CONFIDENTIALITY AND PRIVILEGE ISSUES ARISING FROM ELECTRONIC COMMUNICATIONS

Richel Rivers
Hilgers & Watkins, P.C.
P. O. Box 2063
Austin, TX 78768-2063
(512) 476-4716

Advanced Estate Planning and Probate Course
June 5-7, 2002
Dallas, Texas
Chapter 25

TABLE OF CONTENTS

CONFIDENTIALITY AND PRIVILEGE ISSUES ARISING FROM ELECTRONIC COMMUNICATIONS

I. Introduction

Is it possible to enjoy the benefits of technology in our work and still keep our clients' secrets? This paper will explore the ramifications of the use of technology in the context of a legal practice which compels our professional attention to the risks of disclosure of our clients' secrets. The challenge involves the application of the traditional rules of privilege to the realities of a modern legal practice. We will review the rules and the technology issues, then focus on the conclusions drawn by courts and our profession's policing mechanisms concerning our professional responsibilities in this brave new cyber-age.

II. Confidentiality Obligations

A. Nature and Beneficiaries of the Privilege

The work of attorneys is protected by one of the oldest recognized privileges of confidentiality under the common law. ***Upjohn Co. v. United States***, 449 U.S. 383, 389, 101 S.Ct. 677, 682 (1981); ***Hunt v. Blackburn***, 128 U.S. 464, 470, 9 S.Ct. 125, 127 (1888). The United States Supreme Court has repeatedly recognized that:

> The [attorney-client] privilege is intended to encourage "full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and the administration of justice."

Upjohn, supra, at 389, 101 S.Ct. at 682; ***Swindler & Berlin v. U.S.***, 118 S.Ct. 2081, 2084 (1998) [lawyer's notes of conference w/ Vincent Foster re: White House Travel Office dismissals remained confidential after Foster's suicide].

The attorney-client privilege survives the death of the client. ***Swindler & Berlin v. U.S.***, *supra*. In upholding the almost universal maintenance of the privilege after a client's death, the Supreme Court dismissed the Independent Counsel's arguments for abolishing the privilege in the context of a criminal investigation, and commented:

> Knowing that communications will remain confidential even after death serves a weighty interest in encouraging a client to communicate fully and frankly with counsel. … Clients may be concerned about reputation, civil liability, or possible harm to friends or family. Posthumous disclosure of such communications may be as feared as disclosure during the client's lifetime.

Id., at 2086.[1]

And the Supreme Court has observed that the attorney-client privilege is perhaps more significant to the administration of justice than even the Fifth Amendment privilege against self incrimination:

> [T]he privilege serves much broader purposes. Clients consult attorneys for a wide variety of reasons, only one of which involves possible criminal liability. Many attorneys act as counselors on personal and family matters, where, in the course of obtaining the desired advice, confidences about family

[1] Some jurisdictions provide that the privilege may not survive after the client's death if communications are sought to be disclosed in litigation between the testator's heirs; the rationale for such disclosure is that it furthers the client's intent. ***Swindler & Berlin v. U.S.***, *supra* at 2085; *see also* Rule 503(d)(2), Texas Rules of Evidence.

> members or financial problems must be revealed in order to assure sound legal advice. The same is true of owners of small businesses who may regularly consult their attorneys about a variety of problems arising in the course of the business. These confidences may not come close to any sort of admission of criminal wrongdoing, but nonetheless be matters which the client would not wish divulged.

Id. at 2086.

It is our clients who are protected by the confidentiality privilege. In ***United States v. United Shoe Machinery Corp.***, 89 F. Supp. 357 (D. Mass. 1950), the court held that the privilege applies in the federal courts if the following conditions are met:

(1) the asserted holder of the privilege is or sought to become a client;
(2) the person to whom the communication was made is a member of the bar or is the subordinate of a member of the bar;
(3) the communication relates to a fact of which the attorney or his subordinate was informed of by his client without the presence of strangers for the primary purpose of obtaining either a legal opinion, legal services or assistance in a legal proceeding and not for the purpose of committing a crime or tort; and
(4) the privilege must be claimed and not waived by the client.

B. Confidentiality Obligations in Texas

1. Confidentiality Rule

Our obvious duties start with the Rules. *Texas Disciplinary Rules of Professional Conduct* (*TDRPC*). TDRPC Rule 1.05(b) is the basic confidentiality rule, and it mandates:

> Except as permitted by paragraphs (c) and (d), or as required by paragraphs (e), [sic] and (f), a lawyer shall not knowingly:
>
> (1) Reveal confidential information of a client or a former client to:
>
> (i) a person that the client has instructed is not to receive the information; or
>
> (ii) ***anyone else***, other than the client, the client's representatives, or the members, associates, or employees of the lawyer's firm. [emphasis supplied]

Comment 1 to Rule 1.05 reflects the common law heritage of the confidentiality obligations:

> Both the fiduciary relationship existing between lawyer and client and the proper functioning of the legal system require the preservation by the lawyer of confidential information of one who has employed or sought to employ the lawyer. Free discussion should prevail between lawyer and client in order for the lawyer to be fully informed and for the client to obtain the full

> benefit of the legal system. The ethical obligation of the lawyer to protect the confidential information of the client not only facilitates the proper representation of the client but also encourages potential clients to seek early legal assistance. [Emphasis added.]

In an often-confusing use of language our Rules protect "confidential information," which consists of both "privileged" and "unprivileged" client information. Rule 1.05(a), *TDRPC* sets out these definitions:

> "Confidential information" includes both "privileged information"and unprivileged client information." "Privileged information" refers to the information of a client protected by the lawyer-client privilege of [the Rules of Evidence]. "Unprivileged client information" means **ALL** information relating to a client or furnished by the client, other than privileged information, acquired by the lawyer during the course of or by reason of the representation of the client. [Emphasis added.]

While our Rules do provide some authorization – and indeed some obligation -- for lawyers to reveal confidential information, the overriding mandate requires that a lawyer "shall not knowingly reveal confidential information to anyone or use confidential information to the disadvantage of the client unless the client consents after consultation. Rule 1.05(b), *TDRPC*. So what we know about the effects of our use of technology is crucial, and how we explain it to our clients to obtain their consent to use the technology is important.

2. The Client's Privilege

Our obligation as lawyers to preserve the confidentiality of our clients' information is set out in the *TDRPC* Rule 1.05 set out above. But the privilege itself belongs to the client, and the strength of the privilege is tested by the extent to which a client (or his representative) may be compelled to disclose confidential information. Our *Texas Rules of Evidence* provide that in general, no person has a privilege to refuse to be a witness, disclose any matter, produce any object or writing, or prevent another from doing so, *except* as otherwise provided by law or the rules. Rule 501, *Texas Rules of Evidence* (*TRE*).

The Lawyer-Client Privilege is set out in *TRE* 503, which essentially grants to the client a privilege to:

> … refuse to disclose and to prevent any other person from disclosing confidential communications made for the purpose of facilitating the rendition of professional legal services to the client…

The Rule also defines a communication as "confidential" if it is:

> … 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.

TRE 503(a)(5).

The scope of the privilege is limited to such communications made by and between the client and his representatives. *TRE* 503(b)(1). And even that limited privilege is narrowed by exceptions involving a client's intent to commit a crime or fraud, claimants through the same

deceased client, disputes between the client and lawyer, documents verified by a lawyer, and joint client representations. *TRE* 503(d).

3. The Privileged Container

Our clients' privilege of confidentiality is only good for so long as it is protected. In order to prevent compulsory disclosure of confidential information, it must be preserved within the protected container of the attorney-client relationship and it must be asserted appropriately.

The protected sphere consists generally of the lawyer, the client, and the "representatives" of the client and lawyer. *TRE* 503(a) Texas has somewhat enlarged that protected sphere by its expansion of the definition of a client's "representatives" to include:

> (A) a person having authority to obtain professional legal services, or to act on advice thereby rendered, on behalf of the client, or
> (B) any other person who, for the purpose of effectuating legal representation for the client, makes or receives a confidential communication while acting in the scope of employment for the client.

TRE 503(a)(2). This "subject matter" test was adopted by the Supreme Court in a 1998 rule change that replaced the stricter "control group" test set out by the Texas Supreme Court in ***National Tank Co. v. Brotherton***, 851 S.W.2d 193, 197-198 (Tex. 1993).

So communications must be contained within this protected group to remain privileged. It is the lawyer's duty to keep the container intact.

III. Unauthorized Interception

Both state and federal law prohibit and provide sanctions for wiretapping. Our expectation of the privacy of our confidential communications as against unauthorized interception is reasonable in light of the criminal jeopardy an intruder faces in obtaining information transmitted electronically. And to a large extent, our expectation of privacy of our confidential communications diminishes the legal jeopardy of our use of technology which may not in fact protect that privacy. ***Katz v. United States***, 389 U.S. 347 (1967) [electronic surveillance of defendant's telephone call violated the privacy to which he was entitled in a phone booth]. An overview of the applicable criminal statutes that were enacted following *Katz* is in order:

A. Federal Wiretap Statute

The federal wiretap statute prohibits the interception and use of illegally intercepted communications. 18 U.S.C. §2510 *et seq.* The statute prohibits interception of oral or wire communications by use of any electronic, mechanical or other device. 18 U.S.C. §2511. The penalty for violation of the statute is fine or imprisonment for up to 5 years, or both. With some exceptions set out in the statute, the criminal sanctions apply to any person who:

> (a) intentionally *intercepts, endeavors to intercept, or procures any other person to intercept* or endeavor to intercept, any wire, oral, or electronic communication;
> (b) intentionally *uses, endeavors to use, or procures any other person to us*e or endeavor to use any electronic, mechanical, or other device to intercept any oral communication (when the device is used in wire communication, radio communication, is sent through the mail or transported in interstate or foreign commerce, or involves a business affecting interstate or foreign commerce);

> (c) intentionally *discloses, or endeavors to disclose, to any other person the contents* of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through interception in violation of the statue;
> (d) intentionally *uses, or endeavors to use, the contents* of any wire, oral, or electronic communication with knowledge it was obtained in violation of the statute; or
>
> (e) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by the criminal investigation provisions of the statute.

The federal Wiretap Statute also prohibits the use of information obtained in violation of the law:

> "Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter."

18 U.S.C. §2515.

In enacting these statutes, Congress recognized a strong public policy against the interception of communications particularly by law enforcement officials, and in service of that policy eliminated the evidentiary usefulness of communications obtained unlawfully. But being a criminal statute, it was read narrowly, and until the statute was subsequently amended would not have given much protection to all the forms of electronic communications. For example, the Act has been read to be limited to "interception" of communications, not seizure of the communications once stored, so that law enforcement officials could use the information on a seized computer. ***State v. One Pioneer CD-ROM Changer***, 891 P.2d 600 (Okla.Ct.App. 1994) [rejected owner's contention that seizure of computer containing 150,000 email messages was an interception]. Amendments to the Wiretap Statute have expanded the definitions of protected information to incorporate a greater scope of the technology field.

B. Amendments Expanding Electronic Communications Privacy

The Electronic Communications Privacy Act of 1986 (ECPA) and Communications Assistance for Law Enforcement Act (CALEA) amendments to the federal wiretap law extends to "electronic communications" the same protections against unauthorized interceptions that the wiretap law provide for "oral" and "wire" communications via common carrier transmissions. *See* 18 USC §§ 2510-2520, 2701-2711 (1994); ***Brown v. Waddell***, (4th Cir. 1995), 50 F.3d 285. "Electronic communications" are defined as any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but do not include -

a) any wire or oral communication;

b) any communication made through a tone-only paging device; or

c) any communication from a tracking device (as defined in section 3117);

d) electronic funds transfer information stored by a financial institution in a

> communications system used for the electronic storage and transfer of funds.

See 18 USC §2710.

Because electronic mail utilizes phone lines, television cables, and certain types of fiber optic cables, it falls within the protection of the federal statutes. It is a federal crime to intercept electronic mail while it is stored, in route, or after receipt. Furthermore, the statutes provide in general that it is an offense to:

> (1) intentionally access without authorization a facility through which an electronic communication service is provided; or
> (2) intentionally exceed an authorization to access that facility; and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

18 U.S.C. §2701.

The punishment for an offense under the federal statutes includes fine or imprisonment from 6 months to 2 years, or both, depending on the purpose for which the offense is committed.

Also, §2707 of the federal statute creates a civil cause of action, which includes all appropriate equitable or declaratory relief, damages, including actual damages, reasonable attorney's fees and litigation costs.

An early case illustrates the utility of the ECPA to the protection of e-mail communications. A computer system used by an employee of Steve Jackson Games, Inc. (SG) was seized by the federal government under warrant, because the employee was suspected of hacking into a Bell Telephone computer system. An electronic bulletin board service for SG subscribers was on the seized system. The Secret Service read the stored and undelivered bulletin board e-mail, and during the course of the investigation, some of the stored information was deleted. SG subsequently sued the federal government, and the court found that the government had violated the Privacy Protection Act and Title II of the ECPA. Damages were awarded to SG. ***Steve Jackson Games, Inc. v. U.S. Secret Service***, 36 F.3d 457 (5th Cir. 1994).

These statutes have significantly strengthened the expectation of privacy with respect to, for example, cordless cell phones. Even publicly accessible cordless telephone calls using the most vulnerable transmission technology is protected from unauthorized interception. ***United States v. Mathis***, 96 F.3d. 1577 (11th Cir. 1996), *cert. denied*, 520 U.S. 1213 (1997) ***Askin v. McNulty***, 47 F.3d 100 (4th Cir. 1994), *cert. denied* 116 S.Ct. 382 (1995). But the nuances of the statutes, and the criminal investigation circumstances giving rise to most interpretations of the statutes, continue to present uncertainties in the strength of our reliance upon the statutes to support our expectation of privacy. *See*, R. Scott Simon, *Searching for Confidentiality in Cyberspace: Responsible Use of E-Mail for Attorney-Client Communications*, 20 Hawaii L. Rev 527 (summer/Fall 1998)

C. State Statutes

Texas also has enacted civil and criminal statutes addressing wiretapping. Sections 123.001 - 123.004 of the *Texas Civil Practice and Remedies Code* create a civil cause of action for a person whose communication is intercepted in violation of the statute. The statute permits damages and injunctive relief prohibiting divulgence or use of information obtained by an interception of this nature. This statute applies only to interception of communications by "aural" acquisition of the contents of a communication. It does not include purely verbal communications that are

not transmitted by wire or cable, and additionally does not apply to electronic mail. Section 123.002 of this wiretap statute grants a cause of action against any person who "divulges information" that was obtained by an illegal wiretap.

Additionally, Section 16.02 *et seq.* of the *Texas Penal Code* makes unauthorized interception or use or disclosure of the contents of the interception a felony. And Section 16.04, *Texas Penal Code*, makes it a Class A misdemeanor to obtain, alter, or prevent authorized access to a wire or electronic communication while the communication is in electronic storage, essentially by obtaining access without authorization or exceeding authorization. *See also* definitions set out in §18.20, *Texas Code of Criminal Procedure*.

D. Loopholes

Lest we become complacent by the criminalization of unauthorized interception of our electronic communications, we should remember that the criminal statutes have been found to be unenforceable in the context of certain interceptions.

The United States Supreme Court recently overturned §2511(1) of the federal wiretapping statue, the provision which provides criminal sanctions for anyone who willfully intercepts, uses or discloses illegal oral or wiretap communications. ***Bartnicki v. Vopper***, 121 S.Ct. 1753 (2001). ***Bartnicki*** involved the use of an illegally intercepted cellular telephone conversation between two members of a union representing teachers in a contentious collective bargaining situation in a Pennsylvania high school. The interception was made by an unknown person who disclosed the contents of the interception to a radio commentator, who then played the tape on his public affairs talk show. The contents were also broadcast by another radio station and published by some local newspapers. The Court found that the disclosures to the media and the subsequent disclosures by the media to the public violated both the state and federal statutes, but held these statutes unconstitutional on First Amendment grounds. In doing so, the Court identified the provision of the federal statute, 18 U.S.C. 2511(1)(c), and its Pennsylvania counterpart as "content-neutral" laws of "general applicability" because the statutes single out the communications by virtue of the illegal nature of their interception. The statutes do not distinguish based on the contents of the communication. The Court also focused on the fact that *the parties to be punished in this case were not those that illegally intercepted the communication in the first place*; it saw little purpose in punishing someone other than the person whom the law was designed to punish. *Id*. at 10. Significantly, however, the Court focused on the public policy nature of the communications involved. The Court was concerned with the fact that this statute imposed "sanctions on the publication of truthful information of public concern," and that this interest outweighed that of privacy of communication. *Id*. at 12. An unknown party's illegal activities were not enough to justify removing the protection of the First Amendment in a dispute so clearly involving public concern.

In addition to the proposition that ***Bartnicki*** dilutes the strength of the wiretapping statutes as a tool to prevent admissibility of wiretapped evidence, several exceptions to the general prohibition against use of intercepted oral and wire communications exist. Section 2511(2)(d) of the federal statute provides that it is not unlawful for a person to intercept an oral or wire communication where this person is one of the parties to the communication or where one of the parties has given prior consent to such an interception. The court in ***Pollock v. Pollock*** extended the consent exception in holding that a parent may vicariously consent on behalf of a minor child to the interception of a communication as long as the parent can demonstrate "a good faith, objectively reasonable basis for believing that it is necessary and in the best interest of the child." ***Pollock v. Pollock***, 154 F.3d 601, 610 (6th Cir. 1998). Also, several courts have interpreted the ordinary business exception set out in 18 USC §2510 (5)(a)(i) as intending to cover tape

recorders attached to extension telephones in personal residences. ***Scheib v. Grant***, 22 F.3d 149 (7th Cir. 1994); ***Newcomb v. Ingel***, 944 F.2d 1534 (10th Cir. 1991); ***Janecka v. Franklin***, 843 F.2d 110 (2d Cir. 1988).

Another exception to the general federal prohibition concerns the admissibility of illegal interceptions in a family law context. For example, marital conversations have been found admissible in order to show that one party had been blackmailed or coerced into a court-approved agreement**.** ***In re: Marriage of Lopp***, 378 N.E.2d 414, 419 (1986). In that case, the wife was alleging that such communications had been used to coerce her into signing a custody agreement.

And, other conversations obtained in violation of the federal wiretapping statute have been held admissible for impeachment purposes. ***Jacks v. State***, 394 N.E.2d 166 (1979). The 4th Circuit even held admissible an illegally obtained taped conversation offered to impeach a denial of adultery set out in an affidavit. ***Culbertson v. Culbertson***, 143 F.3d 825, 827 (4th Cir. 1998).

Two federal Circuits have held that the criminal sanctions set out in the federal wiretap statute do not apply to spousal communications. In ***Simpson v. Simpson***, the 5th Circuit held that the federal statute did not apply to a husband's wiretapping of his wife's conversations while they were still married and living together. ***Simpson v. Simpson***, 490 F.2d 803, 809 (5th Cir.), *cert. denied*, 419 U.S. 897 (1974). In ***Simpson***, the Court held that the statute was not sufficiently definite and specific to create a federal cause of action in favor of one spouse against the other spouse for the interception of communications prohibited by the federal statute. The court based its reasoning on the tradition federal courts have typically followed of leaving family matters to state courts; the court stated that it did not believe Congress had intended to act counter to this tradition. The 2nd Circuit likewise found that interspousal wiretaps were a matter of marital disputes, an area typically left to the discretion of the states. ***Anonymous v. Anonymous***, 558 F.2d 677 (2d Cir. 1977). In ***Anonymous***, a father tape-recorded his 8 year old son's conversations with the child's mother. The Court analogized this activity to listening to the conversation on an extension telephone, which is not prohibited by the federal statute. The court further found that the actions by the father did not rise to the level of criminal conduct intended to be punished by the federal statute.

A majority of courts, however, have found no exception for intercepted wire or oral family communications. The most frequently cited case for the majority position, ***United States v. Jones***, was a criminal case finding that the federal wiretap statute intended "to reach private electronic surveillance and that Congress was aware that a major area of use for surveillance techniques was the preparation of domestic relations cases. ***United States v. Jones***, 542 F.2d 661, 668 (6th Cir. 1976). This case involved a husband who was criminally charged with intercepting phone conversations of his estranged wife and using these contents to obtain a divorce (in violation of the federal statute). *Id.* at 663. In addition to the 6th circuit, the 4th, 8th and 10th Circuits have found no Congressional intent to except such willful, intercepted spousal communications. ***Pritchard v. Pritchard***, 732 F.2d 372, 374 (4th Cir. 1984); ***Kempf v. Kempf***, 868 F.2d 970, 973 (8th Cir. 1989); ***Heggy v. Heggy***, 944 F.2d 1537, 1539 (10th Cir. 1991); ***Platt v. Platt***, 951 F.2d 159 (8th Cir. 1989).

In applying the federal statute, state courts have also refused to recognize a spousal exception. Alabama courts have found no exception for spousal wiretapping, even for impeachment purposes, when the intercepting person was not a party to the communication or did not have the consent of either participating party. ***Ex parte O'Daniel***, 515 So.2d 1250, 1252 (Ala. 1987); ***Hudson v. Hudson***, 534 So.2d 617 (Ala. Civ. App. 1988). A Missouri court held that the federal statute was clear and unambiguous in its blanket application to all wiretaps not authorized specifically by the statute, so any communications or evidence obtained in violation of this blanket prohibition,

even those from spousal communications, are not admissible. ***Stamme v. Stamme***, 589 S.W.2d 50, 53 (Mo.App. E.D. 1979).

Similar to the federal statute, §16.02 of the Texas Penal Code makes unauthorized interception or use of disclosure of the contents of the interception a felony. Also, Article 18.20 §2 of the Texas Code of Criminal Procedure prohibits use of the contents of an intercepted communication, and any evidence derived from an intercepted communication in any trial except civil trials, arising out of a violation of the Penal Code, code of Criminal Procedure, Controlled Substances Act, or Dangerous Drug Act. The state penal code and criminal procedure provision appear to prohibit interception of the same communications addressed by the federal statute. It is not a violation of the state or federal statutes if a party to the communication consents to the interception or if the person intercepting the communication is also a party to the communication.

Texas courts have generally declined the opportunity to follow the ***Simpson*** and ***Anonymous*** cases to attach a spousal immunity exception to the applicable federal or state wiretap statutes and except marital cases from the prohibition against use of illegal wiretaps. *See* ***Kent v. State***, 809 S.W.2d 664 (Tex. App. - Amarillo 1991, writ ref'd); ***Turner v. PV Int'l Corp.***, 765 S.W.2d 455 (Tex. App. - Dallas 1988, writ den'd per curium 778 S.W.2d 865); ***Collins v. Collins***, 904 S.W.2d 792 (Tex. App. - Houston [1st Dist.] 1995, writ denied).

The courts in ***Turner*** and ***Collins*** held that tape recordings and transcripts of those recordings made in violation of the state or federal wiretap statutes are inadmissible. The ***Collins*** court noted that §§123.001 - 123.004 of the Texas Civil Practice & Remedies Code did not expressly provide for the exclusion of illegally intercepted communications from evidence in civil cases. ***Collins***, *id.* at 796. The court found that the statutory provision for recovery of damages and injunctive relief were sufficient to overcome the presumption of admissibility under Rule 402 of the Texas Rules of Civil Evidence. *Id.* At 799 ["to permit such evidence to be introduced at trial when it is illegal to disseminate it would make the court a partner to the illegal conduct the statute seeks to proscribe."] Also, the ***Collins*** Court found nothing in either the Texas Constitution or common law to suggest "that the right of privacy is limited only to unmarried individuals," and found that spouses have the same rights of privacy under both statutes. *Collins* at 797.

The El Paso court interpreted the Texas statute, *V.T.C.A., Penal Code § 16.02(b)(1),* as applying to spouses, thereby rendering any intercepted wiretaps unlawful. ***Duffy v. State***, 22 S.W.3d 17, 24 (Tex. App. - El Paso, 2000). The *Duffy* Court declined to follow *Simpson*, and agreed with ***Collins*** holding that the common law and constitutional right of privacy recognized by Texas courts is not limited to unmarried individuals. The court concluded that "a spouse has a right of privacy under Section 16.02." *Id.* at 24.

Nonetheless, the Texas courts recognize the general exception to the blanket prohibition of spousal wiretaps when the intercepting party is a party to or has consented to the interception. ***Kotrla v. Kotrla***, 718 S.W.2d 853, 855 (Tex.. App. - Corpus Christi, 1986). In ***Kotrla v. Kotrla***, the husband taped an in-person conversation with his wife in which she admitted to having used cocaine and marijuana. *Id.* at 855 (Tex. App. -- Corpus Christi 1986, writ ref'd n.r.e.) While the wife's argument on appeal centered around the theory that this tape should not have been admissible because she had not consented to being taped, the court disagreed, holding that the state interception of communications statute does not prohibit this type of interception so long as one party consents to the taping. In the ***Kotrla*** case, the husband doing the taping was the party who consented, so the recording was admissible. *Id.* at 855.

Arguably, illegally-taped telephone conversations may be used for impeachment purposes, provided the recording satisfies a seven-point test for admissibility. ***Cummings v. Jess Edwards***, 445 S.W.2d 767, 773 (Tex. Civ. App. – Corpus Christi 1969, writ ref'd n.r.e.).

This seven-point test requires that the offering party demonstrate:

1) that the recording device was capable of taking testimony;
2) that the operator of the device was competent;
3) the authenticity and correctness of the recording;
4) that changes, additions, or deletions have not been made;
5) the manner of the preservation of the recording,
6) the identity of the speakers; and
7) that the testimony elicited was voluntarily made without any kind of inducement.

Id.

Finally, a court may look to all the surrounding circumstances to determine whether information obtained from wiretapping was wrongfully considered in a civil case. The Austin Court ruled that information obtained from wiretapping would be admitted if the information could have been gathered through means other than that of wiretapping. ***Fabian v. Fabian***, 765 S.W.2d 516 (Tex. App. - Austin 1989, no writ). In ***Fabian***, the husband admitted at trial he had attached a recording device to the family telephone. While the tapes were not admitted, the wife objected to introduction of evidence regarding an affair she was having, claiming the only way the husband knew about the affair was through telephone conversations taped in violation of the Texas Penal Code §16.02. The court allowed the evidence to be admitted because there were other means of discovering this information. The husband had a private investigator check motel records, the husband followed the wife, and the husband also questioned her friends and co-workers. *Id*. at 519.

IV. Unintended Dissemination

Electronic communication with clients or about client matters is now commonplace in our practices, and is likely to become universal throughout the legal profession. *See* Charles R. Merrill, *E-mail for Attorneys from A to Z*, 443 Practicing Law Institute/Patents 187, Dec. 1996, at 189. The problem of e-mail and fax confidentiality is predicated on the vulnerability of the technology to unintended interception, but is significantly compounded by the undisciplined use of the communication tools by both the writer and the recipient. And, in a trial context, these records are often discoverable and can be seriously injurious to the client.

For a helpful description of the technological nuances of electronic communications, find Clint F. Sare's articles on *Attorneys and the Internet: What You Don't Know Can Hurt You. See* May 8, 1998 coursebooks on SboT program entitled *What Attorneys Should Know About the Internet.* He explains in both understandable and frightening detail the vulnerabilities of our circuit switched telephone networks, our packet switched internet networks, and our digital signatures and (hopefully) incorporated cryptographic algorithms. We must conclude that we cannot rely on the integrity of our communication systems to withstand error or intrusion into the content of the material transmitted.

Certainly, we can take some steps beyond the commonplace confidentiality notices to protect electronic communications. For example, when setting up email protocols, the sender and recipient may identify themselves through a unique "signature" on each email that will ensure that an e-mail 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 provider that will guarantee the security of their email. Encryption tools can add at least another layer of protection in that the email should be accessible only by authorized recipients with the proper decoding software. *But see* Jonathan Rose, *E-mail Security Risks: Taking Hacks at the Attorney-Client Privilege*, 23 Rutgers Computer & Tech L. J. 179, 206 n179 (1997)[encryption programs are also vulnerable].

.Even having taken such precautions against unintended disseminations, lawyers

should disclose to their clients the extent of the risk that privileged information will escape the protected sphere, and when the client is relatively unsophisticated technologically, should consider obtaining the client's consent to utilize electronic communication mediums. The general considerations are the classes of people who could force access to the information and the circumstances where the information could be carelessly diverted.

A. Authorized Access

If absolute secrecy of information is a virtue with respect to any communication, then the lawyer must impress upon his client the certainty that the information is at least open to lawful scrutiny by the service providers. When enacting the wiretap statutes, Congress recognized the need for communications providers to have access to the messages it manages. *See* 18 U.S.C. §2511(2)(a)(i) (1994) [deems lawful "for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service … to intercept, disclose, or use that communication in the normal course of his employment"]; *see also* 18 U.S.C. §2701(c)(1) [provides an exception for access by "the person or entity providing a wire or electronic communication service."]. This access is, however, limited in that the use of the information may only be made in the normal scope of the provider in an activity which is a necessary incident to the rendition of service. *Id.* So, the privilege protections should still provide protection against dissemination beyond that operational sphere. *See* ***People by Vacco v. Mid Hudson Medical Group***, 877 F.Supp. 143 (S.D.N.Y. 1995) [motion to compel production of teletype communications denied because analogous ADA prohibitions against teletype relay operators disclosing contents of teletype communications preserved the deaf person's expectation of confidentiality in their communications despite the operator's overhearing and participating in the conversations].

We must also be aware of the risks of retention and retrieval of stored confidential information. Not only is the information deliberately stored by our own machines and systems according to our document retention protocols, it is also often lawfully stored and accessible to the service providers.

With respect to the confidential documents we may store in the ordinary course of our business, presumably a legitimate document retention system establishes guidelines for destruction of documents after the time period that any state or federal regulatory body requires the documents be kept. But the Enron scandal has reminded us that retention systems are not a perfect cover for avoiding even criminal liability. Certainly, once an attorney reasonably anticipates litigation about any matter as to which her own or a client's documents may become pertinent, she should immediately cease, and advise her client to cease all regularized document destruction. Then, the discoverability of the communications may be addressed in the context of the applicable privileges rather than in the context of a threat of obstruction of justice or spoliation of evidence charges.

B. Discoverability

Despite even the most secure protocols for the use of electronic communications, litigation rules may make the communications both discoverable and admissible into evidence. In general, subject to the investigative privileges and attorney work product, party communication and witness statement privileges, electronic communications which may lead to the discovery of admissible evidence is discoverable. It is the exceptions to discoverability that guide our practice of communicating confidential information by electronic means.

Investigative Privilege: If communications involve a matter that eventually results in litigation, they are a clear target for discovery requests. The protection against client communications about such matters is set out in the "anticipation of litigation" test for maintaining confidentiality of communications pertinent to the investigation of matters that are reasonably likely to result in litigation. Rule 192.5(a)(2), *TRCP*. Whether this investigative privilege applies

requires a showing of good cause to believe that litigation will be filed. In the context of the party-communications exemption from discovery, the Texas Supreme Court requires a two-prong showing to determine when good cause exists to believe that a lawsuit will be filed:

> 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.

National Tank Co. v. Brotherton, 851 S.W.2d 193 (Tex.1993). A communication made in anticipation of litigation is discoverable only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of the party's case and that the party is unable without undue hardship to obtain the substantial equivalent of the material by other means. Rule 192.5(b)(2). ***In re: Jimenez***, 4 S.W.3d 894 (Tex.App.—Hou. [1st Dist. 1999) So, the content of the communications may provide a barrier to forced disclosure of such communications regardless of the technological means for distribution.

Attorney Work Product Privilege: The work product of an attorney is privileged, subject to the exceptions of TRE503(d), which pertains to work product as well as attorney-client privileges. ***Owens-Corning Fiberglass Corp. v. Caldwell***, 818 S.W.2d 749 (Tex. 1991) [the privilege is not limited documents that were prepared in the particular case for which discovery is sought]. The attorney work product privilege is limited by an the 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. F.R.C.P. 26(b)(3); Rule 192.5, T.R.C.P. "Core" work product, the work of an attorney that contains mental impressions, opinions, conclusions or legal theories, is not discoverable. Rule 192.5(b)(1). But other work product can be discoverable if the substantial need and undue hardship showing is made. This is a crucial vulnerability in the context of our communications incident to legal services, particularly since so much of our technology based communication is stored indefinitely.

C. Careless Publication

The most disconcerting aspect of the use of technologically sophisticated communication mediums is our tendency to abuse it. Mistaken transmissions are surprisingly common, and opinion seems to be divided in courts across the country as to the treatment of privilege in the event of an inadvertent or accidental disclosure. ***United States v. Keystone Sanitation Company***, 885 F.Supp. 672, reconsideration denied 899 F.Supp. 206 (M.D.Pa. 1995) [inadvertent production of email constituted waiver of attorney-client privilege]. The ***Keystone*** court considered several factors in determining whether the documents had lost their privilege through inadvertent disclosure:

> (1) the reasonableness of the precautions taken to prevent the inadvertent disclosure in view of the extent of the document production;
> (2) the number of inadvertent disclosures;
> (3) the extent of the disclosure;
> (4) any delay and measures taken to rectify the disclosure; and
> (5) whether the overriding interests of justice are or are not served by protecting the party against its error.

Id. at 676. Resort to these standards to determine whether an attorney has taken adequate measures to protect confidential information is a natural

extension of other examinations of an attorney's precautionary measures. *See* ***Suburban Sew 'N Sweep v. Swiss-Bernina***, 91 FRD 254 (N.D.Ill. 1981) [plaintiffs recovered otherwise privileged documents by searching dumpsters used by defendant; court held that defendant had not taken adequate precautions to ensure confidentiality considering the likelihood of disclosure]. There, the court warned that we "need to take all possible precautions to insure confidentiality" in order to preserve privilege. *Id*. at 260. *See also* ***Amgen Inc v. Hoechst Marion Roussel Inc*** (D.Mass 1/2000) [paralegal's carelessness in including a box of privileged documents among the 200,000 documents sent to an outside copy vendor for production to opposing counsel waived the privilege because inadequate precautions were taken to avoid such mistakes].

Texas also adopts the rule that adequate precautionary measures must be taken in order to preserve the privilege of confidentiality of inadvertently disclosed information. ***Granada Corp v First Court of Appeals***, 844 S.W.2d 223 (Tex. 1992). In *Granada*, the Court found that the privilege had been waived as to attorney-client memos that were inadvertently produced in response to discovery requests. The Court characterized inadvertent disclosures as either voluntary (as to which privileges are waived under Rule 511, *T.R.E.*) or involuntary (as to which the privileges remain intact), indicating that the dsclosure is involuntary only if efforts reasonably calculated to prevent disclosure were unavailing. Other factors the Court found to be significant are the delay in rectifying the error, the extent of any inadvertent disclosure and the scope of discovery. The Court admonished that a party seeking to protect documents inadvertently disclosed must show more than inadvertence; the party must show circumstances demonstrating the involuntariness of disclosure. *See also* ***Alldread v, Grenada***, 988 F.2d 1425 (5th Cir. 1993) [using the same 4 factors set out in *Granada* and adding 5th factor of overriding issues of fairness].

D. Authorization Confirmation by Digital Signature (Adapted from several of Tom Watkins' papers on Ethics and E-Commerce)

Authentication protocols have necessarily developed in order to facilitate the use of electronic communications to carry on commerce. State law provides that a document is signed when it contains "any symbol executed or adopted by a party with present intention to authenticate a writing." Tex. Bus. Comm. Code Ann. §1.201(39). 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 to the financial institution transferring the funds.

Digital signatures have evolved as a legally authorized means by which a sender may be reliably identified. A 1997 amendment to §2.108(d) of the Texas Business and Commerce Code 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) gives digital signatures the same force and effect as a manual signature in transactions governed by Chapter 2 of the Texas Business and Commerce Code. 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. Tex. Gov. Code Ann. § 2054.060.

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. 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 second, 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.

Parties to electronic transactions often use third party vendors to verify the identity of the sender of sensitive electronic information and certify that the public/private "key" pair is legitimate. These third party "certification authorities" 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. *See* Information Security Committee, Electronic Commerce Division, Science and Technology Section, American Bar Association, *Digital Signature Guidelines* (August 1, 1996). 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.

V. Ethics Analyses

Early opinions concerning a lawyer's use of electronic communications modalities recognized the risk of inadvertent disclosure, and generally concluded that the lawyer has a responsibility for obtaining the client's informed consent before communicating through email. *See* South Carolina Ethics Advisory Opinion 94-27 (January 1995) [citing possibility that system operators had access to email, analogizing email to cell phones]; North Carolina Ethics Opinion 251 (April 1995) [use of email requires encryption or consent].

But, as use of electronic communications has dramatically increased both within the profession and societally, the opinions concerning protection of confidentiality have softened. *See* South Carolina Ethics Advisory Opinion 97-08 (May 1997) [revisited prior holding: operators' access no different than ordinary telephone operators]; Illinois Ethics Opinion 96-10 (May 1997) [may use email without encryption unless special circumstances require enhanced security]; Vermont Ethics Opinion 97-05 [use of unencrypted email not violative of lawyer's ethical duties].

An ABA ethics opinion has concluded that a lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct (1998) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. ABA ***Formal Opinion 99-413*** (March 10, 1999, available at http://www.abanet.org/cpr/fo99-413.html); *see* a copy of the opinion attached to this article. But, that opinion goes on to advise that a lawyer should consult with the client and follow her instructions as to the mode of transmitting highly sensitive information relating to the client's representation.

Many ethicists have concluded that a recipient of a misdirected communication has a responsibility to serve the interest of preservation of any privilege intended to attach to the communication. For example, the ABA Committee on Ethics and Professional Responsibility considered the obligations of a lawyer who receives a misdirected fax clearly intended for another: the attorney should notify the sender and return the document without using it. ABA Comm. on Ethics & Prof. Responsibility, ***Formal Op. 92-368*** (1992) and ***Formal Op. 92-936*** (1992). The ABA Committee concluded that inadvertently disclosed client information should still be protected as confidential and privileged, and specifically recognized the exposure created by technological advances such as fax and e-mail communications. The ABA Committee declined to adopt what it considered to be the minority view that unforced disclosure of privileged communications would destroy confidentiality and terminate the privilege. "The sending lawyer

... cannot be begin to be presumed to have consented to any use of the missent materials ... Any attempt by the receiving lawyer to use the missent letter for his own purposes would thus constitute an 'unauthorized use.'" *See also* ***Formal Op. 94-382*** (1994) [unauthorized dissemination of information from whistleblowers treated same as other inadvertently discovered information; despite the receiving lawyer's obligation zealously to represent the interests of her client, the receiving lawyer is bound to advise the opposition that the information has been received and follow their instructions or seek instructions from court].