

## **CPA –Client-Attorney Privilege and Information Technology Risk<sup>1</sup>**

Alan Reinstein, DBA, CPA  
George R. Husband Professor of Accounting  
School of Business Administration  
Wayne State University  
Detroit, MI 48202  
(313) 577-4530; (248) 368-8841; FAX (248) 368-8950  
E-Mail: a.reinstein@wayne.edu

Jack Seward  
Digital Forensic Accounting Technologist  
Jack Seward & Assoc., LLC  
New York, New York  
(917) 450-9328; FAX (212) 656-1486  
E-Mail: jackseward@msn.com

August 17, 2008

We appreciate the helpful comments from David Stout (Youngstown State University), Myles Stern (Wayne State University), Brian Green (University of Michigan-Dearborn), David Sinason (Northern Illinois University), Jeff Wong (University of Nevada-Reno), Marilyn Prosch (Arizona State University-West), Rene Souvigney (Delphi Corp.), Martin Leibowitz (Yeshiva University), Carl Pacini (Florida Gulf Coast University) and Deepti Verma (Wayne State University MBA Student).

<sup>1</sup>The authors are not attorneys, and this article must not be relied upon as legal advice. The information contained in this article represents a broad overview of issues relating to the evidentiary privileges that may arise in the context of the CPA's practice. Appropriate legal counsel must be tailored to the specific circumstances of each case. Thus, nothing provided herein should be used as a substitute for the advice of competent legal counsel.

**FOR DISCUSSION PURPOSES ONLY. PLEASE DO NOT CITE THIS WORK WITHOUT THE AUTHORS' PERMISSION**

## **CPA-Client-Attorney Privilege and Information Technology Risk**

### **ABSTRACT**

CPAs serving as experts for attorneys and their clients are expected to maintain privileged information in many of their communications to protect it from opposing attorneys and their experts—and in accordance with AICPA guidelines. However, advances in modern technology can threaten this privilege and allow unwarranted access to such information. For example, clients merely sending attorney-client privileged information to CPAs “to look over” can break legal safeguards, making such information discoverable in depositions and trials.

The purpose of this paper is to discuss these information technology risks and suggest ways to minimize avoidance of the privilege and unwarranted intrusion into the CPA’s electronic information. We also discuss the history of the concepts involved and some implications of this issue relating to the Sarbanes-Oxley Act of 2002

## **CPA-Client-Attorney Privilege and Risks Imposed by Information Technology Risk**

In the last two years, the public has seen over 150 million records compromised: “data breaches” (including AICPA membership lists), losses of crucial university databases, and Big 4 firms losing laptops containing confidential information ([www.privacyrights.org](http://www.privacyrights.org) and Zeller, 2006). The Department of Veterans Affairs reported the theft of 26.5 million Social Security numbers in May 2006 from an employee whose home was burglarized (MSNBC, 2006). Perhaps the best known incident was the 2005-2006 hacking of over 45 million files of TJX Companies, Inc. (Pereira, 2007). None of the responsible parties used readily available encryption technologies to protect their electronic data, and the FBI reports that 97 percent of reported lost laptops are never recovered (CPA website, 2007).

While data stored and transmitted using such conventional means as snail mail, FedEx and courier face loss and theft, using Information Technology (IT) creates additional risks, as when unauthorized access or damage to information arises from Trojan horses, viruses, worms and rootkits, and easily transportable storage devices such as flash drives and laptops make theft much easier. Thus, CPAs should understand the threat of malicious software (“malware”) (Berghel and Hoelzer, 2005) and recognize the dangers of ineffective, unprotected or improperly configured wireless networks that allow unauthorized harvesting of electronic information.

A client expects its CPA to keep certain communications confidential, especially privileged information that goes to its attorney as part of legal actions, or to and from the CPA in his or her capacity as a forensic accountant or damage assessor. In fact, the AICPA and the Canadian Institute of Chartered Accountants have set up a task force to design and implement sound privacy practices and policies, including the disclosure of personal information to third parties only with the client’s implicit or explicit consent ([www.aicpa.org/privacy](http://www.aicpa.org/privacy)).

This article discusses potential risks in electronic communications and information technology when CPAs enter into an attorney-client relationship. CPAs should recognize that clients sending them attorney-client privileged information and work-product “to look over” before the attorney engages them could make the information discoverable in depositions and trials. Information technology can also impair relationships, as when a CPA in calculating business loss for an attorney’s client unwittingly waives the attorney-client privilege and “work-product doctrine” (i.e., the doctrine that “allows attorneys to prepare for litigation without fear that their work product and mental impressions will be revealed to adversaries,” Mathis, 2006) by e-mailing preliminary computations or proposed client strategy directly to the client, rather than sending it to the attorney who, in turn, discusses it with the attorney’s client.

### **UNDERSTANDING ATTORNEY-CLIENT PRIVILEGE**

Attorney-client privilege, a well-established principle that seeks to insure open and candid discussions between these parties (*Upjohn Co. v. United States*, 1981), applies to “(1) communications (2) made in confidence (3) by the client (4) in the course of seeking legal advice (5) from a lawyer in his capacity as such, and [it] applies only (6) when invoked by the client and (7) not waived” (*Meoli v. American Medical Service of San Diego*, 2003). This topic is especially important for accountants operating in an IT environment because of the concentration of data in accessible repositories such as laptop computers.

In ascertaining whether a communication is confidential, courts apply both a subjective and an objective test (*Asia Global Crossing, Ltd.*, 2005). The parties must have intended and expected the communication to be confidential and, given the facts and circumstances, the expectation of confidentiality must be reasonable.

The parties’ conduct either expressly or by implication may waive the attorney-client privilege (*In re Keeper of the Records*, 2004). An implied waiver “occurs when a party claiming

the privilege *voluntarily* disclosed confidential information on a given subject matter to a party not covered by the privilege (Hanson, 2006).” Herein lies the danger to the CPA. In the *Asia Global Crossing* (2005) case, the bankruptcy court held that e-mails forwarded to third parties waived privilege. It identified four factors that can increase the risk of disclosure and could destroy the attorney-client privilege. Privilege is endangered if (1) the company does not maintain a policy banning personal or objectionable use of its e-mail system; (2) the company does not monitor its employees' use of their computers or e-mail accounts; (3) third parties have a right of access to employees' computer or e-mail accounts; and (4) the employee was not notified of or was otherwise unaware of the policies regarding the use and monitoring of their computers and e-mail.

Directors and corporate officers cannot invoke attorney-client privilege to protect disclosure of their personal communications with corporate counsel when those communications concern the corporation (Bevill, Bresler & Schulman Asset Management Corp, 1986). Communications between corporate counsel and individual corporate managers are protected only when the communications are for the corporate manager's *personal* liability, rights or causes of action (McLucas, Shapiro and Song, 2006).

A five-part test helps to determine whether a corporate manager has a personal attorney-client privilege with corporate counsel: (1) the manager must approach counsel seeking legal advice; (2) the manager must have made it clear that he/she was seeking advice in his/her individual capacity; (3) corporate counsel communicated with them in their individual capacity, knowing that a conflict-of-interest might arise; (4) the communications were confidential; and (5) their communications do not concern company affairs (In re Grand Jury Subpoena).

On a related topic, transnational discovery of Client-CPA-Attorney privileged information outside of common law countries is limited. However, bankruptcy reorganization

and insolvency greatly increase the likelihood that the communications will be made available in the digital age. For example, most bankruptcy restructuring and insolvency proceedings entail reviews of company electronic records related to transfer of assets and changes in company management that might lead to others gaining access to previously confidential electronic communications. Under U.S. Jurisprudence, attorney-client privilege protects communications of in-house counsel, unlike such European jurisdictions as France, Germany, Switzerland, Netherlands and the European Union that attach no privilege to such communications, deeming in-house counsel as not “independent” (Pratt, Fall 1999).

#### Litigation Setting for Protecting Client-CPA-Attorney

Clients expect their CPAs to keep received information confidential, if not privileged, e.g., outsiders can access information in audit working papers only in cases of court subpoenas or CPA peer reviews. They expect to limit access to privileged information in litigation support matters, lest the opposing parties gain a “road map” to the client’s detriment. To preserve the attorney-client privilege, the attorney usually engages the CPA as an agent. Both the client and CPA then communicate through the attorney, so that all three parties can preserve this privileged relationship, thereby restricting certain crucial information within this “privileged circle.”

All parties should understand recent amendments to the *Federal Rules of Civil Procedure* (FRCP). Becoming law on December 1, 2006, the FRCP relates to the discovery of electronically stored information (ESI) in litigation. Moreover, many state courts have adopted provisions similar to the amended FRCP, and the Proposed Uniform Electronic Discovery Act uses the FRCP as its framework. Exhibit I summarizes various Acts, rules and opinions that can affect Client-CPA-Attorney Privilege.

Lack of understanding of the risks associated with ESI exposes many CPAs, attorneys (including general counsel) and their clients to significant adverse consequences. The Southern

District of New York in *Phoenix Four* (2006) found that a law firm's failure to find its clients' ESI constituted "gross negligence" and ordered both the firm and the defendants to pay monetary sanctions. The law firm's "gross negligence" arose from its not conducting a methodical search for ESI while simply relying upon the defendants' representations that there were no sources of ESI because the company ceased operations. The court found after the completion of discovery that the computer's hard drive had a "hidden partition."

Prior to the amended FRCP, opposing counsel might not have engaged in electronic discovery looking for weaknesses to unearth privileged information, but that has changed. The American Bar Association, Formal Opinion No. 05-437, in 2005 withdrew its 1992 opinion regarding amendments to Rule 4.4(b). That is, the attorneys must only notify the other side when they produce privileged documents, but this 2005 opinion does not require abstaining from looking at the contents of the document. The Committee Note to FRCP Rule 26, subdivision (f) states, "The volume and dynamic nature of electronically stored information may complicate preservation obligations," which CPA practitioners using electronic communications should recognize. For example, the widely reported theft of information from celebrity Paris Hilton's cell phone database (Harrison and Froelich, 2005) shows the ease of access and adverse publicity associated with stolen information. Krebs (2005) found that this event occurred when a 16-year-old caller said, "This is [an invented name] from T-Mobile headquarters in Washington. We heard you've been having problems with your customer account tools."

#### Client Electronic Communications

Client communications entailing electronic methods such as instant messaging (IM), cell phone texting, file sharing and electronic conferencing affect the attorney's ability to protect the privilege and work-product. Schweitzer (2006) notes that waiving privileged communications arises through sharing of ESI with third parties because, "It is easy to have e-mail accidents, and

accidents are more common in important business and personal communications than most people may realize.” A single, non-retrievable, errant keystroke or mouse click can send a message to the wrong recipient. For example, attaching electronic files to group instant messaging could trigger waiving privilege, which could cause serious consequences if such a discoverable, electronic file contained the voice of the CPA using voice recognition software (Ball, 2007).

Under the “strict responsibility approach,” courts treat inadvertent disclosure as a waiver of privilege, not requiring the element of intent, reasoning that once a third party obtains a privileged communication, confidentiality is lost and cannot be restored. Some courts even insist disclosure is evidence of the client’s intention to forfeit privilege. This thesis is simple for courts to administer and yields predictable results. Thus, attorneys and their agents should safeguard sufficiently confidential information that they do not want their legal adversaries to obtain.

## **PROTECTING THE PRIVILEGE FOR CPA SERVICES**

### History of the Privilege

Federal and state governments have long upheld attorney-client and third-party privileged communications, as in the U.S. Supreme Court Standard 503 Lawyer-Client Privilege Law and the Bieter case (16 E3d 929 [8th Cir. (1994)]). The *United States v. Kovel* 296 F. 2d 918 [2d Cir. (1961)] case extended attorney-client privilege to communications between clients and those whom their attorneys retain to help the attorney provide legal services (Segal, 1997), which allows attorneys to shield a non-testifying accountant and all resultant work product and communications.

### Litigation Support Services

Attorneys often hire CPAs to perform litigation support services related to discovery and production of documents, electronic data discovery, corporate accounting investigations, white-

collar crime, bankruptcy, business valuations, economic damage calculations and other types of services that require privileged communications. While the Federal Rule of Civil Procedure (FRCP) 26(b) helps protect privileged documents during discovery, it may allow opposing counsel to obtain privileged documents in discovery that may be non-admissible at trial.

Opposing counsel could use obtained drafts of such communications as a road map to impugn the CPA's testimony and related calculations. To prevent privileged information from reaching inappropriate hands, CPAs should at least physically separate sensitive information from other data; set up a routine to change systems using passwords such as e-mail, ESI and Internet Service Provider (ISP) accounts; and recognize that unexpected ESI and other files can emerge during discovery under the FRCP.

Pacini et al. (2004) discuss the Kovel Rule, which can allow an attorney to shield a non-testifying accountant or other business expert. This rule extends the attorney-client privilege to accountant-client communications and to work product for accountants hired to help render legal services. The party claiming the privilege bears the burden to prove the existence of the factors required to sustain it. Various protective measures reviewed herein can preserve the extension of the privilege to accountants and other business experts.

CPAs usually can extend the Kovel Rule to protect electronically stored attorney-client privileged information. For example, federal law grants Internet e-mail and other "electronic communications" the same privacy that applies to the Postal Service, commercial mail services, landline telephone communications and facsimile ("fax") transmissions (Pacini et al. 2003). The *Electronic Communications Privacy Act* (ECPA) of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986), amends the Federal Wiretap Statute, 18 U.S.C.A. Sec. 2510 et seq. (1998) to provide criminal and civil penalties for the unauthorized interception or disclosure of any wire, oral or electronic communication. 18 U.S.C.A. Sec. 2511 (Bierce & Kenerson, P.C., 2003-2004).

Thus, CPAs performing litigation consulting should document the circumstances of their hiring, record relevant phone calls and appointments, obtain engagement letters from the attorneys, label the project's work product "confidential," properly conduct client meetings, directly invoice the attorney (not the client), send reports directly to the lawyer (rather than through the client), and segregate engagement report materials from other work files. Pacini et al. (2004) also recommend that CPAs use encryption tools to reduce the likelihood of waiver of privilege due to inadvertent disclosure.

### Privilege in Audits

In financial audits, the principle of *privilege* applies to confidential financial communications among the CPA, the attorney and the attorney's client. Section 307 of the Sarbanes-Oxley Act (SOA) of 2002 requires attorneys to report evidence of material violations of securities laws, breaches of fiduciary duty, or similar issuer violations "up-the-ladder" to the company's chief legal counsel or chief executive officer. If an inadequate response arises, the attorney must file a "mandatory report" of the evidence to the audit committee, another committee of independent directors, or the full board of directors. Attorneys also may file a "permissive report" to the board of directors (Davis 2003), in which they can report possession of confidential information that could damage the company, or commit a fraud or perpetrate actions that hurt investors' interests.

McCord and Weisdorn (2003) claim that the attorney-client privilege might not protect such attorney communications, thus allowing Securities and Exchange Commission (SEC) access to significant, otherwise unobtainable, information from auditors or other sources (Fein and Huie, 2003). The pressure to waive attorney-client privilege is real, and in essence SOA places corporate attorneys in a Catch-22. The SEC, of course, could also seek to expand this source of information and turn it over to the Department of Justice for further prosecution and

further erosion of privileged information. Thus, CPAs should encrypt, segregate and label as “privileged” information that they do not want to end up in the SEC’s possession.

### The Safe Harbor

Title III of the *Omnibus Crime Control and Safe Streets Act of 1968*, 18 U.S.C. 2517(4) provides that “no otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character,” if reasonable precautions are taken to secure electronic communication. Members of the opposing counsel team and hackers often want to obtain such information. This provision could protect against claims of waiving privilege through interception (Baker and Hintze, 1998).

Title I of the ECPA prohibits random or other monitoring of electronic communications without court orders or consent of one of the parties to the communications. The Third U.S. Circuit Court of Appeal found that an employer did not violate this statute when it examined a former employee’s e-mails stored on its computer. See *Fraser v. Nationwide Mutual Insurance Co.* Civ. A. No. 01-2921, 2003 U.S. App. LEXIS 24856 (3d Cir. Dec. 10, 2003), (Ford and Harrison LLP, 2003) [Fraser Case]. Thus, employers can monitor employee e-mail without violating these statutes, as employers are searching their own computers, even when providing electronic communication service (Dwyer, 2004).

Privacy safeguards may not protect all privileged information. In the Maxwell case, the court in *United States v. Charbonneau* held that “conversations” in chat rooms are not afforded the same reasonable expectation of privacy as e-mails among individuals because messages sent to the public at large in a chat room lose any semblance of privacy (Foote, 2003).

To minimize potential litigation and to inform all parties of appropriate risks, CPAs should carefully consider the ramifications of all data going to their and their clients’ attorneys, including e-mail, digital and other electronic communications. For example, the CPA’s retainer

language should inform the attorney of the possible deliberate/non-deliberate interception of e-mails and digital or electronic information and inability to ensure secure communications. CPAs should also consider informing clients that all electronic communications sent regarding actual or threatened litigation can become discoverable and not protected by privilege unless directed through the attorney (rather than through the client) that engages the CPA in the matter.

### Practical Solutions and Risk

To lessen threats of interception and reduce the future costs associated with electronic discovery of ESI, CPAs should use encryption technology when communicating and transferring such electronic media as IM and real-time Internet video communications. CPAs should also note that unlike prior encryption technology solutions, many current enterprise level solutions provide for Public Key Infrastructure (PKI), Pretty Good Privacy (PGP) or other encryption algorithms software keys from the corporate client or attorney if they already use these systems.

Many encryption solutions are now affordable, easy to use and include professional and enterprise editions that are compliant with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and can greatly reduce time and implementations costs associated with the “roll-out.” E-mail and electronic information encryption has become a needed cost of CPA’s doing business—often entailing (as in other software purchases) the necessary download link to install encryption software to secure internal hard drives, removable drives, network drives, documents, data and e-mail.

Some application service providers also supply encryption solutions. Bumgarner (2001) shows the effectiveness of some relatively inexpensive and easy to use encryption programs, parts of which appear in Exhibit II.

Accounting practitioners should know of other helpful services available with common encryption software like The CyberAngel® ([www.thecyberangel.com](http://www.thecyberangel.com)). Besides encrypting the

hard drive, folders, documents and data files, The CyberAngel can help provide hardware recovery, limitations to unauthorized use of lost or stolen desktop and laptop computer devices, and otherwise track computer assets. Its website calls itself “The only computer security product and service offering data protection, intrusion detection, exportable strong encryption, plus a unique tracking system for stolen computers” Moreover, Absolute Software's LoJack notebook computer security software helps protect sensitive data as well as tracks and locates lost or stolen laptops, by having the notebook “report” each day its global position to Absolute during normal use. If the notebook is lost or stolen, the owner calls Absolute. Then Absolute will find and report the global position of the computer in question to local law officials, who, in turn, will obtain the computer and return it to its proper owner. Absolute can also produce a log of unauthorized use of the stolen computer including the computer's access to the Internet.

Encryption software may place privileged information in attachments rather than in the body of the e-mail, thus making e-mail equivalent to an electronic envelope. Using strong pass phrases can increase the e-mailed and encrypted documents' security. Since e-mail solutions, including some encryption technologies, do not protect the clear text found in the “Subject Line,” the CPA should consider placing there, *“This e-mail is confidential or privileged. If you are not the intended recipient, do not read this, and contact the sender.”*

Placing the full disclaimer at the start (rather than at the end) of the e-mails and increasing the disclaimer's prominence by using large or bold fonts on privileged e-mail should improve the CPA's position that this is privileged electronic communications. Adding watermarks that read, “This document is confidential or privileged” on each page of the electronic documents distributed to the privilege circle may aid in protecting the privilege.

To enhance confidential and privilege relationships, practitioners' and clients' e-mail disclaimers should use language such as “all e-mails sent to or from the firm are for business

purposes only.” The CPA should also refrain from allowing anyone outside of the control group (privilege circle) to review or monitor confidential or privileged electronic communications, although outsourced personnel and others often examine such client data. To help maintain the integrity of transferring large volumes of unencrypted data to and from clients involved in litigation, CPA practitioners can use such tools as Accellion® ([www.accellion.com](http://www.accellion.com)) Secured File Transfer Appliance (SFTP) solution to send and receive large files (10GB with one click). Accellion has received endorsements from Harvard Medical School, Beth Israel Deaconess Medical Center, Cornell University’s Weill Medical College and many large law firms.

CPAs should recognize that employees who access e-mail sent through their employers may lose their reasonable expectation of privacy (Fraser Case), especially when communicating with clients using an e-mail address that is obviously the place of the client’s employment. Using free e-mail accounts is generally not recommended since it can also allow unauthorized parties access to e-mail through many servers that share e-mail accounts and addresses (e.g., “jeffmarysmith@yahoo.com”). Moreover, CPAs should recognize that such widely used service providers as Yahoo! and AOL can claim under common carrier laws that a shipper-consignee relationship exists when data passing through their e-mail servers belongs to the company, which can lead to the loss of privilege/confidentiality and even to losing the content’s copyright.

*The New York Times* reported recently (Stone, 2007) that “A growing number of Internet-literate workers are forwarding their office e-mail to free Web-accessible personal accounts offered by Google, Yahoo! and other companies. Their employers, who envision corporate secrets leaking through the back door of otherwise well-protected computer networks, are not pleased.” This concept of the “weakest link” was further described as “a battle of best intentions: productivity and convenience pitted against security and more than a little anxiety.”

CPAs should thus adequately train their staff and warn their clients about this problem, stressing that it could lead to the loss of privileged relationships of sensitive client data.

CPAs engaged by attorneys as litigation and discovery experts should recognize the risks associated with removing metadata from documents produced during litigation. Metadata is structured information about data that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource, as when 12345 in the context of a U.S. zip code refers to a location in Schenectady, N.Y. The term “metadata” often associates with Microsoft Office (Word, Excel and PowerPoint) documents but pertains to all “data about data.” For example, USB flash drives, external hard drives and digital devices leave behind metadata footprints (“make and model”) of most types of devices attached to computers. Moreover, since the Microsoft WORD metadata includes the document’s author (under the “Properties” option in the *File* pull-down icon), the CPA might receive a memo; revise it (e.g., using the Track Changes option) extensively; and then send it to a third party, unwittingly revealing the original author’s name. Newer versions of Microsoft WORD often allow easy removal of personal information. CPS could also simply convert all sent memos using newer versions of ADOBE Acrobat to avoid such potential problems.

Because Metadata is critical in spreadsheets, accounting and financial databases, electronic books and records and financial information, newly amended FRCP Section 34 seeks to be comprehensive and media neutral in electronic document discovery. Reviewing ESI evidence files during discovery and prior to producing ESI to counsel can change the metadata, which affects the attorney and the attorney’s client, and could become an ethical violation. CPAs should also consider copying the data to new files for review to ascertain that the metadata did not change. Accessing “live” metadata files (which, by definition, contain embedded information) leaves traceable “footprints,” which the opposition’s experts can detect.

## **RISK FROM “AUTOMATION”**

### Beyond Privilege

Encryption technology software reduces the risk of forged electronic communications. Authentication, such as digital certificates and digital signatures, uses cryptographic methods to confirm that the information comes from a certain sender. Authentication can prevent senders from falsely denying that they sent the message. Cryptography helps to assure the electronic message’s integrity, confirming to recipients that the message was not altered in transit (Baker and Hintze 1998). Taking advantage of sending options available in commonly used email software like Outlook and such encryption technology solutions as Secured eMail’s ePrivacy Suite Enterprise® (and ePrivacy Suite®) provide CPAs with assurance of the integrity of the messages communicated plus “proof of delivery” to reduce litigation risks from disputes arising in electronic communications. They also protect against the receiving party repudiating receipt of electronic documents and reduce significantly risks of privacy breaches and compliance violations by encrypting files, folders, USB drives and e-mail when requested to do so.

CPAs using these solutions help to “secure” this type of information on laptops which access the Internet using wireless networks (“Wi-Fi”). Using unsecured Wi-Fi networks (the kind available for free at coffee shops, hotels, and in airports) advanced network users or hackers can find and read unencrypted data when it is sent over the network. Additionally, anyone using the wireless network without the file owner’s knowledge can access any files that are configured to be shared over the network, which is like locking up your house, but leaving some valuables on the front porch. Professionals with confidential electronic data should be very careful when connecting to Wi-Fi networks open to the general public.

Encryption software solutions differ, and accordingly some may not keep electronic information secret because the “weakest link” can be found in using passwords. (Wilcox, 2007)

These tools can reduce the cost of electronic discovery because they lower the time needed to locate and separate privileged electronic communications.

### **PROTECTING ACCESS TO THE CPA'S ELECTRONIC DATA**

CPAs, attorneys and clients should realize that electronic information often remains on hard disk drives and media storage for years, since “deleted” does not mean “erased.” Opposing parties may gain access to the computers of CPAs, attorneys, clients and other parties. Opposing parties sometime engage digital forensic technologists to recover and restore presumed deleted electronically stored information, files, databases, and other information, including items created using alternative data streams, encryption and digital steganography (Seward, 2003).

On a related matter, (Westphal, 2003) defines steganography (a/k/a “stego”) as “the art of writing in cipher, or in characters, which are not intelligible except to persons who have the key; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured.” CPA practitioners should also recognize that fraudsters can use “digital steganography” to hide whatever they can define (Seward, 2004). Using adequate physical protection of privileged communications can strengthen the legal arguments and make it difficult in litigation and bankruptcy restructuring to discover the privileged material.

The economic realities of litigations often require that attorneys, CPAs and clients share electronic databases using litigation support software. Simply keeping the litigation database information on a Web repository may cause the court to find that the work product doctrine does not protect this information. The courts can use the FRCP to order CPAs to “share” discoverable electronic databases with the opposition. Moreover, CPA experts relying on information found in litigation support databases may cause the databases to be discoverable by the opponent, as when they copy the litigation databases onto external hard drives or other digital media.

Furthermore, CPAs obtaining ESI evidential matter may make them client custodians or agents, including for bankruptcy and restructuring matters than can surface many years later.

*Spoliation* is another threat. *Spoliation* (defined broadly as the intentional, reckless destruction, loss, material alteration or obstruction of evidence relevant to litigation) (Segal, 1997), which constituted a key factor in the Enron matter, carries heavy penalties. While spoliation may include both negligent and intentional destruction or withholding of evidence, the courts generally presume that parties only destroy evidence that is harmful to their case—following the legal maxim, *omnia preasumuntur contra spoliatores*, “all things are presumed against the spoliator.”

CPAs face severe court sanctions if found guilty of spoliation, i.e., helping to hide or delete discoverable ESI during threatened or actual litigation. Thus, they should only remove unneeded backup media, and periodically and systematically delete e-mails not subject to legal record-retention requirements, by using such software tools (see Exhibit III) as SecureClean®<sup>1</sup> and WipeDrive® by WhiteCannon, Inc. ([www.whitecannon.com](http://www.whitecannon.com)).

Documentation-retention policies (DRP) also require ascertaining the correct status of the ESI. CPAs should recognize that e-mail and related files are often considered business records and should be treated as such. CPAs should electronically “shred” (see SecureClean® discussed above) such information to ascertain that it does not remain on a computer’s hard drive and backup media— without destroying discoverable records, recognizing that many forms (shadow files) may exist after the intended document or file was deleted. CPAs should also analyze their clients’ data retention policies for e-mail and other data. For example, some corporations require purging e-mail from gateway e-mail servers every 30 days, thereby deleting e-mail that may

---

<sup>1</sup> SecureClean® erases all traces of “deleted information,” including e-mail, Internet history, temporary files, files searches, deleted files and fragments, temporary folders, printer files, thumbnail files, autosave files, recycle bin, recent documents, file history for recently used files and documents and names of files along with the “file slack” found on hard drives and external storage devices to DoD standard 5220.22-M standards and beyond (7 or up to 12 data overwrites).

have a litigation hold. CPAs and their clients should develop policies for monitoring, printed and electronic documentation retention, including in a bankruptcy environment.

CPAs can minimize “identity theft” by using such specialized software packages as WipeDrive® by WhiteCannon, Inc. ([www.whitecannon.com](http://www.whitecannon.com)) before disposing of computer hard drives, USB drives and digital devices. It thoroughly cleans (shreds) computer hard drives and digital devices to the above mentioned DoD standard, and is used by the U.S. Air Force, Coast Guard, Navy, Post Office and Department of Homeland Security.

The Sarbanes-Oxley Act requires CPAs to maintain audit records for seven years. Titles VIII to XI increase penalties for illegal actions; a CPA found guilty of documents spoliation could face imprisonment for up to 20 years. For example, in October 2004, former Ernst & Young audit partner Thomas Trauger pled guilty to criminal violations under the Sarbanes-Oxley Act. He admitted to knowingly altering, destroying and falsifying electronic information with the intent to impede and obstruct an investigation related to the collapse of NextCard Inc., Delaware, case no. 02-13376 (Bankruptcy Law & Litigation Report, December 2003). He was sentenced to a year in federal prison and fined \$5,000 for destroying documents that authorities investigating NextCard sought.

The Open Compliance & Ethics Group provides information on compliance and ethics to corporate boards ([www.oceg.org](http://www.oceg.org)). CPAs can help their clients protect privileged information by ascertaining that they: (1) establish such proper procedures as using secure “electronic” locations that only “control” group members can access, encrypting electronic communications and limiting the electronic devices upon which they store or communicate privileged materials; and (2) legally protect privileged material by following counsel’s advice, including identifying privileged communications and material and not circulating privileged material outside of the control group (lest that imply an implicit waiver of that privilege).

## CONCLUSION

The existence of attorney-client privilege for electronic information can no longer be automatically presumed. Because “[a]n attorney now risks committing malpractice or receiving court sanctions if he or she does not adequately understand how electronic information is created, stored and communicated” (Fielding and Seward, 2006), the attorney will find it increasingly difficult to protect the privilege regarding testimony related to the evidentiary foundations necessary to admit electronically stored business records, which, in turn, affects CPAs and other accounting experts performing such testimonies.

Given the relatively trivial costs of encryption technology, CPAs, attorneys and clients, should select appropriate encryption solutions to help protect privileged information. Although encryption technology does not completely eliminate the risk of misuse of electronic information, it is necessary and does help to control the risks. CPAs may need to educate their clients that electronic communications can only be as safe as the “*weakest* link” in the chain of data communications because waived attorney-client privilege can rarely be undone. CPAs using such techniques will earn their clients’ admiration for insisting on using the “best practices” to protect privileged and confidential information.

**EXHIBIT 1**  
**Provisions of Certain Acts, Rulings and Opinions Affecting Privileged Information**

Authoritative Act

Affect upon Privileged Information

Kovel Rule, 1961	CPAs serving as attorney's non-testifying agents for attorney's legal matters receive benefits of all CPA-attorney communications for that specific client
Omnibus Crime Control and Safe Streets Act (OCCSSA) of 1968	Willfully intercepting certain unauthorized oral or written communications can result in federal civil and criminal penalties
Electronic Communications Privacy Act of 1986	The OCCSSA now extends to intentional interception and disclosure of electronic information.
American Bar Association, Formal Opinion No. 05-437, 2005	Attorneys receiving materials that on their face appear to be subject to the attorney-client privilege or otherwise confidential information under Model Rule 1.6, where they were clearly not intended for the receiving lawyer should refrain from examining this information, notify the sending lawyer and abide by the sending lawyer's instructions.
Federal Rules of Civil Procedure, Rule 26, 2007	The producing party must immediately notify the receiving (party of inadvertently disclosed privileged information, and the receiving party must promptly return, sequester or destroy specified information it holds. The receiving party cannot use this information until the Courts resolve the matter.

**EXHIBIT II**  
**Some Providers of Encryption Software**

1.	Secured eMail's ePrivacy Suite® ( <a href="http://www.securedemail.com">www.securedemail.com</a> )
2.	ArticSoft® ( <a href="http://www.articsoft.com">www.articsoft.com</a> )
3.	Cypherix®, ( <a href="http://www.cypherix.co.uk">www.cypherix.co.uk</a> )
4.	Kryptiq® ( <a href="http://kryptiq.com">http://kryptiq.com</a> )
5.	LogMeIn® ( <a href="https://secure.logmein.com">https://secure.logmein.com</a> )
6.	WinMagic® Disk Encryption ( <a href="http://www.winmagic.com">www.winmagic.com</a> )
7.	Zixmail® ( <a href="http://www.zixcorp.com">www.zixcorp.com</a> )

**EXHIBIT III**  
**Some Providers of Data Deletion Software**

1.	Kazi Software - 123 Cleaner
2.	WhiteCanyon – WipeDrive PRO
3.	Yitian Software – Privacy Cleaner
4.	R Tools Technology – R-Wipe and Clean
5.	PC Tools Software – Privacy Guardian
6.	Blue Chillies – Fast Eraser
7.	Pro Data Doctor – Secure Data Wiper

## REFERENCES

American Bar Association, (May 2005) Committee on Ethics and Professional Responsibility, *Protecting the Confidentiality of Unencrypted E-Mail*, Formal Opinion No. 05-437

Asia Global Crossing, Ltd., 322 B.R. 247, 255 (Bankr. S.D.N.Y. 2005).

Baker, S.A. and Hintze, M.D. (September 14, 1998). The Risks and Myths of E-Mail  
[http://mhintze.tripod.com/pubs/e-mail\\_risks\\_NYLJ.htm](http://mhintze.tripod.com/pubs/e-mail_risks_NYLJ.htm)

Ball, Craig (2007) 4 on Forensics, Four Articles on Forensics for Lawyers.  
[http://www.craigball.com/CF4\\_0807.pdf](http://www.craigball.com/CF4_0807.pdf)

Bevill, Bresler & Schulman Asset Management Corp., see 274 F.3d at 573; 805 F.2d 120, 125 (3d Cir. 1986).

Berghel, Hal and David Hoelzer, "Pernicious Ports," *Communications of the ACM*, December 2005, Volume 48, Issue 12, pp. 23-30.

Bierce & Kenerson, P.C. (2003-2004). Confidentiality of Your Communications with a U.S. Attorney. <http://www.biercenerson.com/B&K/confidential.htm>

Bumgarner, John M., "Hashing out Encryption Solutions," *Security Management*, June 2001, Volume 45, Issue 6, pp. 66-71.

Canadian Psychological Association (CPA) Website:  
<http://www.cpa.ca/members/membershipbenefits/computracelaptoptheftrecoverysolution/>

Davis, Evan A., "The Meaning of Professional Independence," *Columbia Law Review*, Vol. 103, No. 5 (Jun., 2003), pp. 1281-1292

Dwyer, M.Q. (February, 2004). E-Mail Monitoring –What Can an Employer Do?

Fein, D.B. and Huie, P.S. (June 24, 2003). Attacks on Client Privilege Increasing.

Fielding, M. and Seward, J. (December/January 2007) You Need To Know This: Bankruptcy and the Attorney-Client Privilege in the Electronic Age, *American Bankruptcy Institute Journal*

Ford and Harrison LLP, (December 15, 2003). Third Circuit Finds Examination of Former Employee's E-Mail did not Violate ECPA  
[http://www.fordharrison.com/fh/news/articles/20031215email\\_ecpa.asp](http://www.fordharrison.com/fh/news/articles/20031215email_ecpa.asp)

Foote, R.J. (2003). E-mail, Privilege, Confidential Information and Inadvertent Disclosures.  
<http://www.fmew.com/archive/EmailSecurity/>

FRCP 16(b), 26(a), 26(b)(2), 26(b)(5), 26(f), 33(d), 34(b), 37(f), 45, and Form 35.

Grand Jury Subpoena, 274 F.3d at 571, 2006.

Hanson, 372 F.3d at 294, 2006.

Harrison, Bridget and Paula Froelich, "Inside the Scary Tale of Paris' Purloined Privacy," *New York Post (Online Edition)*, February 22, 2005, <http://nypost.com/news/nationalnews/40993.htm>.

Keeper of the Records, 348 F.3d 16, 22 (1<sup>st</sup> Cir. 2003); see also *Hanson v. United States Agency for Int'l Development*, 372 F.3d 286, 293-94 (4<sup>th</sup> Cir. 2004).

Krebs, Brian, "Teen Pleads Guilty to Hacking Paris Hilton's Phone," *Washingtonpost.com*, September 13, 2005, see: [www.washingtonpost.com/wp-dyn/content/article/2005/09/13/AR2005091301423.html](http://www.washingtonpost.com/wp-dyn/content/article/2005/09/13/AR2005091301423.html)

Mathis, Karen J., President, American Bar Association, Statement before the U.S. Senate Judiciary Committee (September 12, 2006), <http://www.abanet.org/buslaw/attorneyclient/materials/064/064.pdf>.

McCord, L.B. and Weisdorn, G.H. (2003). Will your Corporate Attorney be the New Whistleblower? <http://gbr.pepperdine.edu/033/lawyers.html>

McLucas, William R, Howard M. Shapiro and Julie J. Song, "The Decline of the Attorney-Client Privilege in the Corporate Setting," *The Journal of Criminal Law & Criminology*, Vol. 96, No. 2, pp. 621-641.

*Meoli v. American Medical Service of San Diego*, 287 B.R. 808, 813 (S.D. Cal. 2003) (citing *United States v. Abrahams*, 905 F.2d 1276, 1283 (9<sup>th</sup> Cir. 1990)).

Merrill, C. (March 2002). Ethics: Revisiting the Question of Attorney/Client Internet E-Mail Encryption *Internet Newsletter*© NLP IP Company.

MSNBC, 2006: <http://www.microsoft-watch.c://www.msnbc.msn.com/id/12916803/>

NextCard Fraud Case Dawns Digital Bankruptcy Enforcement. (December 2003) *Bankruptcy Law & Litigation Report*.

Pacini, Carl, William Hillison, M.G. Fennema and Raymond Placid, "Attorney-Client Privilege: CPAs and the E-Frontier," *Journal of Accountancy*, April 2004, pp. 64-71.

Pacini, Carl, Pamela A. Seay and Raymond Placid, "Accountants, Attorney-Client Privilege and the Kovel Rule: Waiver through Disclosure via Electronic Communication," *Delaware Journal of Corporate Law*, Vol. 28, No. 3, 2003, pp. 1-39.

Periera, Joseph, "Breaking the Code: How Credit-Card Data Went Out Wireless Door - Biggest Known Theft Came from Retailer with Old, Weak Security" *Wall Street Journal On Line*, May 4, 2007

Phoenix Four, Inc. v. Strategic Resources Corp., 2006 WL 1409413 (S.D.N.Y. 2006).

Pratt, Joseph, and The Parameters of the Attorney-Client Privilege for In-House Counsel at the International Level: Protecting the Company's Confidential Information. 20*Norwestern Journal of International Law and Business* 145, 166 (Fall 1999).

Schweitzer, D. (June 26, 2006) E-mail Insecurity in a Litigious Society  
<http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=111607>.

Segal, M.A. (April 1997). Accountant and the Attorney-Client Privilege. *Journal of Accountancy*, pp. 53-56.

Seward, J. (Fall 2003). The Debtor's Digital Reckonings, *International Journal of Digital Evidence*. [http://www.ijde.org/docs/03\\_fall\\_seward.pdf](http://www.ijde.org/docs/03_fall_seward.pdf)

\_\_\_\_\_, (March 2004). Digital Stealth Secrets and the Act. *LJN's The Corporate Compliance & Regulatory Newsletter, Law Journal Newsletters*, <http://www.ljnonline.com>

Stone, Brad, "Companies Fret as Office E-Mail Is Detoured Past Security Walls," *The New York Times*, January 11, 2007, Section A, page 1, Column 1.

Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

Westphal, Kristy, *Security Focus*, April 9, 2003, see <http://www.primidi.com/2003/04/12.html>

Wilcox, Joe. (January 2007) The Weakest Link Is You, *Microsoft Watch - Security*  
[http://www.microsoft-watch.com/content/security/the\\_weakest\\_link\\_is\\_you.html](http://www.microsoft-watch.com/content/security/the_weakest_link_is_you.html)

[www.aicpa.org/privacy](http://www.aicpa.org/privacy)

[www.oceg.org](http://www.oceg.org) - Practice Aid, Internal Audit Guide, Evaluating a Compliance and Ethics Program, Appendix J: Corporate Governance - A primer on protecting the evidentiary privileges available to the enterprise.

[www.privacyrights.org](http://www.privacyrights.org)

[www.thecyberangel.com](http://www.thecyberangel.com)

Zeller, Tom J. New York Times Website, December 16, 2006;  
<http://www.nytimes.com/2006/12/18/technology/18link.html?ex=1188360000&en=abf8643ae0c71640&ei=5070>