ILLEGALLY OBTAINED EVIDENCE
(Wiretapping, Interception of Electronic Communication, Surveillance, Private Investigators, and the Attorney/Client Privilege)

WARREN COLE
KRISTI WIDNER
Piro and Lilly, L.L.P.
1400 Post Oak Blvd., Suite 600
Houston, Texas  77056-3008
warcole@piro-lilly.com
(713) 966-4444

State Bar of Texas
29TH ANNUAL ADVANCED FAMILY LAW COURSE
August 18-21, 2003
San Antonio

CHAPTER 54
I. EDUCATIONAL BACKGROUND.
   A. Undergraduate: University of St. Thomas, B.A. 1971
   B. Graduate: University of Houston, Houston Law Center, J.D. 1974
   D. Trained as Arbitrator in Matrimonial Law Arbitration by the American Academy of Matrimonial Lawyers

II. PROFESSIONAL ASSOCIATIONS.
   A. State Bar of Texas - Family Law Section, Litigation Section, Probate, Trust & Real Estate Section
   B. American Bar Association - Family Law Section
   C. Houston Bar Association - Family Law Section
   D. Fellow, American Academy of Matrimonial Lawyers
   E. Texas Chapter of American Academy of Matrimonial Lawyers
   F. Member- Gulf Coast Family Law Specialists Association (1982-present)
   G. Member - Texas Academy of Family Law Specialists
   H. Master, American Inns of Court

III. PROFESSIONAL ACTIVITIES.
   A. Chairman - State Bar of Texas - 4G Grievance Committee (1984-1990)
   B. Past Director - Family Law Section - Houston Bar Association
   C. Past President and Director - Gulf Coast Family Law Specialists
   D. Family Law Council - State Bar of Texas (Member 1994-present; Secretary-2001-2002; Treasurer-2002-2003; Vice Chair-2003-2004)

IV. LEGAL TEACHING/Writing.
   A. Authored and lectured at many CLE Programs, 1983 to present.
   B. Writing consultant to Bancroft-Whitney Publishing Co.
   C. Writing consultant to Matthew Bender Publishing Co. on Matrimonial and Family Law Advocacy, "Expert Witnesses".

V. PROFESSIONAL HONORS AND AWARDS.
   A. David A. Gibson Memorial Award of Excellence - Gulf Coast Family Law Specialists Association (1991)
   B. Outstanding Service Award 1977-1978 - Houston Bar Association
   C. President's Award 1978-1979 - Houston Bar Association
TABLE OF CONTENTS

I. SCOPE OF ARTICLE ................................................................. 1

II. INTRODUCTION ...................................................................... 1

III. THE BASIC CONCEPTS OF PRIVACY AND INTRUSION .............. 1

IV. FAMILY LAW AND ILLEGALLY OBTAINED EVIDENCE ...................... 1
   A. Use as Substantive Evidence ................................................. 1
   B. Use as Impeachment Evidence .............................................. 1
   C. Wiretapping (Including Cell Phones) and Video Surveillance. .................. 2
      1. What Is Unlawful? .................................................. 2
      2. Exceptions ......................................................... 2
      3. Video Taping ...................................................... 2
   D. Computer Data and E-Mail ................................................. 3
   E. Liability for Unlawful Disclosure ........................................... 3
   F. Wiretapping and Parent Child Cases ...................................... 3
   G. Trash or Treasure? ...................................................... 4

V. PRIVATE INVESTIGATORS .......................................................... 4
   A. Who Has Hired or Who Should Hire the Investigator? ................. 4
   B. Tort Liability .................................................................. 4

VI. SPOLIATION V. ILLEGALLY OBTAINED EVIDENCE ......................... 4
   A. What is Spoliation? ...................................................... 4
   B. Elements Required to Establish Spoliation. ................................. 5
      1. Duty to Preserve Evidence ......................................... 5
      2. Has There Been a Breach of the Duty? ......................... 5
      3. Prejudice to the Innocent Party .................................... 5
   C. Remedies to Spoliation. .................................................. 5
      1. Rule 215 Sanctions .................................................. 5
      2. Jury Instruction-Spoliation Presumption ....................... 5

BIBLIOGRAPHY ........................................................................ 7

APPENDIX I ............................................................................. 9

APPENDIX II ........................................................................... 13
ILLEGALLY OBTAINED EVIDENCE

by Warren Cole

I. SCOPE OF ARTICLE

This paper is intended to educate the family law practitioner on the current state of the law relative to recognizing and dealing with evidence which may have been obtained by illegal means. In light of the advanced nature of technology, the attorney will undoubtedly find him or herself in a position to address, not only the admissibility of emails and tape recordings, but more importantly the ethical impact of mere possession of such data. Included in this writing is a discussion of the effects of illegally obtained evidence on discovery, attorney-client privilege issues, civil and criminal sanctions, and professional responsibility. A brief review on the related topic of spoliation of evidence is also included.

II. INTRODUCTION

Every family law litigator is frequently faced with their client inundating them or their staff with reams of information that the client feels is important and crucial to their case. Some, if not all, of this data has often been obtained by the client, or their agent, by surreptitious means. In such instances, the lawyer’s task in representing the client becomes extremely complex and extends far beyond just securing a favorable property division or an acceptable parent-child arrangement. It presents issues which may result in criminal or civil liability for not only the client, but also for their counsel. Those unfortunate practitioners who have found themselves in similar situations will readily admit that their knowledge and skills as a good family law attorney is of no moment if their efforts will be focused on protecting themselves and the client from the grasps of the district attorney’s office or the grievance committee. Hopefully, some of the comments contained in this paper will assist in avoiding such instances.

III. THE BASIC CONCEPTS OF PRIVACY AND INTRUSION

At the risk of insulting the intelligence of the reader, a brief, rudimentary discussion of the concepts of the right of privacy and protection from unwanted intrusion is warranted. All citizens of the United States are guaranteed an ambit of privacy from which they should be free from intrusion by both governmental and private sources. U.S.C.A Const. Amend. 4; Vernon’s Tex. Const. Art 1, §§; Billings v. Atkinson, 489 S.W.2d 858, 860 (Tex. 1973). Fundamentally, the protected area should only be invaded in exigent circumstances. While most family law attorneys have a working knowledge of the application of this concept in the area of criminal law, it becomes somewhat blurred in the civil arena. The nature of the protected realms range from a person’s trash to the more technical areas of cell phones and computers. Some believe that the rules should be relaxed in family law litigation, especially when the “best interest” of minor children are the primary focus of the case. Regardless of one’s misplaced interpretation, the same basic rules are applicable. Crossing the line may result in exclusion of improperly obtained evidence, or worse, criminal and civil sanctions for both the client and their lawyer. The attached appendices contain excerpts from the applicable statutes referenced in this paper. It is strongly suggested that the family law practitioner become familiar with the general terms and conditions of these laws and assure that their clients are appropriately advised of the negative affects on them and their case if a violation occurs.

IV. FAMILY LAW AND ILLEGALLY OBTAINED EVIDENCE

A. Use as Substantive Evidence.

As a general rule, evidence obtained in violation of the law is inadmissible as substantive evidence in civil cases. Collins v. Collins, 904 S.W.2d 792, 799 (Tex. App.- Houston [1st Dist.] 1995, writ den’d); 18 U.S.C §2515. The party seeking the exclusion of such evidence must object in a timely manner and also bears the burden of proving that the exclusion is required by the particular Federal or State statute which was violated. Sims v. Cosden Oil & Chemical Co., 663 S.W.2d 70 (Tex. App. - Eastland 1984, writ ref’d n.r.e). It should also be noted that the exclusionary rule [Tex. Code Crim. P. Art. 38.23] does not apply to civil cases. Schenck v. Ebby Halliday Real Estate, Inc., 803 S.W.2d 361, 327 (Tex. App. - Fort Worth 1991, no writ)

B. Use as Impeachment Evidence.

Although the proponent may be precluded from introducing the illegally obtained evidence as substantive evidence, authority does exist for its introduction as impeachment evidence. Barham v. Turner Const. Company of Texas, 803 S.W.2d 731, 739-740 (Tex. App. - Dallas 1990, writ denied); Cummings v. Jess Edwards, 445 S.W.2d 767, 773 (Tex. Civ. App. – Corpus Christi 1969, writ ref’d n.r.e.). It should be noted that the seven point test set forth in Cummings relating to proper operation and content of the recording has been abrogated by Seymour v. Gillespie, 608 S.W.2d 897, 898 (Tex. 1990). The court is permitted to examine the circumstances surrounding the acquisition of the
questioned evidence and if it could have been obtained through legal means, it may be admissible both as both substantive and impeachment evidence. *Fabian v. Fabian*, 765 S.W.2d 516, 519 (Tex. App. - Austin 1989, no writ). See also, *Jack v. State*, 394 N.E.2d 166 (1979); *Calbertson v. Calbertson*, 143 F.3d 825, 827 (4th Cir. 1998). In any event, the practitioner should never encourage or participate in any form of activity which even remotely may be interpreted as a violation of the law.

C. Wiretapping (Including Cell Phones) and Video Surveillance.

Since the beginning of modern technology, divorce litigants have attempted to gain an advantage by any effective means available. In many cases one of the spouses just wants to confirm their suspicions that the other spouse has been unfaithful. Regardless of the motive, Most courts have continued to recognize that there is no interspousal exception to the Federal and State Wiretap laws. See, *Duffy v. State*, 22 S.W.3d 17 (Tex. App. - El Paso, 2000, no pet.). However, there are at least two cases which the author considers to be aberrations, which have read into the federal wiretap statute an interspousal exemption. The first was *Simpson v. Simpson*, 490 F.2d 803 (5th Cir.), cert denied, 419 U.S. 897 (1974). In that case, Mr. Simpson wiretapped the marital residence phone and recorded conversations between his wife and third parties. The Court held that the statute was not sufficiently definite or specific to uphold a federal cause of action for unlawful interception of communications. It also reasoned that such types of family law related instances should be left to the state courts. Three years later the 2nd Circuit followed the holding in *Simpson*. *Anonymous v. Anonymous*, 558 F.2d 677 (2d Cir. 1977). This matter involved the legality of a father tape recording his 8 year son’s conversation with the child’s mother. The Court analogized the tapping with a parent listening to conversations on the family extension phone. For a concise summary of the various state laws relating to wiretapping the reader is directed the [www.rcfp.org/taping](http://www.rcfp.org/taping). A copy of the cover page is attached as Appendix I.

1. What Is Unlawful?

Generally speaking, and as applied to family law litigants, it is illegal to intercept any form of wire, oral or electronic communications between others unless the aggrieved party has consented to the interception. *Tex. Civ. Prac. & Rem. Code* §123.002; *Tex. Pen. Code* §16.02; 18 U.S.C §2511, 2702. The referenced statutes also include any form of illegal interception or tracking of cellular phone conversation. 18 U.S.C §2510-2511. It is also unlawful to disclose or otherwise disseminate any such communications. *Id*. It should be noted that “Communication” means speech uttered by a person or information including speech that is transmitted in whole or in part with the aid of a wire or cable under *Tex. Civ. Prac. & Rem. Code* §123.001. This includes only aural communication, not eavesdropping or photographing, and addresses civil liability only. However, from a criminal standpoint prohibited interception is inclusive of any wire, oral, or electronic communication. *Tex. Pen. Code* §16.02(b)(1). It should be noted that civil liability under the Texas Civil Practice and Remedies Code is premised only upon a “person” who intercepts… *Tex. Civ. Prac. & Rem. Code* §123.002(a). It does not require that the violator act intentionally. For criminal liability to attach, the perpetrator must have acted “intentionally”. *Tex. Pen. Code* §16.02(b); 18 U.S.C §2511(1).

2. Exceptions.

In addition to the numerous governmental or agency exceptions to the general rule, it is not unlawful to intercept any form of wire, oral or electronic communications between others if one of the persons is a party to the communication or one of the parties has given their consent to the interception. *Tex. Civ. Prac. & Rem. Code* §123.001(2); *Tex. Pen. Code* §16.02(c)(3)(A); 18 U.S.C §2511(2)(c); *Kotrla v. Kotrla*, 718 S.W.2d 853, 855 (Tex.. App. - Corpus Christi 1986); See also, *Hall v. State*, 862 S.W.2d 710 (Tex. App. - Beaumont 1993, no writ); *Turner v. PV International Corporation*, 765 S.W.2d 455, 469-71 (Tex. App. - Dallas 1988, writ denied per curiam, 778 S.W.2d 865 (Tex. 1989).

3. Video Taping.

In a case of first impression, *Clayton v. Richards*, 47 S.W.3d 149 (Tex. App. - Texarkana, 2001, pet. denied), interpreted the legality of a clandestine video surveillance. This case involved the liability of a private investigator hired by a spouse to plant a video camera in the bedroom of her husband who was suspected to be an adulterer. Up to this point the courts have distinguished “recordings” from videotaping and acknowledged that the act of videotaping a spouse did not meet the technical requirements to come under the wiretapping prohibitions. *Id* at 156. In reversing the granting a summary judgment in favor of the investigator, the court held, “An individual’s right to privacy is compromised no less from being secretly videotaped than from being secretly recorded. A secret video tape of an individual who presumes to be in a private place is an even greater
D. Computer Data and E-Mail.

On occasion the divorce litigant will appear at the lawyer’s office with binders full of incriminating emails and other data removed from the other spouse’s computer or PDA. Before rummaging through the spoils the practitioner should make some inquiries to avoid the possibility of complicity in an unlawful Federal or State interception. The primary applicable laws involved are Tex. Pen. Code §§16.02(b)-16.04(b), and 18 U.S.C. §§2701-2711, more commonly known as The Electronic Communications Privacy Act (ECPA). It appears that the ECPA was initially directed at internet service providers to prohibit unauthorized intrusion or disclosure of their customers stored data or information. However, it does extend to the private sector and arguably to spousal computer raids. There are no reported civil cases involving spousal intrusion. However, in the child pornography case of United States v. Maxwell,42 M.J. 568 (1995), the appellate court based its decision on the claimant’s expectation of privacy. To determine whether the claimant has a legitimate expectation of privacy in the invaded place, he must prove:(1) that he had an actual, or subjective expectation of privacy, and, (2) that his individual expectation of privacy was one that society objectively recognizes as reasonable. Does a spouse have the subjective expectation of privacy with regard to the family computer? What about discovering the secret password of the other spouse and accessing his/her email?

E. Liability for Unlawful Disclosure.

There is not only civil and criminal liability for illegal interception, but penalties exist for the possession or disclosure of illegally obtained information covered by the statues. Tex. Pen. Code §16.02(b)(2)-(3); 18 U.S.C §2511(1)(c)-(d). See, Collins v. Collins, 904 S.W.2d at 798. The caveat being, if the client presents the attorney with any information or data which even remotely appears to have been obtained in violation of any state or federal statutes, DO NOT ACCEPT IT, advise the client of the applicable laws, and refer them to a criminal law attorney, if warranted.

F. Wiretapping and Parent Child Cases.

As illustrated above, the law in Texas is clear that no interspousal exemption exists to the federal or state wiretap statutes. As with illegal recordings between spouses, many jurisdictions have struggled with the parental “consent”issue as it relates to a parent or guardian’s recording of conversations between the child and the other parent. In Pollock v. Pollock, 154 F.3d 601, 610 (6th Cir. 1998) the court expanded the required consent under 18 U.S.C. §2511(2)(d) to a parent, on behalf of their child. The court found that a parent may vicariously consent for their child when the recording parent can demonstrate “a good faith, objectively reasonable basis for believing that it is necessary and in the best interest of the child”. In the recently reported case of Apter v. Ross, 781 N.E.2d 744 (Ind. App. 2003), the Indiana Court of Appeals followed a similar rationale enunciated in Pollock. Mr. Apter was a joint legal custodian of his children. He tape recorded a phone conversation between one of the children and her mother. The trial court refused to admit the tape recording. In reversing the lower court’s ruling the appellate court held that “because the conversation was made on Gary’s [father] home phone and because a parent with joint legal custody Gary had the power to consent on his daughter’s behalf to the recording of her phone conversation...” Id. at _____. The court found that Gary’s testimony established that he was “concerned” about his daughter welfare. Citing Scheib v. Grant, 22 F.3d 149, 153 (7th Cir 1994), the court found that the “extension phone” exemption was applicable. The exemption relied upon by the Court states:: "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than (a) any telephone or telegraph instrument, equipment or facility, or any component thereof,(i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business...18 U.S.C. 2510(5)(a) [emphasis added].

Texas takes a much more limited approach. The leading case relating to a parent’s right to record their child’s phone conversation with the other parent, absent the knowledge or consent of the recorded parent, is Collins v. Collins, supra. Mr. Collins took it upon himself to record phone communications between his child and the child’s mother. Id at 798. He then furnished the tape to the mental health professional involved in the
ongoing custody case. *Id.* Mrs. Collins objected to the introduction of the tapes and to the testimony of the mental health professional who based her custody opinion, in part, on the content of the tapes. *Id.* The appellate court reversed the custody finding for dad holding that, since the dissemination of the tapes was illegal conduct, if admitted into evidence, the court could be considered a partner in the crime. *Id.* The bottom line: DO NOT ADVISE THE CLIENT TO RECORD CONVERSATIONS.

G. Trash or Treasure?

Digging through the other spouse's trash has sometimes been a popular pastime for acrimonious litigants. Can the empty whiskey bottle or the wadded up love letter found in the trash bin admissible in the divorce case? The answer again turns on the “reasonable expectation of privacy”. In civil cases, it appears that if the evidence was obtained by or though means of an illegal trespass, the evidence should be excluded if offered as substantive evidence. Day & Zimmermann, Inc. 483 S.W.2d 541, 546 (Tex. Civ. App. - Texarkana 1972, writ ref’d. n.r.e.) The court in Day properly excluded the testimony of a witness who’s testimony was to be based on observation made while he was unlawfully trespassing on the plaintiff’s property. If the excluded evidence was not “impeaching”, then it is proper to deny admission. Barham v. Turner Const. Company of Texas, 803 S.W.2d at 739. If the evidence was obtained after the litigation has begun, the admissibility can be challenged by *Tex. R. Civ. P. 215; Schenck v. Ebby Halliday Real Estate, Inc., 803 S.W.2d at 372-373* (noting that the trial court is authorized to exclude evidence as a discovery sanction.). As this area of evidence is applied to family law cases, one could infer that if the parties are separated and the other party, or their agent, trespasses on the other party’s property to gain access, the evidence should be excluded as substantive evidence, but not necessarily as impeachment evidence. If however, no trespass is needed (trash left on the curb for pickup), the evidence should be admitted for all purposes, if properly authenticated. See, *California v. Greenwood, 486 U.S. 35, 108 S. Ct. 1635, 100 L.Ed.2d 30 (1988).*

V. PRIVATE INVESTIGATORS

Next to CPAs, private investigators are probably the most employed persons in family law litigation. The good ones can be of great assistance. The bad ones can be very costly, not only monetarily but professionally.

A. Who Has Hired or Who Should Hire the Investigator?

Generally stated if the investigator is hired by the attorney and controlled by the attorney the resulting investigation will likely fall within the “work product” privilege. *Tex. R. Civ. P. 192.5.* If the client hires the investigator and provides the lawyer the information or instructs the investigator to do so, it is very doubtful that the data will be protected, and must be disclosed if properly requested in discovery. In the later case, it makes no difference whether such information was gathered “in anticipation of litigation”. See, *In Re Weeks Marine, Inc., 31 S.W.3d 389, 390 (Tex. App. - San Antonio 2002, orig. proceeding).* If the investigator is to be a testifying fact witness or a testifying expert, it is unlikely that any of the information obtained could be protected. *Tex. R. Civ. P. 194.2.* Another discovery issue which must be addressed as relates to the required verification of interrogatory answers under *Tex. R. Civ. P. 197.2(d).* When any answers to interrogatories are based on information obtained from someone other than the party responding to the discovery, one is required to state that fact. *Tex. R. Civ. P. 197.2(d)(1).* This obviously includes an investigator. A complete discussion on the rules of procedure is beyond the scope of this article. The reader should review all of the necessary prerequisites and procedures for the claiming of the work product or attorney client privilege.

B. Tort Liability.

The most important aspect of retaining an investigator is being very familiar with the credentials and the ethics of that individual. Any illegal activity which the investigator may be involved could create liability on part of the lawyer and client. In the case of *Clayton v. Richards,* supra, the summary judgment granted in favor of the defendant investigator Richards was reversed. The court found that even if the investigator furnished only technical services in installing the camera, he may still be liable in tort if an actual invasion of privacy was committed. *47 S.W.3d at 154.* Those who pursue a common plan or design to commit a tortious act, actually take part in it or further it by cooperation or request, or to lend aid to the wrongdoer, or ratify or adopt his act are also liable for the tortious act. *Id.* One can be assured that if an errant investigator crosses the line, all involved, including the attorney responsible for the direction and control will be target defendants.
VI. SPOLIATION V. ILLEGALLY OBTAINED EVIDENCE

While the topic of spoliation of evidence is somewhat beyond the scope of this article, the author feels that a brief understanding of the differences and affects is mandated.

A. What is Spoliation?

It has been defined as the intentional destruction, mutilation, alteration, or concealment of evidence, usually a document. Black’s Law Dictionary, 7th Ed., 1999. At this time no independent tort exists against someone who commits an act covered by the definition. Trevino v. Ortega, 969 S.W.2d 950, 952 (Tex. 1998).

B. Elements Required to Establish Spoliation.

The question of whether one is guilty of spoliation and the appropriate action to be taken is a question of law for the judge, not one of fact for the jury. Id. at 954.

1. Duty to Preserve Evidence.

The first question which must be answered is whether the alleged spoliator has a duty to preserve the destroyed evidence. Such a duty arises only when a party knows or reasonably should know that there is a substantial chance that a claim will be filed and that evidence in its possession or control will be material and relevant to the claim. Wal-Mart Stores, Inc. v. Johnson, ___S.W.3d___ (Tex. 2003) (2002 WL 32098152). If there is a statutory requirement that certain records be maintained and preserved, the answer to this inquiry is clear. However, how this would be applied in a family law matter is uncertain. Does it arise at the first cry of “I want a divorce”; the filing of the petition; or service of process?

2. Has There Been a Breach of the Duty?

The next prong is for the Court to determine whether a breach of the duty has occurred. Trevino holds that the person responsible should be held accountable for negligence, as well as, intentional acts. 969 S.W.2d at 957. In essence the entire burden is placed on the culpable spoliating party since they are in the best position to provide an explanation. Id.

3. Prejudice to the Innocent Party.

Even if spoliation is found to have occurred, it doesn’t automatically mean that the nonspoliating party is entitled to a remedy. Id. at 955. The more relevant the destroyed evidence, the more harm to the nonspoliating party. Id. at 958. If he evidence was destroyed intentionally or in bad faith, then the court should find that the destroyed evidence was relevant and harmful to the spoliating party’s case. Id. If the evidence was negligently destroyed, then the nonspoliating party should offer some proof about what the destroyed evidence would show. Id. The spoliating party is certainly entitled to show that the missing evidence would have been cumulative of other competent evidence that can be used in place of the destroyed evidence. Id.

C. Remedies to Spoliation.


Depending upon when the destruction occurs, the court has wide discretion in remedying the situation. If the relevant evidence is destroyed during the discovery phase of the litigation, the court can impose any sanctions authorized under Tex. R. Civ. P. 215, including death the penalty sanction resulting in a default judgment against the spoliating party or preclusion of the introduction of evidence. Id. at 959. These sanctions are to be applied on a case by case basis. Id.

2. Jury Instruction-Spoliation Presumption.

The court has its choice of two spoliation instructions. The most severe is a rebuttable presumption and is used when the nonspoliating party cannot prove its prima facie case without the destroyed evidence. Id. at 960. The jury is instructed that they should presume that the destroyed evidence was unfavorable to the spoliating party and that the spoliating party bears the burden of disproving the presumed fact or issue. Id. Depending on the exact wording of the instruction, it could relieve the nonspoliating party of the burden of proving each element of their case. Id. The second type of presumption merely instructs the jury that the evidence would have been unfavorable to the spoliating party. It does not relieve the nonspoliating party of proving each element of their case. Id. at 961.
BIBLIOGRAPHY

The Pitfalls of Illegal Eavesdropping; Criminal, Civil, Ethical...Where Does it End”, Poole, R., Advanced Family Law Course, State Bar of Texas, 1999


Invasion of Privacy - Illegally Obtained Evidence, Lewis, M., Marriage Dissolution Institute, State Bar of Texas, 1999


APPENDIX I
## Tape-recording laws at a glance

<table>
<thead>
<tr>
<th>State</th>
<th>Is consent of all parties required?</th>
<th>Are there criminal penalties?</th>
<th>Does the statute allow for civil suits?</th>
<th>Is there a specific hidden camera law?</th>
<th>Are there additional penalties for disclosing or publishing information?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Alabama</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Alaska</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Arizona</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Arkansas</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>California</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Colorado</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Connecticut</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Delaware</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>D.C.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Florida</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Georgia</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Hawaii</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Idaho</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Illinois</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Indiana</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Iowa</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Kansas</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Kentucky</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Louisiana</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Maine</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Maryland</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Massachusetts</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Michigan</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Minnesota</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Mississippi</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Missouri</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>State</td>
<td>Law</td>
<td>Consent</td>
<td>Permission</td>
<td>Recording</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>-----</td>
<td>---------</td>
<td>------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>Montana</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Nebraska</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Nevada</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>New Hampshire</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>New Jersey</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>New Mexico</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>New York</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>North Carolina</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>North Dakota</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Ohio</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Oklahoma</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Oregon</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Pennsylvania</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Rhode Island</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>South Carolina</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>South Dakota</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Tennessee</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Texas</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Utah</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Vermont</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Virginia</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Washington</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>West Virginia</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Wisconsin</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Wyoming</td>
<td>☑️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX II

CHAPTER 123. INTERCEPTION OF COMMUNICATION

§§ 123.001. Definitions
In this chapter:

(1) "Communication" means speech uttered by a person or information including speech that is transmitted in whole or in part with the aid of a wire or cable.
(2) "Interception" means the aural acquisition of the contents of a communication through the use of an electronic, mechanical, or other device that is made without the consent of a party to the communication, but does not include the ordinary use of:

(A) a telephone or telegraph instrument or facility or telephone and telegraph equipment;
(B) a hearing aid designed to correct subnormal hearing to not better than normal;
(C) a radio, television, or other wireless receiver; or
(D) a cable system that relays a public wireless broadcast from a common antenna to a receiver.

§§ 123.002. Cause of Action
(a) A party to a communication may sue a person who:

(1) intercepts, attempts to intercept, or employs or obtains another to intercept or attempt to intercept the communication;
(2) uses or divulges information that he knows or reasonably should know was obtained by interception of the communication; or
(3) as a landlord, building operator, or communication common carrier, either personally or through an agent or employee, aids or knowingly permits interception or attempted interception of the communication.

(b) This section does not apply to a party to a communication if an interception or attempted interception of the communication is authorized by Title 18, United States Code, Section 2516.

§§ 123.003. Defense
(a) A switchboard operator or an officer, employee, or agent of a communication common carrier whose facilities are used in the transmission of a wire communication may intercept, disclose, or use a communication in the normal course of employment if engaged in an activity that is necessary to service or for the protection of the carrier's rights or property. A communication common carrier may not use service observation or random monitoring except for mechanical or service quality control checks.

(b) It is a defense to an action under Section 123.002 that an interception, disclosure, or use of a communication is permitted by this section.

(c) A defendant must establish by a preponderance of the evidence a defense raised under this section.

§§ 123.004. Damages
A person who establishes a cause of action under this chapter is entitled to:

(1) an injunction prohibiting a further interception, attempted interception, or divulgence or use of information obtained by an interception;
(2) statutory damages of $10,000 for each occurrence;
(3) all actual damages in excess of $10,000;
(4) punitive damages in an amount determined by the court or jury; and
(5) reasonable attorney's fees and costs.

TEXAS PENAL CODE
CHAPTER 16. CRIMINAL INSTRUMENTS, INTERCEPTION OF WIRE OR ORAL COMMUNICATION, AND INSTALLATION OF TRACKING DEVICE

§§ 16.01. Unlawful Use of Criminal Instrument
(a) A person commits an offense if:

(1) he possesses a criminal instrument with intent to use it in the commission of an offense; or
(2) with knowledge of its character and with intent to use or aid or permit another to use in the commission of an offense, he manufactures, adapts, sells, installs, or sets up a criminal instrument

(b) For the purpose of this section, "criminal instrument" means anything, the possession, manufacture, or sale of which is not otherwise an offense, that is specially designed, made, or adapted for use in the commission of an offense.

(c) An offense under Subsection (a)(1) is one category lower than the offense intended. An offense under Subsection (a)(2) is a state jail felony.
§§ 16.02. Unlawful Interception, Use, or Disclosure of Wire, Oral, or Electronic Communications

Text of section effective until Sept. 1, 2005

(a) In this section, "computer trespasser," "covert entry," "communication common carrier," "contents," "electronic communication," "electronic, mechanical, or other device," "immediate life-threatening situation," "intercept," "investigative or law enforcement officer," "member of a law enforcement unit specially trained to respond to and deal with life-threatening situations," "oral communication," "protected computer," "["electronic communication,"] readily accessible to the general public," and "wire communication" have the meanings given those terms in Article 18.20, Code of Criminal Procedure.

(b) A person commits an offense if the person:

(1) intentionally intercepts, endeavors to intercept, or procures another person to intercept or endeavor to intercept a wire, oral, or electronic communication;

(2) intentionally discloses or endeavors to disclose to another person the contents of a wire, oral, or electronic communication if the person knows or has reason to know the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(3) intentionally uses or endeavors to use the contents of a wire, oral, or electronic communication if the person knows or is reckless about whether the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(4) knowingly or intentionally effects a covert entry for the purpose of intercepting wire, oral, or electronic communications without court order or authorization; or

(5) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when the device:

(A) is affixed to, or otherwise transmits a signal through a wire, cable, or other connection used in wire communications; or

(B) transmits communications by radio or interferes with the transmission of communications by radio.

(c) It is an affirmative defense to prosecution under Subsection (b) that:

(1) an operator of a switchboard or an officer, employee, or agent of a communication common carrier whose facilities are used in the transmission of a wire or electronic communication intercepts a communication or discloses or uses an intercepted communication in the normal course of employment while engaged in an activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the carrier of the communication, unless the interception results from the communication common carrier's use of service observing or random monitoring for purposes other than mechanical or service quality control checks;

(2) an officer, employee, or agent of a communication common carrier provides information, facilities, or technical assistance to an investigative or law enforcement officer who is authorized as provided by this section [article] to intercept a wire, oral, or electronic communication;

(3) a person acting under color of law intercepts:

(A) a wire, oral, or electronic communication, if the person is a party to the communication or if one of the parties to the communication has given prior consent to the interception;

(B) a wire, oral, or electronic communication, if the person is acting under the authority of Article 18.20, Code of Criminal Procedure; or

(C) a wire or electronic communication made by a computer trespasser and transmitted to, through, or from a protected computer, if:

(i) the interception did not acquire a communication other than one transmitted to or from the computer trespasser;

(ii) the owner of the protected computer consented to the interception of the computer trespasser's
communications on the protected computer; and

(iii) actor was lawfully engaged in an ongoing criminal investigation and the actor had reasonable suspicion to believe that the contents of the computer trespasser’s communications likely to be obtained would be material to the investigation;

(4) a person not acting under color of law intercepts a wire, oral, or electronic communication, if:

(A) the person is a party to the communication; or

(B) [if] one of the parties to the communication has given prior consent to the interception, unless the communication is intercepted for the purpose of committing an unlawful [any criminal or tortious act in violation of the constitution or laws of the United States or of this state or for the purpose of committing any other injurious] act;

(5) a person acting under color of law intercepts a wire, oral, or electronic communication if:

(A) oral or written consent for the interception is given by a magistrate before the interception;

(B) an immediate life-threatening situation exists;

(C) the person is a member of a law enforcement unit specially trained to:

(i) respond to and deal with life-threatening situations; or

(ii) install electronic, mechanical, or other devices; and

(D) the interception ceases immediately on termination of the life-threatening situation;

(6) an officer, employee, or agent of the Federal Communications Commission intercepts a communication transmitted by radio or discloses or uses an intercepted communication in the normal course of employment and in the discharge of the monitoring responsibilities exercised by the Federal Communications Commission in the enforcement of Chapter 5, Title 47, United States Code;

(7) a person intercepts or obtains access to an electronic communication that was made through an electronic communication system that is configured to permit the communication to be readily accessible to the general public;

(8) a person intercepts radio communication, other than a cordless telephone communication that is transmitted between a cordless telephone handset and a base unit, that is transmitted:

(A) by a station for the use of the general public;

(B) to ships, aircraft, vehicles, or persons in distress;

(C) by a governmental, law enforcement, civil defense, private land mobile, or public safety communications system that is readily accessible to the general public, unless the radio communication is transmitted by a law enforcement representative to or from a mobile data terminal;

(D) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(E) by a marine or aeronautical communications system;

(9) a person intercepts a wire or electronic communication the transmission of which causes harmful interference to a lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of the interference;

(10) a user of the same frequency intercepts a radio communication made through a system that uses frequencies monitored by individuals engaged in the provision or the use of the system, if the communication is not scrambled or encrypted; or

(11) a provider of electronic communications service records the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service towards the completion of the communication, or a user of
that service from fraudulent, unlawful, or abusive use of the service.

(d) A person commits an offense if the person:

(1) intentionally manufactures, assembles, possesses, or sells an electronic, mechanical, or other device knowing or having reason to know that the device is designed primarily for nonconsensual interception of wire, electronic, or oral communications and that the device or a component of the device has been or will be used for an unlawful purpose; or

(2) places in a newspaper, magazine, handbill, or other publication an advertisement of an electronic, mechanical, or other device:

(A) knowing or having reason to know that the device is designed primarily for nonconsensual interception of wire, electronic, or oral communications;

(B) promoting the use of the device for the purpose of nonconsensual interception of wire, electronic, or oral communications;

(C) knowing or having reason to know that the advertisement will promote the use of the device for the purpose of nonconsensual interception of wire, electronic, or oral communications.

(e) It is an affirmative defense to prosecution under Subsection (d) that the manufacture, assembly, possession, or sale of an electronic, mechanical, or other device that is designed primarily for the purpose of nonconsensual interception of wire, electronic, or oral communication is by:

(1) a communication common carrier or a provider of wire or electronic communications service or an officer, agent, or employee of or a person under contract with a communication common carrier or provider acting in the normal course of the provider's or communication carrier's business;

(2) an officer, agent, or employee of a person under contract with, bidding on contracts with, or doing business with the United States or this state acting in the normal course of the activities of the United States or this state;

(3) a member of the Department of Public Safety who is specifically trained to install wire, oral, or electronic communications intercept equipment; or

(4) a member of a local law enforcement agency that has an established unit specifically designated to respond to and deal with life-threatening situations.

(f) An offense under this section is a felony of the second degree, unless the offense is committed under Subsection (d) or (g), in which event the offense is a state jail felony.

(g) A person commits an offense if, knowing that a government attorney or an investigative or law enforcement officer has been authorized or has applied for authorization to intercept wire, electronic, or oral communications, the person obstructs, impedes, prevents, gives notice to another of, or attempts to give notice to another of the interception.

(h) This section expires September 1, 2005, and shall not be in force on and after that date.


§§ 16.03. Unlawful Use of Pen Register or Trap and Trace Device

(a) A person commits an offense if the person knowingly installs or uses a pen register or trap and trace device to record or decode electronic or other impulses for the purpose of identifying telephone numbers dialed or otherwise transmitted on a telephone line.

(b) In this section, "authorized peace officer," "communications common carrier," "pen register," and "trap and trace device" have the meanings assigned by Article 18.21, Code of Criminal Procedure.

(c) It is an affirmative defense to prosecution under Subsection (a) that the actor is:

(1) an officer, employee, or agent of a communications common carrier and the actor installs or uses a device or equipment to record
a number dialed from or to a telephone instrument in the normal course of business of the carrier for purposes of:

(A) protecting property or services provided by the carrier; or
(B) assisting another who the actor reasonably believes to be a peace officer authorized to install or use a pen register or trap and trace device under Article 18.21, Code of Criminal Procedure;

(2) an officer, employee, or agent of a lawful enterprise and the actor installs or uses a device or equipment while engaged in an activity that:

(A) is a necessary incident to the rendition of service or to the protection of property of or services provided by the enterprise; and
(B) is not made for the purpose of gathering information for a law enforcement agency or private investigative agency, other than information related to the theft of communication or information services provided by the enterprise; or

(3) a person authorized to install or use a pen register or trap and trace device under Article 18.21, Code of Criminal Procedure.

(d) An offense under this section is a state jail felony.

§§ 16.04. Unlawful Access to Stored Communications

(a) In this section, "electronic communication," "electronic storage," "user," and "wire communication" have the meanings assigned to those terms in Article 18.21, Code of Criminal Procedure.

(b) A person commits an offense if the person obtains, alters, or prevents authorized access to a wire or electronic communication while the communication is in electronic storage by:

(1) intentionally obtaining access without authorization to a facility through which a wire or electronic communications service is provided; or
(2) intentionally exceeding an authorization for access to a facility through which a wire or electronic communications service is provided.

(c) Except as provided by Subsection (d), an offense under Subsection (b) is a Class A misdemeanor.

(d) If committed to obtain a benefit or to harm another, an offense is a state jail felony.

(e) It is an affirmative defense to prosecution under Subsection (b) that the conduct was authorized by:

(1) the provider of the wire or electronic communications service;
(2) the user of the wire or electronic communications service;
(3) the addressee or intended recipient of the wire or electronic communication; or
(4) Article 18.21, Code of Criminal Procedure.

§§ 16.05. Illegal Divulgence of Public Communications

(a) In this section, "electronic communication," "electronic communications service," and "electronic communications system" have the meanings given those terms in Article 18.20, Code of Criminal Procedure.

(b) A person who provides electronic communications service to the public commits an offense if the person knowingly divulges the contents of a communication to another who is not the intended recipient of the communication.

(c) It is an affirmative defense to prosecution under Subsection (b) that the actor divulged the contents of the communication:

(1) as authorized by federal or state law;
(2) to a person employed, authorized, or whose facilities are used to forward the communication to the communication's destination; or
(3) to a law enforcement agency if the contents reasonably appear to pertain to the commission of a crime.

(d) Except as provided by Subsection (e), an offense under Subsection (b) that involves a scrambled or encrypted radio communication is a state jail felony.

(e) If committed for a tortious or illegal purpose or to gain a benefit, an offense under Subsection (b) that involves a radio communication that is not scrambled or encrypted:

(1) as a Class A misdemeanor if the communication is not a public land mobile radio service communication or a paging service communication; or
(2) is a Class C misdemeanor if the communication is a public land mobile radio service communication or a paging service communication.


§§ 16.06. Unlawful Installation of Tracking Device
(a) In this section:

(1) "Electronic or mechanical tracking device" means a device capable of emitting an electronic frequency or other signal that may be used by a person to identify, monitor, or record the location of another person or object.
(2) "Motor vehicle" has the meaning assigned by Section 501.002, Transportation Code.

(b) A person commits an offense if the person knowingly installs an electronic or mechanical tracking device on a motor vehicle owned or leased by another person.

(c) An offense under this section is a Class A misdemeanor.

(d) It is an affirmative defense to prosecution under this section that the person:

(1) obtained the effective consent of the owner or lessee of the motor vehicle before the electronic or mechanical tracking device was installed;
(2) was a peace officer who installed the device in the course of a criminal investigation or pursuant to an order of a court to gather information for a law enforcement agency;
(3) assisted another whom the person reasonably believed to be a peace officer authorized to install the device in the course of a criminal investigation or pursuant to an order of a court to gather information for a law enforcement agency; or
(4) was a private investigator licensed under Chapter 1702, Occupations Code, who installed the device:

(A) with written consent:

(i) to install the device given by the owner or lessee of the motor vehicle; and

(ii) if that entry was necessary to install the device, given by the owner or lessee of the property; or

(B) pursuant to an order of or other authorization from a court to gather information.

SELECTED EXCERPTS - TITLE 18 U.S.C

Sec. 2510. - Definitions
As used in this chapter -

(1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;
(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;
(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;
(4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.
(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than -

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof,

(i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by
the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or
(ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;
(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;
(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;
(9) "Judge of competent jurisdiction" means -
   (a) a judge of a United States district court or a United States court of appeals; and
   (b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;
(10) "communication common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) [2] of title 47 of the United States Code;
(11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;
(12) "electronic communication" means 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 does not include -
   (A) any wire or oral communication;
   (B) any communication made through a tone-only paging device;
   (C) any communication from a tracking device (as defined in section 3117 of this title); or
   (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;
(13) "user" means any person or entity who -
   (A) uses an electronic communication service; and
   (B) is duly authorized by the provider of such service to engage in such use;
(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;
(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;
(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not -
   (A) scrambled or encrypted;
   (B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;
   (C) carried on a subcarrier or other signal subsidiary to a radio transmission;
   (D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or
   (E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;
(17) "electronic storage" means -

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

(18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception;

(19) "foreign intelligence information", for purposes of section 2517(6) of this title, means -

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against -

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power;

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to -

(i) the national defense or the security of the United States; or
(ii) the conduct of the foreign affairs of the United States;

(20) "protected computer" has the meaning set forth in section 1030; and
(21) "computer trespasser" -

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and
(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

Sec. 2511. - Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter 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 use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when -

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or
(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or
(iv) such use or endeavor to use

(A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or
(B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or
(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;
(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 the interception of a wire, oral, or electronic communication in violation of this subsection; 

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e)(i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter,

(ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation,

(iii) having obtained or received the information in connection with a criminal investigation, and

(iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation, shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)

(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with -

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this chapter.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.
(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person -

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;
(ii) to intercept any radio communication which is transmitted -

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;
(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;
(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or
(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which -

(I) is prohibited by section 633 of the Communications Act of 1934; or
(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter -

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.
(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if -

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;
(II) the person acting under color of law is lawfully engaged in an investigation;
(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and
(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication -

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;
(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;
(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or
(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled, encrypted, or transmitted using modulation techniques the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication, then -

(i) if the communication is not the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, and the conduct is not that described in subsection (5), the offender shall be fined under this title or imprisoned not more than one year, or both; and

(ii) if the communication is the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, the offender shall be fined under this title.

(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted -

(i) to a broadcasting station for purposes of retransmission to the general public; or
(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls, is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)(a)

(i) If the communication is -
(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection -

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

Sec. 2512. - Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who intentionally -

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication any advertisement of -

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or (ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications, knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce, shall be fined under this title or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for -

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know
that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device.

Sec. 2513. - Confiscation of wire, oral, or electronic communication intercepting devices

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to

(1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code,
(2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof,
(3) the remission or mitigation of such forfeiture,
(4) the compromise of claims, and
(5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

Sec. 2515. - Prohibition of use as evidence of intercepted wire or oral communications

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.

Sec. 2520. - Recovery of civil damages authorized

(a) In General.

Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief.

In an action under this section, appropriate relief includes -

(1) such preliminary and other equitable or declaratory relief as may be appropriate;
(2) damages under subsection (c) and punitive damages in appropriate cases; and
(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of Damages.

(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and not more than $500.
(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1000.

(2) In any other action under this section, the court may assess as damages whichever is the greater of -

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

(d) Defense.
A good faith reliance on -

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;
(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or
(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of is a complete defense against any civil or criminal action brought under this chapter or any other law.

(e) Limitation.
A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

(f) Administrative Discipline.
If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(g) Improper Disclosure Is Violation.
Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).

SELECTED EXCERPTS FROM THE ELECTRONICS COMMUNICATIONS PRIVACY ACT (ECPA) - TITLE 18 U.S.C.
Sec. 2701. - Unlawful access to stored communications
(a) Offense.
Except as provided in subsection (c) of this section whoever -

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents 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.

(b) Punishment.
The punishment for an offense under subsection (a) of this section is -

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain -
(A) a fine under this title or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and
(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and
(2) a fine under this title or imprisonment for not more than six months, or both, in any other case.

(c) **Exceptions.**

Subsection (a) of this section does not apply with respect to conduct authorized -

(1) by the person or entity providing a wire or electronic communications service;
(2) by a user of that service with respect to a communication of or intended for that user; or
(3) in section 2703, 2704 or 2518 of this title

Sec. 2702. - Voluntary disclosure of customer communications or records

(a) **Prohibitions.**

Except as provided in subsection (b),

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service -

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and
(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) **Exceptions for disclosure of communications.**

A provider described in subsection (a) may divulge the contents of a communication -

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;
(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;
(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or
(6) to a law enforcement agency -

(A) if the contents -

(i) were inadvertently obtained by the service provider; and
(ii) appear to pertain to the commission of a crime;
(B) if required by section 227 of the Crime Control Act of 1990; or
(C) if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.

(c) **Exceptions for Disclosure of Customer Records.**

A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2)) -

(1) as otherwise authorized in section 2703;
(2) with the lawful consent of the customer or subscriber;
(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious
physical injury to any person justifies disclosure of the information; or
(5) to any person other than a governmental entity.

Sec. 2707. - Civil action
(a) Cause of Action.
Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief.
In a civil action under this section, appropriate relief includes -
(1) such preliminary and other equitable or declaratory relief as may be appropriate;
(2) damages under subsection (c); and
(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages.
The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

(d) Administrative Discipline.
If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(e) Defense.
A good faith reliance on -
(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title);
(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or
(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of; is a complete defense to any civil or criminal action brought under this chapter or any other law.

(f) Limitation.
A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

(g) Improper Disclosure.
Any willful disclosure of a "record", as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.