions for preliminary injunction and temporary restraining orders are used as an early mechanism against the defendant to do something or refrain from doing something. This is a temporary decision that may enjoin a party while and until the court considers the entire action at trial. The temporary restraining order can be used to temporarily restrain a party from the action complained of until a hearing on the motion for preliminary injunction hearing can be had. Such powers provide for immediate relief, but do not necessarily mean that all of the electronically stored information will be given up. It is possible to gain access to digital evidence more quickly by filing a motion for expedited discovery. Generally, however, a motion for expedited discovery is not granted unless the court intends to have a hearing on the motion for preliminary injunction.

General powers available in the civil courts

In general, in order to obtain information or electronically stored information from either the defendant or a third party under United States civil proceedings, the plaintiff may have recourse to: Deposition;[33] Interrogatories;[34] Request for admissions;[35] Request for Production of Documents or Inspection, or both,[36] and Subpoena.[37]

Using a deposition, the plaintiff is allowed to send an official notice to the defendant or a third party or both, to force them, under penalty of court order, to testify and have their testimony recorded.[38] The plaintiff may also demand that the defendant bring with them certain documents about which they will testify.[39] This may occur well before the trial, but normally months after the court action is initiated. The aim is for the plaintiff to obtain information relevant to their case and to pursue any remedies based upon the information that is produced as a result of the deposition. It can be very effective for obtaining electronically stored information.[40]

Under the Federal Rule of Civil Procedure 33, the plaintiff has the ability to ask written questions (the interrogatory) of the defendant, and the defendant only, and the defendant must answer the questions, providing they comply with the requirements of the rule. Defendants may, however, object to the form of the

[29] *For instance, while an individual employee generally has no right to privacy in e-mail retained on a company network, the analysis is not relevant in deciding whether or not to issue a search warrant. See Fraser v. Nationwide, 135 F.Supp.2d 623, 636 (E.D. Pa 2001)(In Pennsylvania, employee generally has no right to privacy in e-mails on company owned computer.).*

[30] *This is true, only to an extent. In actuality, the defendants themselves, but only defendants, are under a duty to preserve digitally stored evidence in their possession, or under their control once they are reasonably aware that litigation is imminent. Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 72–73 (S.D.N.Y. 1991).*

[33] *Fed. R. Civ. P. 30.*

[34] *Fed. R. Civ. P. 33.*

[35] *Fed. R. Civ. P. 36.*

[36] *Fed. R. Civ. P. 34.*

[37] *Fed. R. Civ. P. 45.*

[38] *Fed. R. Civ. P. 30.*

[39] *Fed. R. Civ. P. 30(b)(2).*

[40] *For instance, if the plaintiff is able to obtain an Order based upon a motion for expedited discovery, the plaintiff may be able to depose the custodian of electronically stored information from the defendant's new employer within a few days after filing the complaint. This would the plaintiff to determine where electronically stored information is held, so that the information can be used to present to the court. Discovery does not usually take place until the initial pleadings are complete. The pleadings in civil litigation in the United States comprise of a complaint, the response to the complaint and any subsequent responses. Fed. R. Civ. P. 7. After the pleadings have all been filed, which is commonly at least 90 to 120 days after the complaint is filed, the court action typically enters the phase when depositions may be scheduled.*

question, as well as what is asked for, and may answer the question on the assumption that the objections are valid. This means that information will be given to the plaintiff, but only after one or more lawyers have reviewed the responses, which tends to mean the plaintiff does not gain as much as they would prefer from undertaking such an exercise. Nevertheless, the interrogatory can be very valuable, even though it is not as effective as a deposition.

Another method of obtaining electronically stored information, in additional to discovery, is the request for admission. Under Federal Rules of Civil Procedure 26, a litigant can ask the defendant, and the defendant only, to admit certain statements. The request for admission is not very helpful in obtaining electronically stored information, as it is normally only utilized to establish very basic information. One example would be to request that the defendant admit its proper name.

Fourth, under Federal Rules of Civil Procedure 34, the plaintiff may request the court for an order to enable it to go on site to the defendant's place of work or residence to inspect evidence in their possession. Under certain circumstances, such an order can be extremely valuable, but recourse to such an order is not utilized often. Such action may only be taken when previously approved by the presiding court, and approval is rarely granted. However, courts sometimes will grant this extraordinary remedy when the plaintiff knows that the defendant may be trying to, or could destroy evidence in its possession once it becomes aware that legal action is under way. Under such circumstances, federal courts have ordered that a plaintiff be allowed to enter the defendant's premises and preserve evidence in the defendant's possession to prevent it from being destroyed.[42] Generally, it is very difficult to convince a judge in practice to issue such an order, because the underlying premise of the civil legal system in the United States is that the defendant will follow the rules of civil procedure and, therefore, will not destroy evidence in their possession

The second part of Rule 34 that is utilized in discovery allows for one party to request documents from the other party to the litigation.[43] Since this Rule was modified as of December 1, 2006, and it is also now utilized to permit a sampling of electronically stored information to establish if there may be any responsive information within the data provided for the purpose of the sample process.[44] Both of these uses are helpful in acquiring electronically stored information from the other party to the litigation; but, because the actions only take place after the filing of the complaint, and because they only apply to the other party to the case, they are not as effective as they otherwise could be.

The subpoena can be used to acquire documentary evidence (including digital evidence) from third parties.[45] Under this rule, the plaintiff can 'command each person to whom it is directed to' produce 'designated documents, electronically stored information, or tangible things' at a time and place of the plaintiff's choosing.[46] While the subpoena is valuable in obtaining digital evidence from third parties in civil litigation, it can only be utilized by parties during the time periods designated by the courts, and is subject to objections by the defendant.

Benefits of proceeding through civil proceedings

Clearly, there are significant differences with pursuing digital evidence through civil proceedings in comparison to pursuing criminal proceedings. The plaintiff has complete control over the process in pursuing a civil action. The aggrieved party is able to control what evidence they preserve, and how they preserve it. Furthermore, the plaintiff has a greater ability to control the speed of litigation, if litigation ever is filed at all. For example, if something embarrassing is found during the initial investigation, the plaintiff has the ability to simply forego further pursuit and not file an action. Conversely, if a law enforcement agency is invited to conduct an investigation control rests with the prosecuting agency.

There are disadvantages to taking civil proceedings. One of the main disadvantages is cost, because of the need to pay both the attorney and any consultants. Further, the speed at which information can be preserved is slow in comparison to the process of a criminal investigation. For instance, there is no general order similar in nature to a notice under 2703(f), whereby a third party or the defendant or both may be forced to preserve any digital evidence in their possession.

Analysis of the sample case

Under the rules of criminal procedure, it will be possible to obtain all the digital information from and possessed by the employer. This evidence might be analyzed very quickly and at very little cost to the aggrieved party. Indeed, any law enforcement officers involved could

[42] *Antioch Co. v. Scrapbook Borders, Inc., 210 F. R. D. 645, 2002 U.S. Dist. LEXIS 20811 (D. Minn. 2003), summary granted and denied in part, 2003 U.S. Dist. LEXIS (D.Minn. 2003) and Simon Property Group, L.P. v. mySimon, Inc., 194 F.R.D. 639, 641-642 (N.D. Ill 2000).*

[43] *Fed. R. Crim. P. 34.*

[44] *Fed. R. Crim. P. 34(a).*

[45] *Fed. R. Civ. P. 45.*

[46] *Fed. R. Civ. P. 45(a)(1)(A)(iii).*

immediately send out notices to preserve information held by the relevant Internet Service Providers. In order to pursue such an alternative, however, it is crucial to ensure any law enforcement officers that might be allocated the investigation know what they are doing. However, the problem is that law enforcement officers tend to be overworked, and might not be the best qualified personnel to analyze the information in their possession. Given such a situation, it may be in the business's best interest to ask an independent consultant to analyze the evidence before reporting to a law enforcement agency. This approach tends to be the preferred methodology most of the time. Even though this is the preferred approach, there is some risk that a law enforcement agency could reject the evidence obtained by the private consultant if the consultant has altered the evidence in some way.[47] In such a case case, the aggrieved party would have pursue only private remedies. It is much more likely, however, for the evidence to be altered by an internal manager looking for evidence when they do not have the requisite expertise to properly preserve the evidence at hand.

Some businesses might choose to pursue only civil remedies, because they are greatly concerned about the ability to control the information in their possession. For instance, there are various states within the United States that require the victims to be informed of a qualifying data breach.[48] Under such circumstances, the risks of doing harm to the reputation of a company may be too great to pursue the remedies. Conceivably, the right consultants may be able to immediately analyze the situation, before inviting a law enforcement agency to consider an investigation.

In conclusion, what and when to do it largely will be a matter of personal preference to the businesses involved. However, without being informed about the consequences of pursuing a remedy through criminal proceedings or civil proceedings, or both, the aggrieved business may be foregoing their best option to pursue an effective remedy while preserving their business interests.[49] This paper has depicted a brief overview of some of major considerations involved in what action to take when seeking a remedy, it is necessary to make it clear that every situation is different, and the decision-making process ought to take the facts into account before pursuing any action.

Joseph J. Schwerha IV, M.S., J.D. is an expert in the areas of computer forensics, electronic discovery and privacy. He serves as both an Associate Professor of Business Law at the California University of Pennsylvania, and as a private consultant through his firm, TraceEvidence, LLC. schwerha@cup.edu

jschwerha@traceevidence.net.
http://www.traceevidence.net

[47] *It is rare for a professional consultant to taint evidence during the course of their investigation. In such a case, however, the law enforcement agency may elect to not pursue the investigation or lay charges because they do not want to be in a position to explain why the evidence was tainted, even it made no significant difference in the case.*

[48] *For instance, see Cal. Civ. Code § 1798.82.*

[49] *For instance, in the recent case of In re Subpoena Duces Tecum to AOL, LLC, -- F.Supp.2d.--, 2008 WL 1956266 (E.D. Va. 2008), the court ruled that ECPA bars production of e-mail records held by an ISP in a civil case.*

