

**CONFIDENTIALITY,  
ATTORNEY/CLIENT PRIVILEGE  
AND THE ELECTRONIC AGE -  
IT CAN BE QUICK AND PAINFUL**

**THOMAS H. WATKINS  
Brown McCarroll, L.L.P.  
111 Congress Avenue  
Austin, Texas 78701  
[twatkins@mailbmc.com](mailto:twatkins@mailbmc.com)**

**The University of Texas School of Law  
15<sup>th</sup> Annual Conference on State and Federal Appeals  
June 2, 2006  
Austin**

## Table of Contents

I. WHY IS THE INTERNET A PROBLEM FOR ATTORNEYS.....	1
A. Attorney-Client Privilege.....	1
B. Discovery and Investigative Privileges.....	3
II. CONFIDENTIALITY/DIGITAL SIGNATURE.....	4
A. Encryption.....	4
B. Digital Signatures.....	5
1. What is a Digital Signature? .....	5
2. Certification Authorities .....	5
3. The Legal Effect of a Digital Signature Under Texas Law .....	5

**I. WHY IS THE INTERNET A PROBLEM FOR ATTORNEYS**

The Internet is a potentially vast source of information, a tool for communication and a weapon of destruction. The key to using the Internet productively is recognizing its shortcomings and compensating for them before a problem occurs. Although the Internet can be a great benefit to the legal profession, its use raises concerns unique to this profession in two ways. First, attorneys are obligated to maintain client confidences. Improper use of the Internet can jeopardize client confidentiality exposing the client and the attorney to liability. Second, email can be the subject of discovery requests, raising concerns about protecting attorney work-product.

Electronic mail, or "email", can be used to send messages around the corner or around the globe almost instantaneously.<sup>1</sup> However, by virtue of the way email messages travel from computer to computer, the messages are at some risk from intruders, as are telephone calls, fax transmissions and items sent through the mail. Most computer networks providing email use the "store and forward" method of transmitting email. The sender transmits her message to the nearest computer between the sender and recipient.<sup>2</sup> That computer is called a "station."<sup>3</sup> The message travels from station to station, circumventing problems on the Internet, until it reaches the recipient's computer.<sup>4</sup>

The email is at risk during its route because during the travel time, the message is like a postcard traveling through the postal system.<sup>5</sup> Anyone with the skills who wants to search for email between the sender and recipient, or on a particular subject matter, can search for, read, modify and/or delete a message before it ever reaches the recipient.<sup>6</sup> With this background in mind, consider how these risks play in the legal arena.

**A. Attorney-Client Privilege**

The attorney-client privilege exists to foster uninhibited communication between the attorney and client. The elements of the attorney-client privilege were described by the U.S. Supreme Court as "[c]onfidential disclosures by a client to any attorney made in order to obtain legal assistance..." which are "...necessary to obtain informed legal advice - which might not have been made absent the privilege."<sup>7</sup> The Texas Disciplinary Rules of Professional Conduct define "confidential information" to include "privileged information" as defined in §503 of the Texas Rules of Evidence.<sup>8</sup> In general, these rules mandate that any communication between an attorney and her client is "confidential if not intended to be disclosed to third persons other than those to whom disclosure is made in furtherance of the rendition of professional legal services to the client or those reasonably necessary for the transmission of the communication."<sup>9</sup>

At stake when an attorney and client communicate via an insecure medium such as the Internet, is whether the communication originated in confidence and whether the parties to the communication have maintained its confidentiality.<sup>10</sup> As with telephones, cordless phones, cellular phones, and faxes which came before email, courts will be subject to a learning curve in understanding that while security is an issue with email, it is possible to send email confidentially and maintain its confidential nature. Courts have recognized email users expectation of privacy, although not in the context of the attorney-client privilege.<sup>11</sup> Although the courts have yet to rule that email is protected by the attorney-client privilege or what is necessary to maintain the privilege, the prudent practitioner will implement procedures now which demonstrate an intent to maintain confidentiality.

Efforts to maintain email confidentiality range from low-tech to cutting edge high-tech. Email that has been printed should receive the same basic protection from disclosure that any piece

of mail would receive. An attorney should make her computer physically secure by using passwords and screen locking devices to prevent persons who are walking down the hall from logging onto her computer and reading her mail or reading mail off her screen while she is away from her desk. In addition, she is strongly advised to include a notice/disclaimer at the beginning of all her email, much like the disclaimer used on many fax cover sheets today, identifying the communication as privileged and instructing anyone other than the addressee not to read the document.<sup>12</sup>

There are also more high-tech means of protecting email. As discussed above, sender and recipient may identify themselves through a unique digital "signature" on each email that will help ensure that an email purporting to come from a particular person actually originated on that person's computer. The attorney and client may also agree to use the same Internet service provider that will guarantee the security of their email. Finally, also as discussed above, senders and receivers may encrypt their email so that it may be understood only by authorized recipients with the proper decoding software.<sup>13</sup>

Although email can put the attorney-client privilege at risk, so can having a conversation with a client that might be overheard. Despite the risks, it is necessary to speak with clients. As long as an attorney does so in a manner that creates and protects confidentiality, the communications should be protected. Similarly, as email becomes an increasingly important means of communication, it will become necessary to communicate with clients through email. If attorneys take reasonable steps to protect and maintain confidentiality, courts should understand that email communications are intended to be private and should therefore extend the privilege to this newfangled technology.

One serious problem with email is the relative ease with which it can be, and often is, disseminated to persons other than the intended recipient(s). Unlike a paper document, an email can be sent to untold numbers of people with the click of a mouse. This is most particularly a problem in the situation of a business as client, where the intended recipient's urge to forward and/or distribute emails is, by all appearances, irresistible. The further an email travels past its intended recipient(s), the more likely that it will lose its attorney-client privileged status. Courts have generally used one of two tests to determine whether a person is a representative of a client so as to have communications to or from that person protected by attorney-client privilege. At first, Texas adopted a control-group test implemented through a narrow definition of a "representative of the client" as one who has authority:

1. to obtain professional legal services on behalf of the client or
2. to act on advice rendered pursuant to that authority.<sup>14</sup>

The control-group test generally protects only statements made by the upper echelon of corporate management on the premise that only an employee who controls the action of the corporation can personify it,<sup>15</sup> and has been rejected by the United States Supreme Court as improper under the federal rules.<sup>16</sup>

The subject matter test adopted by the federal courts protects a communication made by an employee, at the direction of a corporate superior, for the purpose of securing legal advice. The subject matter of the communication must be within the scope of the employee's duties and must not be disseminated beyond those persons who need to know its contents.<sup>17</sup>

The Texas Supreme Court, through a rule change, adopted a broader definition more in line with the Federal rule.<sup>18</sup>

Under either of these tests, it is dangerous and potentially fatal to the attorney-client privilege for any client representative to forward email either from or to the client's attorney to any other employee or representative of the client. This is particularly true if the person receiving the forwarded email is not a management-level individual who is actively involved in the client's legal direction and decision-making.

One way for an attorney to force her client to ignore the urge to share attorney-client privileged information contained in email by forwarding the email is to select the non-forwarding feature if available, prior to sending such an email. This feature renders the email "dead" in the recipient's hands by preventing the recipient from forwarding the email. Obviously, a determined client can circumvent the non-forwarding feature by doing such things as printing out the email and distributing it manually, or by creating her own new email with the same information contained in the non-forwardable email. However, using the feature regularly, particularly when combined with a conspicuous "Do Not Copy, Forward or Otherwise Disseminate This Transmission Notice," could prevent disclosure to non-management client personnel.

## **B. Discovery and Investigative Privileges**

The most important thing to realize when considering the impact of email on the discovery process is that, subject to the investigative privileges such as the work product, party communication and witness statement privileges, email is discoverable.<sup>19</sup> An Illinois district court required a defendant drug manufacturer to produce thirty million pages of email at its own cost of \$50,000-\$70,000.<sup>20</sup> Discovered email has also provided the smoking gun in a number of sexual harassment and wrongful termination cases.<sup>21</sup>

So, how does an attorney protect her client from these potentially embarrassing and damaging documents? Two things can save an attorney and client many headaches in this age of computerized litigation: a document retention system and the investigative privileges.

Document retention systems are the mechanisms by which one deletes some computer records on a regular basis while archiving others. A retention system is legal and ethical if it is reasonable given the totality of the circumstances and is instituted in good faith.<sup>22</sup> Furthermore, a court will consider the frequency and severity of the legal issues at issue in the documents.<sup>23</sup>

An example of a legitimate document retention system is one that purges documents after the time period that a state or federal regulatory body requires the documents be kept.<sup>24</sup> However, once an attorney reasonably anticipates litigation, she should advise her client to cease all regularized document destruction.<sup>25</sup> Selective retention or destruction of documents separate from an organization's regularized retention system will pique a court's suspicion that a party has not managed its documents in good faith.<sup>26</sup>

While an attorney or client may be able to successfully delete some documents, it will be necessary to preserve others. One way to protect the preserved documents may be through investigative privileges. The investigative privileges extend to documents prepared by either the attorney or the client in anticipation of litigation, but the work product privilege is limited by an exception that ordinary work product may have to be produced if the requesting party cannot get the substantial equivalent, or to do so would impose an undue burden on the requesting party.<sup>27</sup>

However, work product that contains an attorney's mental impressions, conclusions, opinions and legal theories receives almost absolute protection.<sup>28</sup>

The "anticipation of litigation" test applied to documents to determine whether an investigative privilege applies is a trap for the unwary client, and attorneys must educate clients of the dangers of discoverable email. Generally, the anticipation of litigation test requires the existence of good cause to believe that litigation will be filed. As an example, the Texas Supreme Court has established a two-prong test to determine when good cause exists to believe that a lawsuit will be filed. Texas' two-prong test combines an objective test approach with a subjective good-faith standard:

...investigative documents are prepared in "anticipation of litigation" for purposes of TEX.R. CIV. P. 166b(3) if a) a reasonable person would have concluded from the totality of the circumstances surrounding the investigation that there was a substantial chance that litigation would ensue; and b) the party resisting discovery believed in good faith that there was a substantial chance that litigation would ensue and conducted the investigation for the purpose of preparing for such litigation...<sup>29</sup>

Although the National Tank court issued its test in the context of the party communications exemption, there is no reason that the "anticipation of litigation" test cannot also be applied to the other investigative privileges.<sup>30</sup> Courts can reasonably be expected to apply the same protection to attorney work product communicated across the Internet via email as that extended to documents prepared on computers and ultimately housed in a filing cabinets. However, until these issues are resolved in court, attorneys will be well advised to proceed with caution.

## **II. CONFIDENTIALITY/DIGITAL SIGNATURE**

Many trees have been killed and much ink spilled in the discussion of how online transactions can be made more private and less susceptible to interception and fraud. Two important components of a successful online transaction are confidentiality and authenticity. How can an online transaction be made relatively secure and the parties to the transaction made comfortable with its authenticity? Some of the most frequently used tools are encryption and digital signatures. Parties using these tools, plus a few other precautionary measures, can transact online with relative security. Attorneys also worry about the privacy component of communicating online, particularly in the context of attorney-client privilege. That issue will be addressed in Section II of this article.

### **A. Encryption.**

While there is only a small likelihood of any non-recipient third party successfully intercepting an email transmission that is correctly addressed, people still worry about the confidentiality of email transactions. And well they should, since email is no more safe for purposes of conveying confidential information than is the Postal Service, overnight delivery services, or a telephone discussion. Exactly. People disseminate incredibly confidential information on a regular basis through the mails, by overnight delivery, and by telephone. Why should they worry to any greater degree about the confidentiality of information disseminated online? The fact remains, however, that it may make good sense to take every reasonable precaution to avoid having confidential information end up in the wrong hands. This is especially true for information sent electronically, given the propensity to hit the "send" button without thoroughly reviewing the address given for the email recipient. Encryption may just be that additional "reasonable precaution" for sensitive information transmitted electronically.

Encryption is a method by which a message or document to be transmitted online can be scrambled, and thereafter can be unscrambled only by a person who has the right “key.” All others who do not possess the correct “key” cannot unscramble the message or document, as though it were in a foreign language known only to the sender and the intended recipient. A large number of commercial email packages today have an encryption program already built into them, and using these encryption programs is as simple as activating the encryption feature. The recipient must have a compatible encryption program, though, in order to utilize the proper “key” to unscramble the encrypted message.

## **B. Digital Signatures.**

The age when a valid contract meant a pen-and-ink signature on an original contract document is drawing to a close. Transactions handled exclusively on an electronic basis are more frequent than ever before. And why not? They are as quick, easy and, if proper precautions are taken, as reliable as traditionally-signed contracts. Texas Business and Commerce Code states that a document is signed when it contains “any symbol executed or adopted by a party with present intention to authenticate a writing.”<sup>31</sup> If a party intends that a digital signature be her symbol for authentication of a writing, all other parties to the writing need only satisfy themselves that the digital signature is, in fact, generated by the intending party. How is that satisfaction of authenticity achieved by the other party to the writing? Digital signatures are perhaps the best way of achieving satisfaction that the other party to the electronic writing is authentic and, thus, reliable.

### **1. What is a Digital Signature?**

Perhaps it is easiest to understand the concept of a digital signature by first saying what a digital signature is NOT. It most definitely is NOT a digitized copy of a person’s manual signature transmitted electronically. It also most definitely is NOT a given set of figures meant to forever identify a given person. Rather, a digital signature is a machine-generated series of bits which is then encrypted with the document sender’s private “key.” Visually, the digital signature appears as an undecipherable string of alphanumeric characters, and is unique for each document to which it is attached. The recipient of the document containing the digital signature can only un-encrypt the digital signature if he has access to the public “key” created by the sender. The recipient can also determine through the un-encryption process whether the document to which the signature is attached has been altered in any way subsequent to the time of application of the digital signature to the document.

### **2. Certification Authorities**

How can a recipient verify that the public “key”/private “key” connected with a given digital signature is a valid pair not generated by an imposter? Parties to electronic transactions are making more use than ever of third parties whose purpose is to verify the identity of the sender and certify that the public/private “key” pair is legitimate. These third parties are called “certification authorities,” and their purpose is to issue certificates verifying the relationship between the sender and the public key. A good overview of digital signatures can be found in the ABA Digital Signature Guidelines.<sup>32</sup> These Guidelines are available from the American Bar Association, Financial Services Division, P.O. Box 10892, Chicago Illinois 60610-0892, or can be downloaded at no cost from the ABA web site at [www.abanet.org/scitech/ec/isc](http://www.abanet.org/scitech/ec/isc).

### **3. The Legal Effect of a Digital Signature Under Texas Law**

Chapter 4A of the Texas Business and Commerce Code addresses funds transfers, and was perhaps the first Texas law to deal with electronic funds transfers and methods by which the

person or entity desiring the electronic funds transfer can identify himself or itself electronically with certainty (albeit without specifically mentioning digital signatures) to the financial institution transferring the funds. Texas has enacted several other laws dealing with the use of digital signatures. In 1997, Texas enacted Section 2.108(d) of the Texas Business and Commerce Code, which defines a digital signature as "...an electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature." Section 2.108(a) affirmatively empowers digital signatures with the same force and effect as a manual signature in transactions governed by Chapter 2 of the Texas Business and Commerce Code (generally the sale of goods). Texas also allows authentication of an electronic communication with any state agency or local government by digital signature, if the digital signature otherwise complies with regulations adopted by the Department of Information Resources.<sup>33</sup>

Clearly, the State of Texas has recognized the movement toward electronic communications in business transactions, and now by specific statutory enactment allows electronic applications for certain licenses and permits.<sup>34</sup>

- 
- <sup>1</sup> William P. Matthews, *Encoded Confidences: Electronic Mail, the Internet and the Attorney-Client Privilege*, 45 KAN. L. REV. 273, 274 (1996).
- <sup>2</sup> *Id.* at 277-78.
- <sup>3</sup> *Id.* at 278.
- <sup>4</sup> *Id.*
- <sup>5</sup> *Id.* at 279.
- <sup>6</sup> Robert L. Jones, *Client Confidentiality: A Lawyers's Duties with Regard to Internet Email*, Computer Law Section of the State Bar of Georgia (Aug. 16, 1995).
- <sup>7</sup> *Fisher v. United States*, 425 U.S. 391, 403 (1976).
- <sup>8</sup> Texas Disciplinary Rules of Professional Conduct §1.05.
- <sup>9</sup> Texas Rules of Evidence Rule 504(a)(5).
- <sup>10</sup> Matthews, *supra* note 8, at 286.
- <sup>11</sup> *Id.* at 285 (citing Clinton Wilder, *Lawyers in Cyberspace*, INFORMATION WEEK, Apr. 25, 1994, at 78).
- <sup>12</sup> Jones, *supra* note 13.
- <sup>13</sup> Jonathan Rose, *Email Security risks: Taking Hacks at the Attorney-Client Privilege*, 23 RUTGERS COMPUTER & TECH L. J. 179, 206 n.179 (1997).
- <sup>14</sup> *National Tank Co. v. Brotherton*, 851 S.W.2d 193, 198 (Tex. 1993); TEXAS RULES OF CIVIL EVIDENCE 503(a)(2).
- <sup>15</sup> *National Tank Co.*, 851 S.W.2d at 197.
- <sup>16</sup> *Upjohn Co. v. United States*, 449 U.S. 383, 396-97 (1981).
- <sup>17</sup> *Cigna Corp. v. Spears*, 838 S.W.2d 561, 565 n.1 (Tex. App.--San Antonio 1992, orig. proceeding) (citing 1 STEVEN GOODE ET AL., TEXAS PRACTICE: GUIDE TO THE TEXAS RULES OF EVIDENCE: CIVIL AND CRIMINAL §503.3 (2d ed. 1993 & Supp. 1996)).
- <sup>18</sup> Texas rules of Evidence 503(a)(2)(B).
- <sup>19</sup> Susan J. Silvermail, *Electronic Evidence: Discovery in the Computer Age*, THE ALABAMA LAWYER, May 1997, at 176.
- <sup>20</sup> *Id.* (citing *In re Brand Name Prescription Drugs Antitrust Litigation*, 1995 WL 360526 (N.D.Ill. June 15, 1995)).
- <sup>21</sup> *Id.* (citing *Knox v. State of Indiana*, 93 F.3d 1327, 1329 (7th Cir. 1996) (hostile work environment harassment and quid pro quo sexual harassment); *Meloff v. New York Life Ins. Co.*, 51 F.3d 372, 373 (2nd Cir. 1995) (employment discrimination and defamation); *Strauss v. Microsoft Corp.*, 856 F.Supp. 821, 822-23 (S.D.N.Y. 1994) (gender discrimination)).
- <sup>22</sup> Patrick R. Grady, *Discovery of Computer Stored Documents and Computer Based Litigation Support Systems: Why Give Up More than Necessary*, 14 J. Marshall Computer & Info. L. 523, 539 (1996) (citing *Lewy v. Remington Arms*, 836 F.2d 1104, 1112 (8th Cir. 1988)).

---

<sup>23</sup> *Id.*

<sup>24</sup> *Id.* at 532-33 n.49.

<sup>25</sup> *Id.* at 540.

<sup>26</sup> *Id.*

<sup>27</sup> FED. R. CIV. P. 26(b)(3).

<sup>28</sup> *Id.*

<sup>29</sup> *National Tank Co.*, 851 S.W.2d at 195.

<sup>30</sup> *Boring & Tunneling Co. v. Salazar*, 782 S.W.2d 284, 286 (Tex. App.--Houston [1st Dist] 1989, orig. proceeding).

<sup>31</sup> Tex. Bus. Com. Code. Ann. §1.201(39).

<sup>32</sup> Information Security Committee, Electronic Commerce Division, Science and Technology Section, American Bar Association, *Digital Signature Guidelines* (August 1, 1996)

<sup>33</sup> Tex. Gov. Code. Ann. § 2054.060.

<sup>34</sup> *See* Tex. Trans. Code §§ 201.931-201.934, 623.074.