UIC John Marshall Journal of Information Technology & Privacy Law

Volume 12
Issue 4 *Journal of Computer & Information Law - Spring 1994*

Article 8

Spring 1994

1993 John Marshall National Moot Court Competition in Information and Privacy Law: Brief for the Respondent, 12 J. Marshall J. Computer & Info. L. 679 (1994)

Spiro P. Fotopoulos

Joseph E. Helweg

Alyce E. Hill

BENCH MEMORANDUM

EAVESDROPPING ON ELECTROMAGNETIC RADIATION: A VIOLATION OF FEDERAL LAW AND/OR AN INTRUSION UPON SECLUSION?

by TIMOTHY R. RABEL

THE TWELFTH ANNUAL JOHN MARSHALL LAW SCHOOL NATIONAL MOOT COURT COMPETITION IN INFORMATION AND PRIVACY LAW

No. 93-8488
IN THE SUPREME COURT
OF THE
STATE OF MARSHALL

Richard LONGSHORE, d.b.a. LONGSHORE COSMETICS,	)	
Petitioner,	)	ON WRIT OF CERTIORARI TO
vs.	)	THE MARSHALL APPELLATE COURT
	)	FIRST JUDICIAL DISTRICT
Harry HACKNER, d.b.a. H&C BEAUTY SUPPLIES,	)	
Respondent.	)	

I. STATEMENT OF THE CASE

Longshore is a resident of the State of Marshall and is the sole proprietor of "Longshore Cosmetics," a mail order cosmetic company located in Newport, State of Marshall. Longshore sells cosmetics throughout the country and advertises through a periodic mailer which

he prepares. In his office, Longshore has a desktop computer equipped with a standard video display terminal (VDT)[1] that he uses for accounting, correspondence, e-mail, billing, inventory and printing labels for the mailer. Because of his low prices, he has developed a very extensive clientele and consequently has been quite successful.

Harry Hackner is also a resident of the State of Marshall and the owner of "H&C Beauty Supplies," a mail order cosmetics company located in Newport and situated directly across the street from Longshore Cosmetics. Hackner has been in direct competition with Longshore for about five years. Recently, H&C had been struggling financially and Hackner told his sales manager Jane Casey that he wished he could obtain Longshore's customer list.

Hackner is quite proficient with computers and as a hobby spends free time keeping up on the latest technologic advances. When he read some articles that discussed the threats of electromagnetic monitoring by a device referred to as "CRT Microspy," Hackner thought this might be the way to obtain Longshore's customer list.

CRT Microspy[2] is a term of art which refers to a device constructed to pick up the electromagnetic radiation that emanates from a computer VDT and then reproduces the VDT image on a remote television screen.[3] Because the emanations from a VDT resemble TV broadcast signals, sometimes basic equipment (for example, a black and white television set) can receive VDT electromagnetic emanations and reproduce the VDT image.[4]

Often, the synchronization frequencies of a VDT do not match those of a TV set and a device can be assembled and attached to the TV set to reproduce the VDT synchronization frequencies.[5] Such an external device generates synchronization signals identical to those of the targeted VDT and sends them into the TV receiver's synchronization separator, thus allowing the reproduction of the targeted VDT image on

---

1. VDT's are also known as video display units (VDU's), computer monitors or computer screens.

2. "CRT" stands for "cathode ray tube," which is the screen of an ordinary television set as well as the monitor or screen of a common desktop computer VDT.

3. *See generally* Vin McLellan, *CRT Spying: A Threat to Corporate Security?*, PC Wk., Mar. 10, 1987, at 35, 46. The author uses "CRT Microspy" to reference the device used to pick up VDT electromagnetic radiation. The process has been referred to as the "van Eck phenomenon." *Id.* at 35.

4. Black and white television receivers are based on the same principles as some VDT's. Wim van Eck, *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?*, 4 Computers & Security 269, 271 (1985). Eck was the first to show how easy it was to receive and decipher the electromagnetic radiation of VDT's.

5. *Id.* The components needed to construct the synchronizing device are readily available at any electronics store.

the TV screen.[6]

Hackner decided to build his own VDT electromagnetic monitoring device so he could receive the electromagnetic emanations from the computer VDT in Longshore's office. On November 19, 1991, Hackner went to a local electronics store, purchased a directional antenna, an antenna amplifier, two adjustable oscillators and a programmable digital frequency divider.[7] Guided by the articles on electromagnetic monitoring and a handbook on television electronics, Hackner used the equipment he purchased to modify a black and white TV set, thus producing his own CRT Microspy.[8]

On November 30, 1991, while sitting in an H&C storeroom, Hackner first used his surveillance device to receive the emanations from the Longshore computer VDT located across the street. At no time did Hackner physically enter Longshore's premises. During the period November 30, 1991, to December 22, 1991, Hackner monitored the electromagnetic emanations of Longshore's computer VDT and simultaneously reproduced the exact data that appeared on Longshore's computer VDT.[9] During this period, Hackner was able to reconstruct Longshore's customer mailing list.

Beginning in January, 1992, H&C began using the list to directly solicit Longshore's clients by offering attractive discounts to new H&C customers. Longshore's business soon began to decline as his customers began switching to H&C. In early March of 1992, Casey learned what Hackner had been doing and became outraged over Hackner's use of his CRT Microspy. On March 13, 1992, Casey left the H&C business. She soon met with Longshore and disclosed Hackner's CRT Microspy procedure.

On April 6, 1992, after learning what Hackner had done, Longshore filed a two count complaint against Hackner in the Newport County Circuit Court. In Count I, Longshore claimed that Hackner's conduct violated the federal wiretap law, specifically, provisions of the Elec-

---

6. *Id.*

7. The programmable digital frequency divider automatically generates the vertical synchronization frequency thus requiring only one of the oscillators to be adjusted manually. *Id.*

8. The technique described herein is based on Wim van Eck's article. Some have claimed that this particular technique could not be duplicated. However, many have been able to achieve the desired result using Wim van Eck's article as guidance. *See, e.g.*, McLellan, *supra* note 3, at 35; John Free et al., *Bugging*, POPULAR SCI., Aug. 1987, at 86 (cover story).

9. Longshore asserts that during this period that he used his computer to compose customer letters, to send and receive e-mail, to conduct an inventory verification and to revise and print his mailing labels.

tronic Communications Privacy Act of 1986 (ECPA).[10] In Count II, Longshore alleged in the alternative that Hackner's use of CRT Microspy was an invasion of privacy as an intrusion upon seclusion.[11] Longshore sought $500,000 in actual damages and an injunction to prevent future use of the customer list.

On April 21, 1992, Hackner filed a motion to dismiss both counts for failure to state a cause of action on two grounds. First, the ECPA did not prohibit the use of CRT Microspy to receive VDT emanations. Second, the alleged facts were insufficient to state a prima facie case for invasion of privacy by intrusion upon seclusion.

On May 1, 1992, Judge Wiseman of the Newport County Circuit Court granted Hackner's motion to dismiss. First, Judge Wiseman held that the ECPA does not encompass the use of a device such as CRT Microspy or Hackner's conduct. Second, the judge held that as a matter of law, Longshore's alleged facts did not state a claim for invasion of privacy by intrusion upon seclusion.

Longshore filed a timely appeal with the Marshall Appellate Court. Because the case was before the appellate court on a motion to dismiss, the appellate court accepted all well pleaded facts set forth above as true.

The appellate court: (1) affirmed the circuit court's order granting Hackner's motion to dismiss Longshore's first count, holding that the ECPA does not apply to the use of a CRT Microspy to receive the electromagnetic radiation of a VDT because Congress did not intend to prohibit the alleged conduct nor did Hackner intercept an electronic communication;[12] and (2) affirmed the circuit court's order dismissing

---

10. Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.) (The ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968).

Longshore filed the first count under 18 U.S.C. § 2520 (1988) (provides civil cause of action for violations of act) asserting that Hackner violated 18 U.S.C. § 2511(1)(a) by intentionally intercepting an "electronic communication" as defined by 18 U.S.C. § 2510(12).

The parties concede, and this court agrees, that the circuit court had jurisdiction over the civil action filed under 18 U.S.C. § 2520. There is a presumption that state and federal courts exercise concurrent subject-matter jurisdiction over a cause of action arising under federal laws absent an explicit or implicit Congressional indication to the contrary. Gulf Offshore Co., Div. of Pool Co. v. Mobil Oil Corp., 453 U.S. 473, 477-78 (1981).

Longshore did not claim that Hackner had intercepted a "wire communication" or "oral communication" as defined by 18 U.S.C. §§ 2510(1), (2) (1988), respectively. Nor did Longshore claim that Hackner intercepted any letter, e-mail message or other correspondence as it was transmitted to the recipient. Longshore's sole assertion is that Hackner's reception of the electromagnetic radiation as it emanated from Longshore's computer VDT violated the ECPA.

11. The State of Marshall has not adopted the Uniform Trade Secrets Act nor recognized a common law cause of action for misappropriation of trade secrets.

12. On appeal, Longshore asserted that the plain meaning of the ECPA prohibits the use of devices such as CRT Microspy to intercept a VDT's electromagnetic radiation.

Longshore's second count, holding as a matter of law, that because Hackner never entered or intruded onto Longshore's premises the alleged facts did not constitute an invasion of privacy by intrusion upon seclusion as the Marshall Supreme Court recognized in *Barstel v. Frepton*, 987 M.2d 345, 348 (Marshall 1980).[13] Longshore then appealed to this court.[14]

II. ISSUES PRESENTED

Whether Hackner's use of a CRT Microspy to receive the electromagnetic radiation from Longshore's computer video display terminal involves:

A. the intentional "interception" of an "electronic communication" in violation of the ECPA; and

B. a violation of privacy by intrusion upon seclusion.

---

13. Though Marshall has recognized a privacy right against intrusion upon seclusion, no Marshall court has had the occasion to apply the tort to the use of new technology, including a CRT Microspy. In *Barstel*, the Marshall Supreme Court cited the RESTATEMENT (SECOND) OF TORTS § 652B (1977), and stated that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." The *Barstel* Court then found that the defendant's unauthorized reading of the plaintiff's diary, while as a guest in the plaintiff's home, was an invasion of privacy by intrusion upon seclusion. The remainder of the facts are not relevant to the case at bar.

14. Review of an order granting a motion to dismiss for failure to state a cause of action is on a de novo basis. In re Delorean Motor Co., 991 F.2d 1236, 1239-40 (6th Cir. 1993); Mayer v. Mylod, 988 F.2d 635, 637 (6th Cir. 1993); McCormack v. Citibank, N.A., 979 F.2d 643, 646 (8th Cir. 1992). Review of a statutory interpretation is also de novo. United States v. Shriver, 989 F.2d 898, 901 (7th Cir. 1993).

A court should grant a motion to dismiss for failure to state a cause of action after construing the complaint in the light most favorable to the plaintiff while accepting all factual allegations as true and if "it appears beyond doubt that the plaintiff can prove no set of facts in support of his claim which would entitle him to relief." Conley v. Gibson, 355 U.S. 41, 45-46 (1957); *Mayer*, 988 F.2d at 638; *McCormack*, 979 F.2d at 646 (citations omitted); *See also* In re Delorean, 991 F.2d at 1240.

III. ANALYSIS OF ISSUES

A. WHETHER HACKNER'S USE OF A CRT MICROSPY TO RECEIVE THE ELECTROMAGNETIC RADIATION OF LONGSHORE'S COMPUTER VIDEO DISPLAY TERMINAL INVOLVES THE INTENTIONAL INTERCEPTION OF AN "ELECTRONIC COMMUNICATION" IN VIOLATION OF THE ECPA.

1. Background

a. The ECPA

In 1968, Congress enacted the Omnibus Crime Control and Safe Streets Act. Title III of this act protected "the privacy of wire and oral communications" and set out the instances of permissible interception for these communications. Title III also provided for both criminal penalties as well as recovery of civil damages. S. REP. NO. 1097, 90th Cong., 2d Sess. — (1968), *reprinted in* 1968 U.S.C.C.A.N 2112, 2153, 2182, 2196.

In 1986, Congress enacted the Electronic Communications Privacy Act which amended Title III. The purpose of the ECPA was to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." S. REP. NO. 99-541, 99th Cong., 2d Sess. 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555. Title I of the ECPA, which is at issue in this case, covers interception of wire, oral and electronic communications and is codified within 18 U.S.C. §§ 2510-2521 (1988). Title II of the ECPA covers "access to stored wire and electronic communications," and Title III of the ECPA specifically addresses devices which do not intercept the contents of communications, such as, pen registers and trap and trace devices. S. REP. NO. 99-541, 99th Cong., 2d Sess. 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

Section 2520 provides that "any person whose wire, oral, or *electronic communication* is *intercepted*, . . . in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate." 18 U.S.C. § 2520(a) (1988) (emphasis added).

Section 2510(4) defines "intercept" as "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." 18 U.S.C. § 2510(4) (1988).

Section 2510(12) defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign

commerce . . . . " 18 U.S.C. § 2510(12) (1988).[15]

Section 2511(1)(a) states:

> (1) Except as otherwise specifically provided in this chapter any person who-
>
> (a) intentionally intercepts, [or] endeavors to intercept, . . . any wire, oral, or electronic communication; . . .
>
> shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5). 18 U.S.C. § 2511(1)(a) (1988).

The key issue in this case under Title I of the ECPA is whether Hackner's conduct amounted to an "interception" of a transaction that constituted an "electronic communication."[16]

b. The CRT Microspy Technology

The fact that electronic equipment emanates electromagnetic radiation has been well known for many years. The phenomenon was first addressed to ensure that such radiation did not interfere with radio and television broadcasts. It was also suspected that someone with highly sophisticated equipment could receive this radiation, "decode" it and obtain the data within the signal. In 1985, Wim van Eck, of the Dr. Neher Laboratories in the Netherlands, published his paper on electromagnetic radiation and described a relatively simple and inexpensive procedure to receive VDT electromagnetic radiation and reconstruct the VDT image; Hackner duplicated this procedure. Wim van Eck, *supra* note 4, at 269.[17]

The United States Government has been concerned with the threat from what commentators have referred to as "electromagnetic eavesdropping" for well over thirty years. *Id.* To counter such threats, the government devised TEMPEST (Transient Electromagnetic Pulse Emanation Standard) to which government equipment must be manufactured. TEMPEST equipment emanates less electromagnetic radiation, thus reducing the possibility of interception. Free, *supra* note 8, at 86-87.[18]

---

15. The definition specifically excludes: "the radio portion of a cordless telephone", wire, oral, tone-only pager and tracking device communications. 18 U.S.C. § 2510(12)(a)-(d) (1988).

16. Section 2511(2)(g)(i) states: "[i]t 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." 18 U.S.C. § 2511(2)(g)(i).

17. Though the ECPA's legislative history discusses testing equipment to ensure such equipment does not interfere with radios and televisions, it does not specifically address eavesdropping on the electromagnetic radiation. S. REP. NO. 541, 99th Cong., 2d Sess. 24-25 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3578-79.

18. Metal shields over the VDT can prevent the electromagnetic radiation's escape.

In the most basic terms, VDT electromagnetic radiation is analogous to a television broadcast.[19] Just as a television broadcast emanates in a sphere for anyone with a television to receive and reproduce, VDT electromagnetic radiation "broadcasts" from the VDT in a sphere where anyone can receive and reproduce the data. While a television broadcast is an intentional transmission of information, VDT electromagnetic radiation is a byproduct of the electronic circuitry.[20]

2. Longshore's Argument

a. Plain Meaning Of The ECPA's Title I Applies To CRT Microspy

i. The "Plain Meaning" Rule

A basic rule of statutory construction requires a court to look at the words of a statute and apply them if the statute is not ambiguous. Except on rare occasion, the plain meaning should prevail. *Rubin v. United States*, 449 U.S. 424, 430 (1981) ("When we find the terms of a statute unambiguous, judicial inquiry is complete, except in rare and exceptional circumstances," citing *TVA v. Hill*, 437 U.S. 153, 187, n.33 (1978)); *Milwaukee Gun Club v. Schulz*, 979 F.2d 1252, 1255 (7th Cir. 1992) ("In so doing, '[w]e begin with the familiar canon of statutory construction that the starting point for interpreting a statute is the language of the statute itself. Absent a clearly expressed legislative intention to the contrary, that language must ordinarily be regarded as conclusive,' " citing *Consumer Prod. Safety Comm'n v. GTE Sylvania, Inc.*, 447 U.S. 102, 108 (1980)). Longshore, therefore, may argue that because the ECPA's plain meaning prohibits Hackner's conduct, the court should not have dismissed the ECPA count.

Wim van Eck, *supra* note 4, at 274. Lining the room with sheets of copper also works. William J. Broad, *Every Computer Whispers its Secrets*, N.Y. TIMES, Apr. 5, 1983, at C-1.

The only reference to TEMPEST in the ECPA's legislative history is in a brief sentence in the House Report which discusses government surveillance done in accordance with an Attorney General approved procedure. The House Report contains a letter from the Attorney General as an example of such surveillance which is exempt from the ECPA. The letter indicates that the sample AG guideline does not cover TEMPEST testing. H.R. REP. NO. 99-647, 99th Cong., 2d Sess., 54-56 (1986).

19. Wim van Eck, *supra* note 4, at 270-71.

20. McLellan, *supra* note 3, at 35; Wim van Eck, *supra* note 4, at 270. Both intentional and unintentional reception can occur. David A. Steele, *Eavesdropping on Electromagnetic Radiation Emanating from Video Display Units: Legal and Self-Help Responses to a New Form of Espionage*, 32 CRIM. L.Q. 253, 255 (1989-90) (VDT image appearing as a ghost image on a TV located in a room adjacent to a computer); "The Radio Control Service of the Netherlands PTT . . . has had several complaints from persons who were receiving information from a nearby travel agency." Wim van Eck, *supra* note 4, at 271.

ii. There Was An Interception

As to the first element, Longshore may claim that there was an "interception" under Title I of the ECPA which defines intercept as the "acquisition of the contents of any . . . electronic . . . communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (1988). Under the statute's plain meaning, Hackner acquired the contents (the information within the electromagnetic radiation) through the use of an electronic or mechanical device (the CRT Microspy).

iii. There Was An "Electronic Communication"

Longshore may assert that the plain meaning of the statute's definition of "electronic communication" is very broad and thus includes VDT electromagnetic radiation. An "electronic communication" is "*any transfer* of . . . writing, images, . . . data, or intelligence of any nature transmitted in whole or in part by a[n] . . . *electromagnetic* . . . system . . . ." 18 U.S.C. § 2510(12) (1988) (emphasis added).

A "transfer" is "to convey, carry, remove, or send from one person, place, or position to another." WEBSTER'S NEW UNIVERSAL UNABRIDGED DICTIONARY 1938 (Deluxe 2d ed. 1979); "To convey or remove from one place, person, etc., to another;" BLACK'S LAW DICTIONARY 1497 (6th ed. 1990). In the case at bar, there was literally a transfer of information, i.e., writing, data and images from Longshore's computer screen to the screen in Hackner's office via electromagnetic radiation.

At least one commentator, viewing electronic communication as "an electrical transfer of information that is not carried by sound waves and cannot be characterized as containing the human voice," concluded that VDT emanations are electronic communications within the ECPA. The ECPA covers all electronic communications unless specifically excluded from the definition. Because VDT's were not specifically excluded, the ECPA protects them. Terri A. Cutrera, Note, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60 UMKC L. REV. 139, 149, 164 (1991).

Though there are no cases that directly address whether electromagnetic radiation is an electronic communication, there are analogous cases.

In *United States v. Herring*, 993 F.2d 784, 786-87 (11th Cir. 1993), the appellants modified a device so it would receive satellite television and were convicted of violating 18 U.S.C § 2512(1)(b) which prohibits the manufacture of devices "primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications . . . ." Appellants argued that the statute applied only to "person-to-person communications where there is a reasonable expectation of privacy."

Id. The court found that the statute's specific definition of electronic communication was very broad and included the television programming involved there. See also *United States v. Davis*, 978 F.2d 415, 416-18 (8th Cir. 1992), where the court held that "electronic communication" was broad enough to include programming transmitted by satellites and the legislative history did not indicate a contrary intent; and *United States v. McNutt*, 908 F.2d 561, 564 (10th Cir. 1990) where the court held that "the plain wording of § 2510(12) [electronic communication] encompasses satellite signals" because they "contain sounds and images and are carried via radio waves."

3. *Hackner's Argument*

a. Title I Of The ECPA Does Not Apply to CRT Microspy

i. Exception To The "Plain Meaning" Rule

Hackner may argue an exception to the "plain meaning" rule when "the literal application of a statute will produce a result demonstrably at odds with the intentions of its drafters . . . ." *Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 571 (1982). Hackner could argue that applying the ECPA's plain meaning to CRT Microspy would bring a result contrary to Congress' intent to protect "communications" or messages by enacting Title III and the ECPA's Title I.

ii. Legislative History Indicates An Intent to Protect Communications

Hackner may claim that Congressional intent and the purpose of Title III was to protect the privacy of communications. S. REP. NO. 1097, 90th Cong., 2d Sess. — (1968), *reprinted in* 1968 U.S.C.C.A.N 2112, 2154, 2156.

In *United States v. Dowdy*, 688 F. Supp. 1477, 1479-80 (D.Colo. 1988), the defendant mail carrier charged with mail embezzlement moved for suppression of evidence gained in alleged violation of Title III. Suspecting that the defendant embezzled mail he was suppose to deliver, postal inspectors placed two undeliverable test letters in the mail for delivery. One letter contained an electronic beeper; as the defendant left work with the undelivered letters the beeper signaled an inspector who had been observing the defendant. The court held that Title III does not apply to monitoring a beeper "because there was no monitoring of the defendant's communications."

When Congress enacted the ECPA to protect electronic communications, Congress' concern was new telecommunications and computer technologies such as electronic mail and computer-to-computer data transmissions. S. REP. NO. 541, 99th Cong., 2d Sess. 2, 5, 14 (1986), *re-*

printed in 1986 U.S.C.C.A.N. 3555, 3556, 3559, 3568. These are forms of communication to deliberately exchange information and messages.

The court in *United States v. Hochman*, 809 F. Supp. 202, 204-06 (E.D.N.Y. 1992), held contrary to the *Herring*, *Davis* and *McNutt* decisions. Here, the defendant's devices allowed viewing of "encrypted pay television programming." In finding that satellite pay television was not an "electronic communication," the court stated:

> Congress enacted the Wiretap Law in 1968 to prohibit "a relatively narrow category of devices whose principal use is likely to be for wiretapping or eavesdropping." The legislative history and the decisions of several courts confirm that the principal concern of Congress was to prevent the use of "spike mikes," disguised microphones, and wiretaps for the purpose of invading the privacy of business and personal communications.
>
> In light of this widely-accepted interpretation, one could easily read the definition of "electronic communications" in § 2510(12) to mean person-to-person or business communications transferred over the electromagnetic spectrum, and nothing more. Afterall, the Court must be mindful of the well-known principle of statutory construction that "if Congress intends for legislation to change the interpretation of a judicially created concept, it makes that intent specific." The failure of Congress in 1986 to expand the category of prohibited devices is presumed to be a ratification of the judicial construction.

Id. at 205 (citations omitted).

In *United States v. Andonian*, 735 F. Supp. 1469, 1470-72 (C.D. Cal. 1990), the court addressed whether video surveillance is covered by the statute. Here, officers installed closed-circuit television in a business suite and conducted video tape surveillance of the defendant. In discussing why Congress passed the ECPA, the court stated that "communications" were Congress' major concern and that Congress passed the ECPA:

> to sharpen the focus on communications, both oral and electronic, and expand the scope to include data transmissions and even the transmissions of electronic images. These are all communications which pass from their origin to the intended recipient and are subject to third-party intervention. Congress' view of interception can be described as a perpendicular concept, where the interception of a communication crosses its path like the trunk of a "T". Video surveillance of a person's activity, unlike the interception of video images in transit, simply does not fit this conception.

Id. at 1472. The court went on to discuss the legislative history indicating that if the video image was intercepted while being transferred, the statute would apply; however, the mere capturing of video images themselves would not be covered. *Id.* at 1472 (quoting S. REP. NO. 541, 99th Cong., 2d Sess. 16-17 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3570-

71). Similarly, Hackner may argue that while Longshore was using his computer, the images on his VDT were not messages being transmitted.

To further support the idea that Title I of the ECPA is not a general surveillance statute, Hackner may cite the ECPA's hearings that included a recommendation that the ECPA be entitled "The Electronic Surveillance Act of 1985." *Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House of Reps. Comm. on the Judiciary*, 99th Cong., 1st & 2d Sess. 348-49 (1985 & 1986) (supplemental statement of Association of North American Radio Clubs). Also, Title III of the ECPA was passed in order to address surveillance technology that did not fit within Title I of the ECPA, i.e., pen registers and trap and trace devices. "A trap and trace device is used to identify the originating number of an incoming wire or electronic communication. These devices do not identify or record the contents of the communication." S. REP. NO. 541, 99th Cong., 2d Sess. 3, 46 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3600.

iii. Electromagnetic Radiation Is Not A Communication

Hackner may define communication as "Information given; the sharing of knowledge by one with another . . . Intercourse; . . . A 'communication' is ordinarily considered to be a *deliberate* interchange of thoughts or opinion between two or more persons . . . . " BLACK'S LAW DICTIONARY 279 (6th ed. 1990) (emphasis added); WEBSTER'S NEW UNIVERSAL UNABRIDGED DICTIONARY 367 (Deluxe 2d ed. 1979) ("intercourse by words, letters, or messages. . ."). Consequently, Hackner may claim that because electromagnetic radiation is itself a byproduct of the electronic circuitry and not a message transmission, it cannot be a communication protected by the ECPA.

In *United States v. Borch*, 695 F. Supp. 898, 899-901 (E.D. Mich. 1988), the court addressed whether under 18 U.S.C. 2510(1) an oral communication overheard when a tapped telephone was left off the hook was a "wire communication." The court noted the split among the courts in how to treat background discussions overheard while a telephone conversation was intercepted and held that the particular conversations involved there were not wire communications under the statute.

> [T]here is a fundamental distinction between background discussions during a point-to-point phone call and face-to-face discourse while no point-to-point call is in progress. Only the former category of conversation can be classified as 'wire communication' within the meaning of the operative statutory language. The latter category, if monitored, involves wire transmission only to the FBI interception equipment, rather than to a "point of reception."

Id. at 901.

[N.B. While the statutory definitions of "wire communication" and "aural transfer" include point-to-point language, the definition of "electronic communication" does not. 18 U.S.C. § 2510 (1), (12), (18). Also, a commentator analyzing communications under a Canadian Law said some may argue that electromagnetic monitoring might be covered because most work done on a computer ultimately becomes a communication. Steele, *supra* note 20, at 260.]

iv. Commentary Support

Hackner may cite at least one commentator who concludes that the ECPA does not cover CRT Microspy. Christopher J. Seline, Note, *Eavesdropping On the Compromising Emanations of Electronic Equipment: The Laws of England and the United States*, 23 CASE W. RES. J. INT'L L. 359, 375-76 (1991): "Either the [National Security Agency] had not informed Congress of its TEMPEST program and Congress failed to criminalize [electromagnetic eavesdropping] through ignorance, or Congress intentionally chose not to criminalize it." Apparently, Seline concluded that the ECPA does not apply because "[t]he information was not transmitted via a common carrier"[21] while failing to note that with the ECPA, Congress removed the "common carrier" requirement found previously in Title III. S. REP. NO. 541, 99th Cong., 2d Sess. 11, 17, 20 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3565, 3571, 3574. Yet, Seline maintains that the definition of electronic communication is broad enough to encompass "a person using his eyes (a photo-optical system) to see [a] neon sign (which by definition transmits information using a photoelectric system)." Seline, *supra* at 377. Later, however, when comparing the ECPA to its English equivalent, Seline notes that the ECPA does not have a common carrier limitation. *Id.* at 379. It appears, therefore, that Seline's analysis may be seriously flawed.

B. WHETHER HACKNER'S USE OF A CRT MICROSPY TO RECEIVE THE ELECTROMAGNETIC RADIATION OF LONGSHORE'S COMPUTER VIDEO DISPLAY TERMINAL IS A VIOLATION OF PRIVACY BY INTRUSION UPON SECLUSION.

1. Background

In a 1890 Harvard Law Review article, Samuel D. Warren and Louis D. Brandeis proposed that privacy was a component of American Tort law.[22] They distinguished the privacy interest from a property

21. Seline, *supra* at 376.

22. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

right and used a Judge Cooley quote to characterize privacy as the right "to be let alone."[23] The first Restatement of Torts reflected Warren and Brandeis' concept of privacy.[24]

In a California Law Review article almost seventy years later, William L. Prosser identified four distinct "branches" to the privacy cause of action. Because of Prosser's involvement with the Restatement (Second) of Torts, that version incorporated his branches[25] and included: 1) "[i]ntrusion upon the plaintiff's seclusion or solitude, or into his private affairs;" 2) "[p]ublic disclosure of embarrassing private facts about the plaintiff;" 3) "[p]ublicity which places the plaintiff in a false light in the public eye;" and 4) "[a]ppropriation, for the defendant's advantage, of the plaintiff's name or likeness." William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

This case involves "intrusion upon seclusion" which in *Barstel v. Frepton*, 987 M.2d 345, 348 (Marshall 1980),[26] the Marshall Supreme Court recognized in accord with the Restatement (Second) of Torts § 652B. "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." At issue is whether the tort applies to the passive reception of freely emanating VDT electromagnetic radiation where the defendant never physically invaded the plaintiff's premises.

2. *Longshore's Intrusion Argument*

a. A Physical Intrusion Is Unnecessary

Longshore may claim that his cause of action for intrusion upon seclusion was improperly dismissed because a "physical" trespass is only one example of an intrusion upon seclusion. Prosser stated that the tort has extended past physical intrusion and is used to fill the gaps left by trespass and other causes of actions. Prosser, *supra* at 390, 392. As the Restatement's comments indicate, the tort imposes liability for invading another's person or "private affairs" by physical intrusion, by aided or unaided senses, or by other "investigation or examination." RESTATEMENT (SECOND) TORTS § 652B cmt. a, b (1977).

For instance, in *Donnel v. Lara*, 703 S.W.2d 257, 259-60 (Tex. App. 1985), the court rejected appellant's contention that telephone harassment cannot be an intrusion upon seclusion as a matter of law and stated that though the tort is generally associated with physical inva-

23. 1 *Privacy Law and Practice* ¶ 1.01, 1-3 (G. Trubow ed. 1991).

24. *Id.*

25. *Id.*

26. *See supra* note 13 for a discussion of *Barstel*.

sions and eavesdropping, such enumerated intrusions are not an all inclusive list.

In *Hamberger v. Eastman*, 206 A.2d 239, 240-41 (N.H. 1964), the plaintiffs, a husband and wife, sued their landlord for invasion of privacy because the defendant placed a recording device in their bedroom. In denying a motion to dismiss, the court cited Prosser and held that the tort is not limited to physical invasions of a home or quarters. In commenting on peeping Toms and eavesdroppers and the potential of harm to personality and mental sanctity, the court stated "[t]he use of parabolic microphones and sonic wave devices designed to pick up conversations in a room without entering it and at a considerable distance away makes the problem far from fanciful." *Id.* at 242 (citing DASH, SCHWARTZ & KNOWLTON, *The Eavesdroppers* 346-58 (1959).

In *LeCrone v. Ohio Bell Telephone Co.*, 201 N.E.2d 533, 536-37, 540 (Ct. App. Oh. 1963), the defendant telephone company provided the plaintiff's estranged husband with an extension on the plaintiffs apartment phone situated nearly 8 miles away. The defendant never went to the plaintiff's apartment or listened to any calls. Instead, the defendant placed a jumper at the central office on the company's equipment. The court held that eavesdropping would be an intrusion; though the defendant's act which made the eavesdropping possible was not an intrusion, the plaintiff stated a prima facie case against her husband.

b. Areas With A Reasonable Expectation Of Privacy

Longshore may claim that his private affairs are an "area" entitled to privacy. Furthermore, the mere unauthorized acquisition of information may be an intrusion upon seclusion. RESTATEMENT (SECOND) TORTS, § 652B, cmt. b, illus. 4 (obtaining access to another's bank records under false pretenses is an intrusion upon seclusion).

In *Pearson v. Dodd*, 410 F.2d 701, 703-05 (D.C. Cir. 1969), the defendant received and published information knowing that some of the plaintiff's former employees obtained the information by entering the plaintiff's office and copying his files. Though the court did not find the defendant liable for intrusion because he only received the information, the court stated:

> [w]e approve the extension of the tort of invasion of privacy to instances of intrusion, whether by physical trespass or not, into spheres from which an ordinary man in a plaintiff's position could reasonably expect that the particular defendant should be excluded. Just as the Fourth Amendment has expanded to protect citizens from government intrusions where intrusion is not reasonably expected, so should tort law protect citizens from other citizens. The protection should not turn exclusively on the question of whether the intrusion involves a

> technical trespass under the law of property. The common law, like the Fourth Amendment, should 'protect people, not places.'

Id. at 704 (footnotes omitted).

3. *Hackner's Intrusion Argument*

a. Hackner Never Intruded Physically Or Otherwise

Hackner may assert that Longshore must allege a physical trespass or intrusion into some area entitled to privacy.

The court in *Heath v. Playboy Enterprises, Inc.*, 732 F. Supp. 1145, 1147-48, n.8 (S.D. Fla. 1990), held that the publication of an article with a photo of the plaintiff while on courthouse steps did not involve the intrusion upon seclusion tort because the plaintiff did not show a "trespass or intrusion upon physical solitude . . . ."

In *Pierson v. News Group Publications, Inc.*, 549 F. Supp. 635, 637-38 (S.D. Ga. 1982), the plaintiff, a soldier, sued a tabloid publisher whose reporters took photographs and gathered information as they accompanied the plaintiff's platoon during a training session on military grounds. The defendant then published articles with photographs of the training. The court granted the defendant's summary judgment because the plaintiff did not show a physical intrusion similar to a trespass; "[a]n essential element of this tort . . . ." Furthermore, the plaintiff was held not to have a reasonable expectation of privacy while on military grounds. *Id.* at 640.

In *Finlay v. Finlay*, 856 P.2d 183, 189-90 (Kan. App. 1993), the plaintiff lived across the street from the defendant who operated a cattle feeding operation. Among other claims, the plaintiff contended that the smell resulting from the cattle feeding operation was an intrusion upon seclusion. In affirming the trial court's granting of the defendant's motion for summary judgment, the *Finlay* court held that the gist of the intrusion tort is "that an individual's right to be left alone is interfered with by the defendant's physical intrusion, or by an intrusion of defendant using his or her sensory faculties." The court further held that for there to be liability, the defendant must "place himself physically, or by means of his senses, within plaintiff's zone of privacy." Because there was no physical or sensory intrusion, and the "plaintiff's private affairs [were] not exposed to the defendant's physical" or sensory presence, granting the defendant's summary judgment motion was correct.

In *Nelson v. Times*, 373 A.2d 1221, 1222-23 (Me. 1977), the plaintiff sued the defendant for intrusion upon seclusion because the defendant published a picture of the infant plaintiff. In affirming the defendant's motion to dismiss, the *Nelson* court held that the intrusion tort requires "an actual invasion 'of something secret, secluded or private pertaining

to the plaintiff.' " (citing *Estate of Berthiaume v. Pratt, M.D.*, 365 A.2d 792, 795 (Me. 1976)). The *Nelson* court held that the Restatement and its comments required the plaintiff to assert at least "a physical intrusion upon premises occupied privately by a plaintiff for purposes of seclusion." *Id.* at 1223.

In *Loe v. Town of Thomaston*, 600 A.2d 1090, 1091-92 (Me. 1991), the plaintiff alleged that the defendant's disclosure of the terms of the parties' union grievance proceeding settlement constituted an intrusion upon seclusion. The court affirmed the defendant's summary judgment because the plaintiff did not minimally allege a physical intrusion, i.e., that the "defendant physically invaded premises that she occupied for purposes of seclusion." *Id.* at 1093 (quoting *Nelson v. Times*, 373 A.2d 1221, 1223 (Me. 1977).

In *Kobeck v. Nabisco, Inc.*, 305 S.E.2d 183, 184-85 (Ga. App. 1983), the plaintiff sued her employer for disclosing to her husband the plaintiff's absentee record. The court held that the plaintiff could not establish an intrusion upon seclusion because there was no physical intrusion similar to a trespass.

b. No Reasonable Expectation Of Privacy In Electromagnetic Radiation

Hackner may cite some cases where law enforcement officers intercepted radio communications (i.e., mobile, cellular and cordless). Most courts that have addressed interception of radio communications concluded that there is no reasonable expectation of privacy in such communications because they utilize radio waves which are accessible by anyone with a receiver tuned to the same frequency in the broadcast range. *See, e.g., United States v. Hoffa*, 436 F.2d 1243, 1246-47 (7th Cir. 1970) (no reasonable expectation of privacy in mobile telephone because the mobile phone's radio signals were "exposed to everyone in that area who possessed a F.M. radio . . ."); *United States v. Carr*, 805 F. Supp. 1266, 1274-76 (E.D.N.C. 1992) (no more reasonable an expectation of privacy in cordless phone use under Fourth Amendment than a "shouter"); *Edwards v. Bardwell*, 632 F. Supp. 584, 589 (M.D. La. 1986), *aff'd*, 808 F.2d 54 (5th Cir. 1986) (mobile phone communication is not protected as an "oral communication" under Title III civil action, there is no reasonable expectation of privacy); *Salmon v. State*, 426 S.E.2d 160, 162 (Ga. App. 1992) ("no justifiable expectation of privacy" in cellular phone communications); *State v. Smith*, 438 N.W.2d 571, 577 (Wis. 1989) (Fourth Amendment does not protect cordless phones labeled with lack of privacy warning as there is no reasonable expectation of privacy). Hackner may also try to analogize the interception of electromagnetic radiation to the use of thermal imagers which detect temperature

changes on the surface of objects. Police use such devices to detect excessive heat escaping from buildings which may indicate heat generated from marijuana cultivation.

In *United States v. Penney-Feeney*, 773 F. Supp. 220, 226-28 (D.Haw. 1991), the defendant ventilated the excessive heat out of the garage where he was cultivating marijuana. The court held that the heat was not a protected communication but a byproduct or "heat waste" in which the defendant could not expect privacy, similar to abandoned garbage and odors from a suitcase. Therefore, thermal imaging was not a search under the Fourth Amendment. *Id.* (citing *California v. Greenwood*, 486 U.S. 35, 40-41 (1988) (no privacy expectation in garbage put out where it is common knowledge others may access it and left for third parties)). Though *Penney-Feeney* was affirmed in 984 F.2d 1053 (9th Cir. 1993), the court did not determine whether thermal imaging violated the Fourth Amendment because probable cause existed without the thermal imaging evidence. *Id.* at 1056.

In *United States v. Kyllo*, 809 F. Supp. 787, 792 (D.Or. 1992), the government used thermal imaging to determine the amount of heat emanating from the defendant's home. The court cited *Penney-Feeney* and denied the defendant's motion to suppress because under the Fourth Amendment, "the use of a thermal imaging device here was not an intrusion into Kyllo's home. No intimate details of the home were observed, and there was no intrusion upon the privacy of the individuals within the home."

No. 93-8488

In The
SUPREME COURT OF THE STATE OF MARSHALL

October Term, 1993

RICHARD LONGSHORE, d.b.a.
LONGSHORE COSMETICS

Petitioner,

v.

HARRY HACKNER, d.b.a.
H&C BEAUTY SUPPLIES

Respondent.

On Appeal from the Marshall Appellate
Court for the First Judicial District

BRIEF FOR THE PETITIONER

Oral Argument Requested

Marie-Louise R. Samuels
Thomas W. Poulton
Scott W. McMickle

Counsel for the Petitioner
University of Florida
College of Law
111 Holland Hall
Gainesville, Fl. 32611
(904) 392-2122

No. 93-8488

In The
SUPREME COURT OF THE STATE OF MARSHALL

October Term, 1993

RICHARD LONGSHORE, d.b.a.
LONGSHORE COSMETICS

Petitioner,

v.

HARRY HACKNER, d.b.a.
H&C BEAUTY SUPPLIES

Respondent.

On Appeal from the Marshall Appellate
Court for the First Judicial District

QUESTIONS PRESENTED

1. Whether the use of CRT Microspy to intentionally intercept confidential business information radiated from a computer terminal in the form of electromagnetic radio waves is prohibited by the Electronic Communications Privacy Act of 1986?

2. Whether the use of CRT Microspy to intentionally intercept confidential business information represents an intrusion upon seclusion under Restatement (Second) of Torts § 652B, where no physical invasion of a place occurs?

TABLE OF CONTENTS

QUESTIONS PRESENTED

1. *Whether the use of CRT Microspy to intentionally intercept confidential business information radiated from a computer terminal in the form of electromagnetic radio waves is prohibited by the Electronic Communications Privacy Act of 1986?*

2. *Whether the use of CRT Microspy to intentionally intercept confidential business information represents an intrusion upon seclusion under Restatement (Second) of Torts § 652B, where no physical invasion of a place occurs?*

TABLE OF AUTHORITIES

Page(s)

UNITED STATES SUPREME COURT CASES

UNITED STATES CIRCUIT COURTS OF APPEAL CASES

UNITED STATES DISTRICT COURT CASES

STATE COURT CASES

CONSTITUTIONAL AND STATUTORY PROVISIONS

REGULATORY PROVISIONS

RESTATEMENT PROVISIONS

LEGISLATIVE MATERIALS

LAW REVIEW ARTICLES

SUPPLEMENTAL SOURCES

OPINIONS BELOW

The opinion of the Marshall Appellate Court for the First Judicial District is unreported and appears in the record below at pages 1-8. The opinion of the Newport County Circuit Court is unreported.

STATEMENT OF JURISDICTION

A formal statement of jurisdiction has been omitted pursuant to Rule § 1020(2) of this competition.

CONSTITUTIONAL, RESTATEMENT, AND STATUTORY PROVISIONS INVOLVED

The Fourth Amendment to the United States Constitution, U.S. Const. amend. IV., portions of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 100 Sat. 1848 (codified as amended in scattered sections of 18 U.S.C.), and the Restatement (Second) of Torts § 652B are relevant to this appeal and can be found in Appendices A, B, and C, respectively.

STATEMENT OF THE CASE

I. Summary of proceedings below.

Petitioner Richard Longshore, d/b/a Longshore Cosmetics (LONGSHORE), sued Respondent Harry Hackner, d/b/a H&C Beauty Supplies (HACKNER), on April 6, 1992. (R.5). The suit was a two-count complaint alleging: 1) that certain acts by HACKNER violated provisions of the federal Electronic Communications Privacy Act of 1986 (ECPA); and, 2) that these acts were intrusions upon seclusion, constituting invasions of LONGSHORE'S common law privacy interests. (R.5).

On May 1, 1992, Newport County Circuit Judge Marlo Wiseman granted HACKNER'S motion to dismiss for failure to state a claim on both counts. (R.6). The Marshall Appellate Court for the First Judicial District, T. Lebar, Judge, affirmed the lower court's ruling. (R.7-8).

The Supreme Court of the State of Marshall, B. Woburt, Chief Judge, on July 19, 1993, granted Petitioner LONGSHORE leave to appeal the decision of the Marshall Appellate Court and ordered the parties to this action to address the following issues raised by the First Judicial District: (1) Whether Hackner violated the ECPA when he used a "CRT Microspy" to receive the electronic emanations of Longshore's computer video terminal (VDT); and, (2) Whether undisputed facts that establish the use of a CRT Microspy to reproduce the images on a remote VDT are sufficient to state a claim for intrusion upon seclusion. The order granting LONGSHORE leave to appeal also granted an oral argument.

II. Summary of the facts.

LONGSHORE, the plaintiff below, is the sole proprietor of a nationwide mail-order cosmetics company located in Newport, Marshall. (R.2). One of his business competitors is HACKNER, the defendant below. (R.2).

In March of 1992, former HACKNER sales manager Jane Casey told LONGSHORE of a scheme by which HACKNER managed to obtain LONGSHORE'S customer list. (R.4). Using a device known as a CRT Microspy, HACKNER copied LONGSHORE's customer list and used it to offer extreme discounts in an effort to lure LONGSHORE customers over to HACKNER'S business. (R.4).

CRT Microspy can be built by computer enthusiasts such as HACKNER from materials available at any electronics store. (R.3). When aimed at a computer monitor, a CRT Microspy can "read" the electromagnetic images emanating from the monitor, reproducing them on a television screen. (R.3). These electromagnetic images penetrate walls and can be picked up by a CRT Microspy from outside the room or building where the computer monitor is operating. (R.3-4). In this case, HACKNER was able to construct a CRT Microspy using a television set, a directional antenna, an antenna amplifier, two adjustable oscillators, and a programmable digital frequency divider. (R.3-4).

HACKNER first used a CRT Microspy to observe LONGHSORE'S computer monitor on November 30, 1991. (R.4). HACKNER, positioned in his own building located across the street from LONGSHORE'S, and used his "surveillance device" to intercept LONGSHORE'S computer monitor images. (R.4). HACKNER continued to use the CRT Microspy to intercept data from LONGSHORE'S computer until December 22, 1991. (R.4). According to LONGSHORE, images retrieved during this period were not limited to LONGSHORE'S customer list and included e-mail, customer letters, and inventory information. (R.4). By January, 1992, HACKNER composed a list of all of LONGSHORE'S customers. (R.4). As a result of HACKNER'S aggressive discount program targeted at the LONGSHORE customer list, LONGSHORE customers began switching to HACKNER. Consequently, LONGSHORE'S business declined. (R.4).

LONGSHORE'S suit sought $500,000 in actual damages and an injunction to prevent HACKNER'S further use of the customer mailing list. (R. 5). Both counts of the complaint were dismissed by the trial court for failure to state a claim. (R.6). The decision of the trial court was affirmed by the Marshall Appellate Court for the First Judicial District. (R. 7-8).

In affirming the trial court's dismissal of LONGSHORE'S federal ECPA allegation, the appellate court rejected LONGSHORE'S argu-

ment that the plain meaning of the ECPA prohibits the use of a CRT Microspy to intercept the electromagnetic emanations from another's video terminal. (R.6). The appellate court also agreed with the trial court's ruling that Congress did not intend to forbid the interception of VDT radiations, nor did Hackner's conduct amount to an interception of an electronic communication. (R.6).

In affirming the trial court's opinion with respect to LONGSHORE'S common law privacy claim, the appellate court acknowledged that no Marshall court had yet confronted the peculiar aspects of such technology in the context of an intrusion upon seclusion claim. (R.6). The appellate court, however, agreed with the trial court that the absence of a physical intrusion by HACKNER justified dismissal of LONGSHORE'S claim. (R.8).

On July 19, 1993, this court granted LONGSHORE leave to appeal.

SUMMARY OF ARGUMENT

This appeal involves the interpretation of a federal statute and the application of a common law principle to the use of a new technology. This technology, CRT Microspy, was used by HACKNER to invade the privacy of LONGSHORE in order to gain an unfair business advantage. LONGSHORE respectfully requests that this court reverse the decisions of the trial and appellate courts below with instructions that this action be allowed to proceed.

This appeal represents a *de novo* review of the decision of the Marshall Appellate Court for the First Judicial District. Both counts were dismissed by the trial court for failure to state a claim and the appellate court affirmed. Thus, the question here is whether the undisputed facts of the case are sufficient to establish causes of action for violations of the Electronic Communications Privacy Act of 1986 (ECPA) and/or tortious intrusion upon seclusion.

HACKNER'S use of a CRT Microspy to intentionally intercept LONGSHORE'S mailing list was an interception of an electronic communication prohibited by the ECPA. Because this is an issue of statutory interpretation, this court must first look to the plain language of the statute. The ECPA broadly defines the terms "intercept" and "electronic communication." An electronic communication is any transfer of data through the use of an electromagnetic or radio system. Because a computer is an electromagnetic system and the information from the VDT was leaked in the form of radio waves, LONGSHORE'S mailing list as it appeared on his VDT was an electronic communication protected by the ECPA.

The plain language of the statute also states that, unless the electronic communication is specifically excluded from the statute, its interception is prohibited. Nowhere in the statute is a VDT transmission or the term CRT Microspy listed as an exception. Therefore, HACKNER'S conduct was prohibited by the ECPA.

Moreover, should this court find that the language of the ECPA is ambiguous, it must still hold that LONGSHORE stated a cause of action because the legislative history, and regulatory scheme of the ECPA demonstrate that Congress intended to protect computer communications. Throughout the legislative history it is clear that the purpose of the ECPA was to fill gaps in existing privacy law created by rapid and increasingly sophisticated technological growth. Congress also recognized the need to draft a broad law which would cover technologies yet to be invented. The fact that Congress does not explicitly list CRT Microspy or radio emissions from a VDT in the legislative history is not dispositive. It is Congress' intent that matters. That intent was to protect privacy with a broad law that was not contingent on meaningless

technological distinctions. Therefore, LONGSHORE stated a cause of action against HACKNER for violation of the ECPA.

With regard to the second count of LONGSHORE'S complaint, this court should hold that the tort of intrusion upon seclusion does not require a physical invasion. The State of Marshall should join the majority of states which, when faced with this question, have interpreted Restatement (Second) of Torts § 652B to mean that no physical invasion is required for that tort to have occurred. This approach is justified because, like the Fourth Amendment, the tort protects people, not places.

LONGSHORE respectfully suggests that the courts below have confused the means by which HACKNER committed this tort with its result. The intrusion upon seclusion tort is not dependent on how it occurs and distinctions relying on the presence or absence of a physical invasion miss the point of the tort. The intrusion occurred in this case when HACKNER intercepted confidential computer information.

To hold that lack of a physical invasion precludes HACKNER'S claim for intrusion upon seclusion would ignore the realities of modern technology. Advances in surveillance mechanisms mandate that traditional notions of invasions of privacy yield to the need to protect critical personal and business interests.

For these reasons, LONGSHORE respectfully requests that this court reverse the decisions of the Marshall Appellate Court for the First Judicial District and of the Newport County Circuit Court and hold that LONGSHORE'S complaint stated claims for both a violation of the ECPA and the commission of the tort of intrusion upon seclusion.

ARGUMENT

I. HACKNER'S USE OF A CRT MICROSPY TO COVERTLY INTERCEPT THE ELECTROMAGNETIC WAVES EMITTED BY LONGSHORE'S PERSONAL COMPUTER FALLS SQUARELY UNDER THE PROHIBITIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

This issue is one of pure statutory interpretation. The dispute is whether HACKNER'S financially motivated and surreptitious use of a CRT microspy to acquire LONGSHORE'S mailing list constitutes an interception of an electronic communication prohibited by the Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (1986)(codified as amended in scattered sections of 18 U.S.C.). Both the plain meaning of the ECPA and the legislative history of the ECPA clearly demonstrate that HACKNER'S interception of LONGSHORE'S customer list is an invasion of privacy prohibited by the ECPA.

A. The ECPA encompasses HACKNER'S conduct because such conduct fits within the broad definitions of "intercept" and "electronic communication" and is not specifically excluded by the statute.

In cases of statutory interpretation, courts must first look to the plain meaning of the statute and assume it accurately reflects the legislative purpose. *Park 'N Fly, Inc. v. Dollar Park And Fly, Inc.*, 469 U.S. 189, 194 (1985). HACKNER'S conduct constitutes an interception of an electronic communication under the plain meaning of the ECPA. When the intent of Congress is expressed in reasonably plain terms, a court must treat that language as conclusive. *Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 575 (1982). Therefore, this Court need look no further than the statute for the definitions of the key phrases, "electronic communication" and "intercepts."

It is clear that HACKNER'S conduct falls within the ECPA's prohibition against an interception of an electronic communication as defined in 18 U.S.C. § 2511. This section provides in relevant part:

> (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 endeavors to intercept any wire, oral or electronic communication . . . [violates this Act]. (emphasis added).

18 U.S.C. § 2511 (1993).

Moreover, in § 2510 (12), the ECPA defines an electronic communication as:

> any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. (emphasis added).

18 U.S.C. § 2510 (1993).

LONGSHORE'S retrieval of data from his hard drive to his VDT meets the essential elements of an electronic communication as defined by § 2510(12). The three elements required by the statute are: one, a transfer of data; two, the transfer must be by an electromagnetic or radio system; and three, the data transferred must affect interstate commerce. When LONGSHORE pulled up his mailing list onto his VDT, the computer transferred information stored in binary digits on the microchip and translated it into readable data which appeared on LONGSHORE's VDT. Murray Sargent III, Richard L. Shoemaker, The IBM PC From the Inside Out, at 242. (Revised ed. 1986). The electronic signals emitted by the VDT during the transfer of information from the hard drive were leaked in the form of radio waves. Terri A. Cutrera, The Constitution in Cyberspace: The Fundamental Rights of Computer

Users, 60 U.M.K.C. L. REV. 139, 141 (Fall, 1991). These waves also resemble television broadcast signals. (R. at 3). This transfer of radio waves included LONGSHORE's customer list. LONGSHORE distributes his products to customers nationwide so the information HACKNER intercepted affects interstate commerce. Therefore, LONGSHORE'S retrieval of his mailing list is clearly an electronic communication as defined by the ECPA.

Furthermore, the electromagnetic emissions leaked by LONGSHORE'S computer resemble television broadcast signals or radio waves, thus they are judicially recognized as a protected communication. Television broadcast signals are electronic communications as defined by the ECPA. *United States v. Splawn*, 982 F.2d 414, 416 (10th Cir. 1992), *cert. denied*, 113 S.Ct. 2365 (1993). In *Splawn*, the court held that satellite television broadcast signals are a form of electronic communication intended to be protected by the ECPA. *Id.* At least five other jurisdictions have also held television broadcast signals to be electronic communications as defined by the ECPA. *See, e.g., United States v. Shriver*, 989 F.2d 898 (7th Cir. 1992); *United States v. One Macom Video Cipher II*, 985 F.2d 258 (6th Cir. 1993); *United States v. Harrell*, 983 F.2d 36 (5th Cir. 1993); *United States v. Davis*, 978 F.2d 415 (8th Cir. 1992); *United States v. Lande*, 968 F. 2d 907 (9th Cir. 1992), *cert. denied*, 113 S.Ct. 1299 (1993). LONGSHORE's VDT waves resemble television waves and therefore, must be included under the ECPA. Additionally, while intercepting mailing list data, HACKNER apparently also intercepted e-mail communications. (R. at 4). This interception alone should bring Hackner's conduct within the confines of the ECPA.

HACKNER'S conduct also amounts to an "interception" as defined in the plain language of § 2510(4). This section defines intercept as ". . . the aural or other acquisition of the contents of any . . . electronic . . . communication through the use of any electronic, mechanical or other device." 18 U.S.C. § 2510(4)(1993). HACKNER's use of the CRT Microspy (consisting of the antenna, the amplifier and the programmable digital frequency divider) to acquire the data from LONGSHORE's VDT meets the clear language of the ECPA.

Additionally the CRT Microspy resembles a radio scanner and radio scanners are devices which "intercept" radio signals for purposes of the ECPA. *United States v. Smith*, 978 F.2d 171 (5th Cir. 1992), *cert. denied*, 113 S.Ct. 1620 (1993). In *Smith*, a man listening to a Bearcat scanner overheard a neighbor's conversation on a cordless phone. *Id.* at 173. The court reasoned that the Bearcat scanner intercepted the radio waves of the phone. *Id.* at 175. While the court held the conduct at issue did not violate the ECPA because "cordless phones are specifically excepted" from the ECPA, it still reasoned that the scanner intercepted the electromagnetic-radio waves. *Id.* HACKNER's use of a device to ac-

quire information falls within the statutory definition of "intercept" and is similar to conduct judicially acknowledged as an interception. Consequently, HACKNER'S conduct amounts to an interception under the ECPA.

HACKNER'S conduct is also covered by the ECPA because it was not specifically excluded by the plain language of the statute. The general rule of statutory interpretation holds that when Congress explicitly lists exceptions to a broad, general scheme, exceptions not explicitly made by Congress should not be implied. *Andrus v. Glover Construction Co.*, 446 U.S. 608, 616-17 (1980). In other words, statutes covering broad categories followed by narrow exclusions include all conduct or things contained in the broad category and not specifically listed as an exception. In addition, the plain language of ECPA § 2511 states that an intentional interception of an electronic communication is a violation of the statute unless it is specifically excluded. 18 U.S.C. § 2511(1) (1993). While CRT Microspy comes under the umbrella of the ECPA's broad definitions of "intercept" and "electronic communication," nowhere in the ECPA is "CRT Microspy" or "computer electronic radio emissions" listed as an exclusion.

The only area which might be deemed ambiguous is the exception contained in § 2511(2)(g), which states that "it shall not be unlawful under this chapter . . . (i) to intercept or access an electronic communication made through an electronic communications system that is configured so that such electronic communication is readily accessible to the general public. . ." 18 U.S.C. § 2510(2)(g) (1993). Furthermore, 18 U.S.C. § 2510(14) defines an electronic communications system as ". . . any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications . . ." 18 U.S.C. § 2510(14) (1993). Additionally, 18 U.S.C. § 2510(16) defines readily accessible to the general public as ". . . with respect to a radio communication . . . [such communication that is]. . . not . . . scrambled or encrypted." 18 U.S.C. § 2510(16) (1993).

While it could be argued that a personal computer falls under the definition of an electronic communications system because it is an "electromagnetic . . . facilit[y] for the transmission of electronic communications . . . or . . . the storage of electronic communications," it would be absurd and contrary to Congress' intent to hold that a computer's radio leaks are "readily accessible to the general public." This is true for two reasons.

First, radio waves emitted by personal computers are not the type of radio communication intended to be covered by the statutory phrase "readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(1993).

A statute is not to be interpreted so that portions of it are rendered meaningless. *Fulps v. City of Springfield*, 715 F.2d 1088, 1093 (6th Cir. 1983). While it is true that the electromagnetic waves leaked from LONGSHORE'S computer and surreptitiously intercepted by HACKNER were a form of radio waves, to hold that these unencrypted radio waves were the type of radio waves Congress intended to exempt would render much of the ECPA meaningless. If such an interpretation were adopted, no computer, unless its leaks were somehow encrypted, would be protected by the ECPA from computer sneak thieves. E-Mail, private financial information, confidential medical files, and almost all electronic communications transmitted by computer would be exempt from protection by the ECPA.

Second, the ECPA does not require encryption of all forms of radio waves for its protections to apply. *Shubert v. Metrophone, Inc.*, 898 F.2d 401, 403-404 (3rd Cir. 1990). In *Shubert*, the plaintiffs alleged that a cellular telephone service provider violated the ECPA provision against divulging the contents of a communication because the company failed to encrypt the transmissions. *Id.* at 402. The court held that the ECPA does not impose a general duty upon a cellular service provider to encrypt or otherwise render its transmissions incapable of interception. *Id.* at 403. Cellular phones are broadcast partially using radio waves and partially using wires. *Id.* at 402. However, merely because cellular phone conversations are partially broadcast through unencrypted radio waves does not mean they are not protected by the ECPA. *Id.* at 403. *See also United States v. Carr*, 805 F. Supp. 1266, 1269 (E.D.N.C. 1992) (recognizing that cellular phone conversations are partially transmitted by radio waves). The radio waves leaked by LONGSHORE's computer are analogous to radio waves leaked by cellular telephones and therefore LONGSHORE had no duty to scramble or encrypt the waves for the ECPA to apply.

While radio waves from computers can be analogized to the ECPA's protection of cellular phones, the ECPA's exclusion of coverage of radio waves emitted by cordless phones is clearly distinguishable at three levels. First, while it is true that cordless phones like cellular phones are partially transmitted through radio waves, cordless phones are explicitly excepted from coverage under the ECPA in § 2510(12)(a). *United States v. Smith* at 175; *Carr* at 1270.

Second, cordless phones carry a warning under FCC rules that "privacy of communications" is not assured. *State v. Smith*, 438 N.W.2d 571, 577 (Wis. 1989). Computers also carry an FCC warning that they unintentionally radiate electromagnetic radio waves. 47 C.F.R. § 15.105(b)(1992). The warning advises the user that a computer monitor is a Class B device that "generates, uses and can radiate radio fre-

quency energy." *Id.* However, this warning does not clearly inform the user that his computer screen can be monitored at any time.

Third, even if this warning did inform the user of a lack of privacy, computer radio emissions are electronic communications not oral communications for purposes of the ECPA. 18 U.S.C. § 2510(14)(1993). The ECPA only requires a reasonable expectation of privacy analysis when dealing with oral communications, not with electronic communications. *Carr* at 1271.

In sum, the distinctions between radio emissions from wire telephones, cordless telephones and cellular telephones are distinctions without a difference. *See State v. McVeigh*, 620 A.2d 133 (Conn. 1993) (recognizing the ECPA does not protect cordless phone conversations but that the Connecticut communications privacy statute recognizes privacy rights for cordless, cellular and wire phone conversations, all three of which are carried in part through radio technology). The only distinction between the three forms of telephone communication and radio waves leaked by computers is that the ECPA itself has specifically carved out an exception for cordless phones. To read an ambiguity into the ECPA and sweep computer radio emissions into that narrow exception would be both absurd and contrary to legislative intent.

B. Assuming, arguendo, that the plain meaning of the ECPA is not clear, this Court should adopt a statutory interpretation that gives effect to Congress' intent to protect confidential computer information.

If this Court concludes that the plain meaning of the ECPA is vague or unclear with regard to the treatment of computer radio wave emissions, then it should adopt an interpretation consistent with Congress' intent.

It is clear that Congress' intent was to protect computer communications and business secrets from computer sneak thieves like HACKNER. Congress' intent in the adoption of the ECPA is critical to the Act's interpretation. This is true because a court constructed meaning which ignores Congress' intent thwarts the very goal of statutory interpretation.

A variety of jurisdictions have recognized that the Legislature's intent is the controlling factor in statutory interpretation. For example, the Supreme Court of Michigan has noted that "[a] court's responsibility when it construes a statute is to implement the purpose and intent of those who enact it." *Michigan v. Gilbert*, 324 N.W.2d 834, 838 (Mich. 1982). The "lodestar" of construction is legislative intent. *Id.* at 841.

To that extent, this court should look to the "purpose, the subject matter, the context, [and] the legislative history" of the ECPA to deter-

mine whether it was Congress' intent that the use of CRT Microspy be prohibited. *United States v. Cooper Corporation*, 312 U.S. 600, 604-605 (1940). The Supreme Court of Washington succinctly stated:

> [t]he goal of statutory construction is, of course, to give effect to the intent of the Legislature. Where the meaning of the statute is clear from the language of the statute alone, there is no room for judicial interpretation. If the language of the statute is amenable to more than one construction, however, resort to legislative history and other aids to construction is appropriate.

Kadoranian v. Bellingham Police Dep't, 829 P.2d 1061, 1064-1065 (Wash. 1992).

To hold that computer radio wave emissions are not protected would place all computer communications in a netherworld of privacy law. This would be an absurd and unreasonable result. The Supreme Court stated in *United States v. American Trucking Ass'n, Inc.*:

> [w]hen [the plain] meaning [leads] to absurd or futile results this court has looked beyond the words to the purpose of the act. Obviously there is danger that the courts' conclusion as to legislative purpose will be unconsciously influenced by . . . factors not considered by the enacting body. A lively appreciation of the danger is the best assurance of escape from its threat but hardly justifies the acceptance of a literal interpretation dogma which withholds from the courts . . . information for reaching a correct conclusion.

United States v. American Trucking Ass'n, Inc., 310 U.S. 534, 543-544 (1940) *reh'g denied* 311 U.S. 724 (1940).

Therefore, if CRT Microspy does not come within the plain meaning of the ECPA, this Court should consider the Congressional intent behind the enactment of the ECPA. Congress endeavored to include CRT Microspy in the Act and this court should honor that purpose.

C. Based on the background and legislative history of the ECPA, Congress' intent was to protect the privacy of computer information from interception by such technologies as CRT Microspy.

The background for the adoption of the ECPA illustrates the Act's purpose. The Framers of the Constitution sought to protect privacy rights by enacting the Fourth Amendment which reads in part "[t]he right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated . . . ." U.S. CONST. amend. IV.

However, as industrialized America churned into the 20th Century, rapidly expanding communication and information technologies threatened to make the Fourth Amendment obsolete. *See* S. REP. NO. 541, 99th Cong. 2d Sess. (1986) 2, *reprinted in* 1986 U.S.C.C.A. 3555,

3556; Robert W. Kastenmeier, Deborah Leavy, David Beier, Communications Privacy: A Legislative Perspective, 1989 WIS.L.REV. 715 (1989). By 1928, a majority of the United States Supreme Court had held that the Fourth Amendment does not protect citizens from Government eavesdropping through the use of a telephone wiretap. *Olmstead v. United States*, 277 U.S. 438 (1928). The court reasoned that government agents' acts failed to amount to a "search" or a "seizure" because the information was "secured by the use of the sense of hearing and that only." *Id.* at 464-65.

Today the *Olmstead* decision is most recognized not for the curious logic of the majority but for Justice Brandeis' "prescient" dissent. *See* S. REP. NO. 541 at 3556. As Justice Brandeis warned "[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court. Can it be that the Constitution affords no protection against such invasions of individual security?" *Olmstead* 277 U.S. at 474. *See also* Donald Battaglia, Note, *State v. Delaurier*: Privacy Rights and Cordless Telephones-The Fourth Amendment Is Put on Hold, 19 J. MARSHALL L. REV. 1087, 1092 (1986).

Forty years later, the Supreme Court recognized Justice Brandeis' reasoning by overruling *Olmstead* and holding that the Fourth Amendment "protects people not things." *Katz v. United States*, 389 U.S. 347 (1967). Approximately one year later Congress confirmed the Court's decision by enacting Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III). 18 U.S.C. §§ 2510-2520 (1982) *See* S. REP. NO. 541 at 3556. Title III sought to protect privacy by prohibiting the interception of wire or oral communications sent by common carriers. S.REP.NO. 541 at 3556.

However, by the early 1970's dramatic technological advances threatened to make the rigid definitional approaches embodied in Title III obsolete. Terri A. Cutrera, The Constitution in Cyberspace: The Fundamental Rights of Computer Users, 60 U.M.K.C. L. REV. 139 (1991). Title III offered little or no protection for the rapidly expanding and increasingly populated realm of "cyberspace," the "network of electron states, magnetic fields, light pulses and thoughts" that connects computers and their users to each other. *Id.* In addition, ad hoc decision making by courts, which drafted bright lines based on technical differences without meaning, left gaps in telecommunications and information jurisprudence. *Id.* at 143. *See, e.g., United States v. Hall*, 488 F.2d 193, 197 (9th Cir. 1973) (acknowledging the literal interpretation of Title III's distinctions between a mobile and a land-line telephone produced an "absurd result").

By the early 1980's, American business leaders were expressing a growing concern that records and confidential information stored and

transmitted by computers were not protected by privacy laws. *See, e.g.*, William J. Broad, Every Computer Whispers its Secrets, N.Y. TIMES, April 5, 1988, at C1; Vin McLellan, CRT Spying: A threat to corporate security? 4 PC WEEK 35 (1987). Businesses and computer buffs began to learn what national security experts and defense contractors had known all along — computers emit radiation at every turn and through the use of a CRT Microspy the radiation can be surreptitiously decoded into readable data. McClellan at 43. Still, the CRT Microspy surveillance threat was believed to be limited. Most experts thought that the technology required to construct a CRT Microspy device was costly and beyond the know how of all but the most powerful governments and multinational corporations. *Id.*

However, in 1983 a Dutch researcher published an article which described how to build a CRT Microspy for a few dollars with material available at the local hardware store. *Id.* In 1986, a Chase Manhattan Bank executive asked an electrical engineering graduate student interning at the bank to build a CRT Microspy. *Id.* With instructions from the Dutch article and about $12 worth of supplies from a nearby Radio Shack, she was able to build a device that could eavesdrop on the bank's computers and divulge their secrets. *Id.* at 44. While it is not clear whether Congress was aware of the specific danger of a CRT Microspy, it was against this backdrop that the ECPA was drafted. As Senator Leahy said, "the existing [communications privacy] law [was] 'hopelessly out of date.' " S. REP. NO. 541 at 3556.

It is clear that the ECPA was enacted in principle part to protect computer privacy. First, the legislative history and committee hearings demonstrate that Congress recognized the tremendous advances in computer technology, both in terms of application of uses and sheer numbers of users. Second, Congress recognized that prior to the enactment of the ECPA the "privacy and security" of computer technology was not protected. S. REP. NO. 541 at 3559. While computer technology was making life "wonderful," many Americans were unaware that the "privacy and security of such communications [was] in tatters . . . . In short, technology and the structure of the communications industry [had] outstripped existing law." 132 CONG. REC. S14449 (daily ed. Oct. 1, 1986) (statement of Sen. Leahy).

Moreover, Congress recognized two fundamental dangers in leaving computer information technology unprotected. First, if computers were not afforded some protection the country faced a gradual erosion of privacy rights, ". . . the loss of the right to whisper and to keep [lives] confidential." Study by the Office of Technology Assessment, Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties and the Administration of Justice of the House Comm. on the Judiciary, 98th Cong., 1st Sess. 41-53 (1985)

(statement of Fred W. Weingarten, Program Manager for the Communications and Informations Technologies Program of the Office of Technology Assessment). Second, consumers would be denied useful applications of evolving technologies and technology related businesses would suffer in the form of reduced sales and development. *Id.*

Were this court to find that it was not Congress' intent to protect computer data from interception by a CRT Microspy, virtually all computer information technology would be unprotected. The result would be a realization of the fears expressed in the committee hearings; namely, the loss of technological benefits and an erosion of that most cherished of rights, the right to privacy. Computer users who now use their computers to store detailed financial information investment plans, personal medical details and even love letters, would do so at the risk of interception and disclosure. Businesses would have to store volumes of confidential documents somewhere other than in an electronic system.

That such a result is contrary to Congress' intent is demonstrated by examining the complete regulatory scheme, *Sutton v. United States*, 819 F. 2d 1289, 1293 (5th Cir. 1987), and an examination of amendments to that scheme. *New Jersey v. Parisi*, 426 A.2d 1081, 1083 (N.J.Super.Ct. Law Div. 1980), overruled on other grounds, 436 A.2d 948 (N.J. Super. Ct. App.Div. 1981). The latter is particularly relevant to this case because the ECPA amended Title III by adding the term "electronic communication" throughout the statute. This amendment broadened the scope of the ECPA to protect data transmissions and VDT terminals. Kastenmeier, Leavy, and Beier, at 727.

For example, in analyzing its own electronic surveillance act the *Parisi* court held that "[w]here a statute alters the previous law, intent may be ascertained from an examination of the old law, the mischief created and the proposed remedy." *Parisi*, 426 A.2d at 1083.

This court should interpret the ECPA to give effect to Congress' intent that CRT Microspy be forbidden rather than reach a result clearly unintended by Congress. *American Trucking Association*, 310 U.S. at 534. In fact, if this court believes it must choose between two interpretations available in this case (that CRT Microspy either is or is not included in the ECPA), this court should err on the side of substance over form. To do otherwise may risk reaching an "absurd" result which is contrary to Congress' intent. *See Winter v. Hollingsworth Properties, Inc.*, 587 F. Supp. 1289, 1294 (S.D. Fla. 1984), overruled on other grounds, 777 F.2d 1444 (11th Cir. 1985). If there is an alternative interpretation consistent with Congress' intent, the court should adopt that interpretation. *American Tobacco Co. v. Patterson*, 456 U.S. 63, 68 (1982). Similarly, the court in this case should adopt the construction

most suited to the apparent intent of Congress to prohibit CRT Microspy.

While it is true that Congress failed to specifically prohibit the use of a CRT Microspy to intercept computer transmissions, that fact alone is not dispositive of Congress' intent. Congress intended that, as a general rule, all communications consisting solely of data are protected. S. REP. NO. 541 at 3568. Also, an intent requirement was added to the statute. *Id.* at 3577. Congress recognized that computers emit electromagnetic radiation. *Id.* at 3579. Testing the levels of computer radiation is a common practice and is not prohibited by the ECPA. *Id.* But, if someone went beyond routine testing and intentionally obtained information during the testing, that person would violate the ECPA. *Id.* While HACKNER was not testing LONGSHORE'S VDT emissions, he was intentionally intercepting information. HACKNER'S conduct is strikingly close to that described in the legislative history.

Should this court find that the conduct described in this portion of the legislative history fails to apply to HACKNER'S conduct, the court should still find that Congress intended to prohibit CRT Microspy. The U.S. Supreme Court has never required that every permissible application of a statute be expressly referred to in its legislative history. *Moskal v. United States*, 498 U.S. 103, 111 (1990). Congress may have been unaware of the capabilities of a CRT Microspy when it enacted the ECPA but unforseen technologies may still be included in a statute by inference if such an interpretation is consistent with Congress' intent.

For example, in *Gilbert* Michigan's high court sought to determine whether a 1929 statute barring citizens from possession of radio equipment tuned to police frequencies could be applied to people who used modern radar detectors to avoid police speed detection. *Michigan v. Gilbert*, 324 N.W.2d 834, 838 (Mich. 1982). The court found that the statute was actually intended to forbid the common 1920's practice of everyday criminals who tuned into police radio broadcasts to get a jump on their adversaries. *Id.* at 839-40. Although the court ultimately held that it could not impute knowledge of radar detectors to the 1929 Michigan Legislature, it did note that unforeseen technologies could be included in a statute by inference if "the new technology facilitates the achievement of an ends which the Legislature clearly meant to encourage or discourage." *Id.*

In this case, it may indeed be argued that Congress was unaware of CRT Microspy when it enacted the ECPA, but it is undeniable that Congress sought in that Act to prohibit the ends to which this technology might be used. The legislative history makes clear that Congress intended to protect information stored, transferred and processed by computers from surreptitious interception. Moreover, the rapidly

changing nature of electronic communications poses unique difficulties to a legislature. As Rep. Kastenmeier stated:

> The first principle is that legislation which protects electronic communications from interceptions . . . should be comprehensive, and should not be limited to particular types or techniques of communicating . . . . Any attempt to write a law which tries to protect only those technologies which exist in the marketplace today . . . is destined to be outmoded within a few years . . . . The second principle . . . is a recognition that what is being protected is the sanctity and privacy of the communication. We should not . . . discriminate for or against certain methods of communication . . . .

132 CONG. REC. H4046 (daily ed. June 23, 1986) (statement of Rep. Kastenmeier).

Clearly, Congress meant to protect the privacy of computer users from existing and developing technologies. The CRT Microspy was exactly the type of technology Congress envisioned when it drafted such a broad law. To require Congress to have specifically mentioned all future technologies when it drafted the ECPA would be like asking Congress to "write with ink on flowing water." Weingarten, at 44.

The ECPA was intended by Congress as a broad prohibition on the type of technology represented by CRT Microspy. This court should honor the plain meaning of the ECPA and Congress' intent and hold that HACKNER'S conduct violated the ECPA.

II. LONGSHORE'S INTRUSION UPON SECLUSION CLAIM SHOULD SURVIVE HACKNER'S MOTION TO DISMISS BECAUSE A PHYSICAL INVASION OR TECHNICAL TRESPASS IS NOT REQUIRED FOR A CLAIM OF INTRUSION UPON SECLUSION.

The Supreme Court of Marshall has recognized the common law tort of an intrusion upon seclusion as stated in the Restatement (Second) of Torts § 652B (1977). (R. 7) (citing *Barstel v. Frepton*, 987 M.2d 345, 348 (Marshall 1980)). The tort of intrusion upon seclusion is defined as "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." Restatement (Second) of Torts § 652B (1977). Whether a physical invasion is required for a valid claim for intrusion upon seclusion to be stated is a question of first impression in the State of Marshall. (R. 7). For two reasons, this court should conclude that a physical invasion is not necessary to establish that LONGSHORE has alleged facts sufficient to state a claim for intrusion upon seclusion. First, language in the Restatement (Second) of Torts § 652B which states that an intrusion may occur

"physically or otherwise" does not require an actual physical invasion for a claim of intrusion upon seclusion. Second, an action for intrusion upon seclusion should not require a physical invasion because the tort should protect the interest in privacy rather than the place invaded.

A. The Restatement of Torts § 652B does not require that Hackner actually physically invade Longshore's business premises before a cause of action for intrusion upon seclusion is stated.

The language of the Restatement (Second) of Torts § 652B explicitly states that an intrusion upon seclusion may occur either "physically or otherwise." Restatement (Second) of Torts § 652B (1977). In considering what is required for a valid cause of action for intrusion upon seclusion to be stated under the Restatement (Second) of Torts § 652B, the Ninth Circuit Court of Appeals has stated that "[d]espite some variations in the description and the labels applied to the tort [of intrusion upon seclusion], there is agreement that. . .the existence of a technical trespass is immaterial . . . ." *Dietemann v. Time, Inc.*, 449 F.2d 245, 247 (9th Cir. 1971). The District of Columbia Circuit Court of Appeals has concluded that the tort of intrusion upon seclusion should extend to instances of intrusion, "whether by physical trespass or not," where an ordinary person in the plaintiff's position could reasonably expect that the particular defendant should be excluded. *Pearson v. Dodd*, 410 F.2d. 701, 704 (D.C. Cir. 1969). Furthermore, a substantial majority of the states that have been faced with the question of whether an actual physical invasion is required for an intrusion upon seclusion have concluded that it is not. *See e.g., Phillips v. Smalley Maintenance Serv., Inc.*, 435 So. 2d 705, 711 (Ala. 1983); *Miller v. National Broadcasting Co.*, 232 Cal. Rptr. 668, 679 (Cal. Ct. App. 1986) (citing *Dietemann v. Time, Inc.*, 449 F.2d 245, 247 (9th Cir. 1971); *Lewis v. Dayton Hudson Corp.*, 339 N.W.2d 857, 858 (Mich. Ct. App. 1983); *Hamberger v. Eastman*, 206 A.2d 239, 241 (N.H. 1964); *N.O.C., Inc. v. Schaefer*, 484 A.2d 729, 732 (N.J. Super. Ct. Law Div. 1984); *Nader v. General Motors Corp.*, 255 N.E.2d 765, 770 (N.Y. 1970).

For example, the Supreme Court of Kansas has concluded that the "physically or otherwise" provision of the Restatement (Second) of Torts § 652B requires only that there be something in the nature of an intentional interference with the plaintiff's private affairs that is highly offensive to the reasonable person. *Werner v. Kniewer*, 710 P.2d 1250, 1255 (Kan. 1985). In concluding that a physical invasion is not required for the statement of an intrusion upon seclusion claim, the *Werner* court recognized comment B to Restatement (Second) of Torts § 652B which states that a claim for intrusion upon seclusion may be either a physical invasion or an intrusion where a person uses his senses, "with or without mechanical aids, to oversee or overhear the plaintiff's private

affairs." *Werner*, 710 P.2d at 1255 (citing Restatement (Second) of Torts § 652B cmt. b (1977)). Thus, the "physically or otherwise" language in the Restatement (Second) of Torts § 652B provides that a physical invasion upon private premises is not required for a claim of intrusion upon seclusion.

B. A physical invasion or a technical trespass should not be required for a valid claim for intrusion upon seclusion to be stated since, as Fourth Amendment jurisprudence demonstrates, it is the interest in privacy that is protected, not the place.

In the past 100 years, the United States Supreme Court has come full circle in deciding that a physical invasion is not required to invoke the Fourth Amendment privacy shield. The Court first addressed the issue in *Boyd v. United States*, 116 U.S. 616 (1886), a case involving an order compelling the production of an invoice to be used to establish criminal liability. *Id.* at 619. The Court held the order unconstitutional as in violation of the Fourth and Fifth Amendments, noting that an invasion of "personal security" occurred despite the lack of a physical intrusion. *Id.* at 630. The *Boyd* Court recognized, as this court should, that "[i]t is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence." *Id.* This court should extend the reasoning of *Boyd* and other United States Supreme Court's Fourth Amendment decisions and hold that LONGSHORE'S tort claim for inclusion upon seclusion does not require a physical invasion.

In *Boyd*, the Court ruled that an order to produce certain incriminating invoices violated the Fourth Amendment even though no physical invasion accompanied the compulsion. *Id.* For the Court in *Boyd*, the traditional images of random physical police searches were simply aggravations of the real constitutional violation — the intrusion on personal security by the state. *Id.* This court, like the Court in *Boyd*, should recognize that there is no distinction between a physical intrusion and a non-physical one. How the intrusion happens is simply not relevant to the initial question of whether it happened at all.

Thirty-two years ago, Justice Douglas foreshadowed the misunderstanding of the courts below in this case when he noted that the means of invading privacy is not particularly relevant to determining that an invasion has taken place. *Silverman v. United States*, 365 U.S. 505 (1961) (Douglas, J., concurring). The problem with the physical intrusion distinction, Justice Douglas wrote, is that "it leads us to a matching of cases on irrelevant facts. An electronic device on the outside wall of a house is a permissible invasion of privacy . . . while an electronic device that penetrates a wall . . . is not." *Id.* at 512.

Justice Douglas argued that the invasion of privacy is the same in both cases and does not turn on whether or to what extent a physical invasion occurred. "The depth of the penetration of the electronic device — even the degree of its remoteness from the inside of the house — is not the measure of the injury." *Id.* at 513. In this case, HACKNER'S invasion of LONGSHORE'S privacy is not to be found in the mechanism HACKNER used. The intrusion upon LONGSHORE'S seclusion happened, not through the use of the CRT Microspy, but as a result of that use.

Thirty years before Justice Douglas' observation of the meaningless nature of the physical invasion distinction, a majority of the Court turned away from its decision in *Boyd* and took the position that a physical invasion would be required to invoke Fourth Amendment protections. *Olmstead v. United States*, 277 U.S. 438 (1928).

In *Olmstead*, the Court upheld the convictions of several defendants for violations of the Prohibition Act (27 USCA). *Id.* Evidence in the case included the substance of conversations officials overheard by tapping the defendants' telephone lines. *Id.* at 456. The Court ruled that the lack of a physical invasion of a constitutionally protected area took the seizure of this evidence out of the confines of the Fourth Amendment. *Id.* at 466.

Criticism of the *Olmstead* decision was fierce. Justice Brennan, speaking to the heart of the issue before this court, wrote that the decision in *Olmstead* would render the Constitution "an utterly impractical instrument . . . if it were deemed to reach only problems familiar to the technology of the eighteenth century. . . ." *Lopez v. United States*, 373 U.S. 427, 459 (1963) (Brennan, J., dissenting). Congress reacted to the *Olmstead* decision by amending the Federal Communications Act, making wiretapping a federal crime. *Id.* at 462.

Ultimately, in *Katz v. United States*, 389 U.S. 347 (1967), the Court overruled its holding in *Olmstead* and returned to the notion that a physical invasion is not required to violate the Fourth Amendment. In *Katz*, the Court declared the law enforcement use of a surveillance device attached to the outside of a telephone booth for listening to the conversations of the defendant inside as unconstitutional. *Id.* at 348. "[O]nce it is recognized that the Fourth Amendment protects people — and not simply 'areas' — against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn on the presence or absence of a physical intrusion . . ." *Id.* at 353.

The reasonable expectation of privacy in a variety of places, and in different contexts, is the linchpin between Fourth Amendment privacy jurisprudence and the common law intrusion upon seclusion claim. *Pearson v. Dodd*, 410 F.2d 701 (D.C. Cir. 1969), cert. denied, 395 U.S. 947

(1969). Citing the United States Supreme Court decision in *Katz*, the *Pearson* court adopted the view that a physical intrusion is not necessary for the invasion of privacy tort. *Id.* at 704. "The protection should not turn exclusively on the question of whether the intrusion involves a technical trespass under the law of property. The common law, like the Fourth Amendment, should 'protect people, not places.' " *Id.*

Other jurisdictions have followed the same principle LONGSHORE urges today — because privacy is extended to people rather than areas, the presence or absence of a physical intrusion is immaterial to the determination that a tortious invasion of that privacy took place. *Evans v. Detlefsen*, 857 F.2d 330 (6th Cir. 1988). In *Evans*, the Sixth Circuit Court of Appeals addressed whether an area must be physically invaded before a valid cause of action for intrusion upon seclusion was stated. *Id.*

In *Evans*, the defendant, a police officer, allegedly bullied and abused the plaintiff in a restaurant. *Id.* at 331-2. The lower court allowed the plaintiff's claim for intrusion upon seclusion to proceed, and the jury found the defendant liable for damages for wrongful intrusion upon seclusion as defined in the Restatement (Second) of Torts § 652B (1977). *Id.* at 337. The defendant's motions for a directed verdict and a judgment notwithstanding the verdict claiming that a physical invasion upon private premises was required were denied by the lower court. *Id.* The denials of the defendant's post-trial motions were the basis of the defendant's appeal on the intrusion upon seclusion issue. *Id.*

The *Evans* court stated that "the short answer to the defendant's argument is that the privacy which is invaded concerns the type of interest involved and not the place where the invasion occurs." *Id.* The court reasoned further that the place of occurrence, while relevant to a determination of the degree of intrusiveness, is certainly not determinative. *Id.* In the instant case, LONGSHORE's interest in keeping his mailing list confidential is unquestionably significant. In fact, HACKNER'S subsequent use of LONGSHORE's mailing list to target LONGSHORE's customers caused LONGSHORE's business to decline significantly. (R. 4). Thus, under the jurisprudence of the Fourth Amendment and the reasoning in *Pearson* and *Evans*, LONGSHORE has alleged an intrusion upon interests that deserve protection under the tort of intrusion upon seclusion.

C. The tort of intrusion upon seclusion was committed by HACKNER because his interception of LONGSHORE'S mailing list data was unreasonably intrusive and highly offensive to a reasonable person.

A plaintiff's privacy is invaded only if the intrusion involved infor-

mation that is of a confidential nature and the defendant's conduct is unreasonably intrusive. *Nader v. General Motors Corp.*, 255 N.E.2d 765, 770 (N.Y. 1970). The defendant in *Nader* attempted to discredit the plaintiff by learning any information that might disparage him in the public eye. In his search for such information, the defendant eavesdropped on the plaintiff's private conversations through the use of electronic equipment and questioned the plaintiff's acquaintances concerning the plaintiff's character. *Id.* The Court of Appeals of New York, in applying the law of the District of Columbia, addressed whether these facts were sufficient to state a cause of action for intrusion upon seclusion as defined in RESTATEMENT (Second) of Torts § 652B (1977). *Id.* at 767.

The *Nader* court did not consider whether a physical boundary was actually crossed in determining whether a valid claim for intrusion upon seclusion had been stated. *Id.* at 767. Instead, the court reasoned that the interest protected is the right of the plaintiff to exclude others from the information, not the rights inherent in the owning of a building. *Id.* at 768 (citing *Pearson v. Dodd*, 410 F.2d. 701, 704 (D.C. Cir. 1969), *cert. denied*, 395 U.S. 947 (1969)). Recognizing that the tort of intrusion upon seclusion was not evident in every situation where an individual is annoyed, the *Nader* court concluded that a plaintiff's privacy is only invaded if the intrusion involved information that is "of a confidential nature and the defendant's conduct is unreasonably intrusive." *Id.* The court concluded that a defendant's conduct is unreasonably intrusive if the plaintiff could reasonably expect the information to remain confidential. *Id.* at 770.

As to the defendant's questioning of the plaintiff's acquaintances, the *Nader* court reasoned that the plaintiff could not have a reasonable expectation that information known by friends would remain confidential. *Id.* The court reiterated its contention that an intrusion upon seclusion is not present merely because someone was annoyed. Thus, the court concluded that the defendant's questioning of the acquaintances of the plaintiff was not sufficient to state a claim of intrusion upon seclusion. *Id.*

However, the *Nader* court found that the defendant's eavesdropping upon the plaintiff's communications by electronic means did present a sufficient basis for an intrusion upon seclusion action because a reasonable person would not expect his private communications to be electronically overheard. *Id.* Thus, under the authority of *Nader*, a valid claim for intrusion upon seclusion is stated if a plaintiff alleges that the defendant obtained confidential information from the plaintiff through means that a reasonable person would consider unreasonably intrusive. *Id.*

In the instant case, LONGSHORE's mailing list is certainly of a

confidential nature since it is the backbone of LONGSHORE's mail-order business. Applying the reasoning of *Nader*, the essential question is whether LONGSHORE had a reasonable expectation that his mailing list would remain confidential. The instant case is closely related to and may be stronger than the facts of *Nader* where the plaintiff's conversations were overheard by electronic means. The plaintiff in *Nader* told a third party something in confidence that was overheard electronically. *Id.* Since the plaintiff in *Nader*, communicated with a third party, it is possible to argue that he should have realized that someone could overhear the communication. In the instant case, LONGSHORE did not expose the contents of his mailing list to a third party. Thus, LONGSHORE has an even stronger privacy expectation than the plaintiff in *Nader*. Surely, a reasonable person would not expect that the impulses of light from his video display terminal could go through solid walls and be intercepted by competitors seeking an unfair advantage. Under the reasoning of *Nader*, LONGSHORE's allegation that HACKNER used a CRT Microspy to obtain LONGSHORE's mailing list is certainly sufficient to state a claim for intrusion upon seclusion.

Virtually all business functions in corporate America are performed with the assistance of computers and video display terminals such as those used by LONGSHORE. From a practical standpoint, it would be impossible for most businesses to function if information that was displayed on their video display terminals could be reproduced by their competitors without fear of penalty. The common law should not allow reasonable privacy interests to cease to exist due to improvements in technology. As the California legislature stated when dealing with the question of how far protections of privacy should go:

> [A]dvances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Miller v. National Broadcasting Co., 232 Cal. Rptr. 668, 679 (Cal. Ct. App. 1986) (citing § 630 of the California Penal Code).

Without question, HACKNER's use of a CRT Microspy is an unreasonably intrusive action. Furthermore, a physical invasion or technical trespass is not required for a valid intrusion upon seclusion claim. Therefore, this Court should reverse the lower court and allow LONGSHORE's complaint to proceed.

CONCLUSION

Because the Petitioner's complaint and the undisputed facts in this case clearly establish a violation by the Respondent of the Electronic

Communications Privacy Act of 1986, and because the Respondent's actions represent an intrusion upon the Petitioner's seclusion, the Petitioner respectfully requests that this court REVERSE the decision of the Marshall Appellate Court for the First Judicial District as to both counts, and instruct the lower courts to permit this action to proceed.

Respectfully submitted,

Counsel for Petitioner

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing was furnished to all counsel of record, by U.S. mail, this twenty-third day of September, 1993.

Counsel for Petitioner

APPENDIX A

U.S. CONST. amend. IV. provides:

> " The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, shall not be violated . . ."

APPENDIX B

Relevant provisions of 18 U.S.C. are:

§ 2510(4)-

" 'intercept' means the aural or other acquisition of the contents of any . . . electronic . . . communication through the use of any electronic, mechanical or other device."

§ 2510(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 . . ."

§ 2510(14)-

" 'electronic communications system' means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications . . ."

§ 2510(16)-

" 'readily accessible to the general public' means, with respect to a radio communication . . . [such communication that is]. . . not . . . scrambled or encrypted."

§ 2511(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, any wire, oral or electronic communication [violates this Act] . . ."

§ 2511(2)(g)-

"It shall not be unlawful under this chapter . . . (i) to intercept or access an electronic communication made through an electronic communications system that is configured so that such electronic communication is readily accessible to the general public . . ."

APPENDIX C

Restatement (Second) of Torts § 652B, provides:

> "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."

No. 93-8488

IN THE SUPREME COURT
OF THE
STATE OF MARSHALL

Richard LONGSHORE, d.b.a.
LONGSHORE COSMETICS,

Petitioner,

vs.

Harry Hackner, d.b.a.
H&C BEAUTY SUPPLIES,

Respondent.

On Writ of Certiorari to
the Marshall Appellate Court
for the First Judicial District

BRIEF FOR THE RESPONDENT

Wake Forest University School of Law
Spiro P. Fotopoulos
Joseph E. Helweg
Alyce E. Hill

QUESTIONS PRESENTED

I. WHETHER ELECTROMAGNETIC RADIATION EMANATING FROM A COMPUTER MONITOR DISPLAYING A CUSTOMER LIST CONSTITUTES AN "ELECTRONIC COMMUNICATION" WITHIN THE *ECPA*?

II. WHETHER FACTS ESTABLISHING RESPONDENT'S RECEPTION OF IMAGES EMANATING FROM PETITIONER'S COMPUTER MONITOR ARE SUFFICIENT TO STATE A CLAIM FOR INTRUSION UPON SECLUSION?

TABLE OF CONTENTS

TABLE OF AUTHORITIES
FEDERAL CASES

STATE CASES

FEDERAL STATUTES

FEDERAL REGULATIONS

LEGISLATIVE MATERIALS

MISCELLANEOUS

OPINIONS BELOW

The opinion for the Marshall Appellate Court for the First Judicial District, No. 93-98323, is not officially reported but is contained in the record. (R. 1-8.)

STATUTORY PROVISIONS

The appendix sets forth the following statutory provisions relevant to this brief: 18 U.S.C. §§ 2510, 2511 (1988).

STATEMENT OF THE CASE

A. *Statement of the Proceedings*

On April 6, 1992, Petitioner filed an action in the Newport County Circuit Court against Respondent for (1) violation of 18 U.S.C. § 2511(1)(a) of The Electronic Communications Privacy Act (hereinafter *ECPA*) and, (2) in the alternative, the common law tort of invasion of privacy by intrusion upon seclusion. (R. 5.) On April 21, 1992, Respondent filed a motion to dismiss both counts for failure to state a cause of action. (R. 5.) On May 1, 1992, the Newport County Circuit Court granted Respondent's motion to dismiss for failure to state a cause of action on both counts of the complaint. (R. 6.)

Petitioner appealed the decision of the Circuit Court to the Marshall Appellate Court for the First Judicial District. (R. 6.) The Marshall Appellate Court affirmed the order granting Respondent's motion to dismiss both counts for failure to state a cause of action. (R. 7-8.) Petitioner appealed the order granting Respondent's motion to dismiss the complaint to the Supreme Court of the State of Marshall. On July 19, 1993, the Supreme Court of the State of Marshall granted certiorari.

B. *Statement of the Facts*

Petitioner is a resident of the State of Marshall and is the sole proprietor of "Longshore Cosmetics," a mail order cosmetic company located in Newport. (R. 2.) Petitioner uses a desk-top computer equipped with a standard video display terminal ("VDT") for accounting, correspondence, e-mail, billing, inventory, and printing mailing labels. (R. 2.)

Respondent is also a resident of the State of Marshall and is the owner of "H&C Beauty Supplies," a mail order cosmetics company located across the street from Petitioner. (R at 2.) Respondent is quite knowledgeable and proficient in using computers and reads articles which discuss the latest technologic advances in the computer industry. (R. 2.) As a result, Respondent learned about the "CRT Microspy." (R. 2.)

The CRT Microspy is a device designed to receive the electromag-

netic radiation that emanates from a computer VDT and then reproduces the VDT image on a remote television screen. (R. 3.) Because the emanations from a VDT resemble television broadcast signals, a black and white television is all that is needed to receive VDT electromagnetic emanations. (R. 3.) However, the frequencies of a VDT frequently do not match the frequencies of a television set. (R. 3.) Thus, in the event that the frequencies do not match, a device can be assembled to reproduce the VDT frequencies. (R. 3.) Such a device generates signals similar to those of the targeted VDT and sends them into the television receiver's synchronization separator. (R. 3.) This process allows the reproduction of the VDT image on the television screen. (R. 3.)

On November 19, 1991, Respondent built his own VDT electromagnetic monitoring device in order to receive the electromagnetic emanations from the computer VDT in Petitioner's office. (R. 4.) From November 30, 1991 until December 22, 1991, Respondent received the electromagnetic emanations from Petitioner's computer VDT which caused the data appearing on Petitioner's computer VDT to be reproduced on Respondent's VDT. (R. 4.) The data that appeared over this period of time formed Petitioner's client list. (R. 4.) Respondent's receipt of the information involved no physical entry onto Petitioner's premises at any time. (R. 4.) Instead, the emanations came to Respondent at his office. (R. 4).

In January, 1992, the information generated by the emanations enabled Respondent to offer his products to Petitioner's clients. (R. 4.) Some of these clients began using Respondent's products. (R. 4.) In March, 1992, one of Respondent's employees learned of Respondent's reception of the emanations and told Petitioner what had occurred. (R. 4-5.) On April 6, 1992, Petitioner filed a two count complaint against Respondent, alleging (1) Respondent's conduct violated the Electronic Communications Privacy Act and (2) Respondent's use of the CRT Microspy was an invasion of privacy as an intrusion upon seclusion. (R. 5.)

SUMMARY OF THE ARGUMENT

I.

The Electronic Communications Privacy Act (hereinafter *ECPA*) prohibits the interception of an "electronic communication." Respondent's reception of Petitioner's emanations did not violate the *ECPA* because the emanations are not an "electronic communication" as defined by the *ECPA*. The plain language of the definition of "electronic communication" requires a transfer of information to an intended recipient. Because Petitioner's emanations were merely a reaction to the display

of data on a computer monitor, no such transfer occurred. This interpretation is supported by the legislative history of the *ECPA*, which indicates Congress enacted the *ECPA* to protect new methods of making the same types of communications covered by the existing law.

Moreover, court decisions considering the applicability of the *ECPA* to closely analogous situations show the *ECPA* does not apply to emanations from a computer monitor. Finally, because including Petitioner's emanations in the definition of "electronic communication" would result in an unenforceable law that could create a false sense of security among computer users, such an interpretation would be contrary to public policy. Therefore, the Marshall Appellate Court properly affirmed the dismissal of Petitioner's *ECPA* claim.

II.

The facts established in this case are insufficient to state a claim for intrusion upon seclusion for three reasons. First, the customer list databank on Petitioner's VDT did not constitute an area of seclusion for Petitioner. The right of privacy underlying the tort for intrusion is intended to protect information relating to one's intimate personality or emotional sanctum. The list of Longshore Cosmetics' customers' names and addresses, however, was of no relevance to Petitioner's intimate personality or emotions. While this information might have been the source of a privacy or seclusion interest for the customers themselves, it did not constitute an area of seclusion for Petitioner.

Second, Respondent's use of a CRT Microspy to receive images freely emanating from Petitioner's VDT did not constitute an intrusion. Instead of prying into the sights or sounds of Petitioner's private world, the CRT Microspy picked up signals that Petitioner was freely projecting and which reached Respondent as he sat in his own office. By merely viewing images freely emanating to Respondent's office, Respondent's conduct did not constitute an intrusion.

Finally, even if one were to classify Respondent's conduct as an intrusion, it did not rise to the level of being "highly offensive," and thus was not actionable under Marshall law. Considering that Respondent's sole interest was to compete with Longshore Cosmetics on an equal footing, Respondent's unobtrusive actions were reasonable. Moreover, since the images freely emanating from Petitioner's VDT could have been received by many other people in the area, Respondent's completely unobtrusive reception of this information cannot, as a matter of law, amount to a "highly offensive" intrusion.

ARGUMENT

I. THE MARSHALL APPELLATE COURT PROPERLY AFFIRMED THE DISMISSAL OF PETITIONER'S *ECPA* CLAIM BECAUSE ELECTROMAGNETIC RADIATION EMANATING FROM A COMPUTER MONITOR DISPLAYING A CUSTOMER LIST DOES NOT CONSTITUTE AN "ELECTRONIC COMMUNICATION."

A. *The plain language of the ECPA definition of "electronic communication" does not include electromagnetic emanations from a computer monitor displaying a customer list.*

The Electronic Communications Privacy Act, 18 U.S.C. § 2510 (1988)(hereinafter *ECPA*), provides both civil and criminal remedies for the intentional interception of any wire, oral, or electronic communication. Petitioner alleges that the emanations generated by the display of data on Petitioner's computer monitor are an "electronic communication" covered by the *ECPA* so that Respondent's reception of the emanations violates the *ECPA*. Because Petitioner's emanations do not fit the *ECPA* definition of an "electronic communication," the Marshall Appellate Court properly affirmed the dismissal of Petitioner's claim.

1. "Electronic communication" does not include the Petitioner's emanations because no "transfer" took place as required by the definition.

The *ECPA* defines an "electronic communication" as "any *transfer* of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system." 18 U.S.C. § 2510(12)(emphasis added). This definition clearly requires a "transfer" of signals. Because the electromagnetic emanations from Petitioner's computer monitor were not "transfers" of data, the emanations were not an "electronic communication" as defined by the *ECPA*.

"Transfer" means "convey or remove from one place, person, etc., *to another, i.e.* he transferred the package from one hand to the other." Black's Law Dictionary 1497 (6th ed. 1990)(emphasis added). Implicit in this definition is the idea that material being conveyed is to be received by another intended party.

In this case, the electromagnetic emanations were emitted as a result of the energy generated by the mere display of Petitioner's customer list on his computer monitor. (R. 3.) The emanations were an inevitable by-product of this display that drifted into every direction until they dissipated. They were not emitted as material to be conveyed by the Petitioner to another party. Since there was no intended recipi-

ent for the emanations, no "transfer" of the material making up the emanations took place. Because the emanations were not part of a "transfer," nor did they result from a "transfer" of information, they did not constitute an "electronic communication."

The requirement of a "transfer" does not exclude all electromagnetic emanations from the coverage of the *ECPA*. Some emanations are purposely transmitted so that an intended person will receive them. Christopher J. Seline, Note, *Eavesdropping on the Compromising Emanations of Electronic Equipment: The Laws of England and the United States*, 23 Case W. Res. J. Int'l L. 359, 364 (1991). Because such emanations are purposely sent into the atmosphere to an intended recipient, a "transfer" has occurred and the emanations would be covered by the *ECPA*. Here, if Petitioner had generated the emanations with the intent that another nearby party receive them in order to share in the information the emanations could provide, a third party would be prohibited from intercepting the emanations.

On the other hand, emanations that were never intended to be transmitted to a particular recipient but were merely incidental to the electronic activity taking place would not be covered by the *ECPA* because there is no "transfer" constituting an "electronic communication." Seline, *supra*, at 364. Here, because the emanations were not emitted for the purpose of providing another party with data but were merely incidental to Petitioner's work, the emanations are not covered by the *ECPA*.

2. The plain language of the *ECPA*'s other provisions requires that in order to be covered by the statute, a communication must be sent to an intended recipient.

The *ECPA* prohibits divulging the contents of an electronic communication except under certain circumstances. 18 U.S.C. § 2511(3) (1988). The statute states that a party providing electronic communication service shall not intentionally divulge the contents of a communication while in transmission "to any person or entity other than an addressee or the *intended recipient* of such communication." 18 U.S.C. § 2511(3)(a) (1988)(emphasis added). One circumstance when this prohibition does not apply is when lawful consent is given by "the originator or any addressee or *intended recipient* of such a communication." 18 U.S.C. § 2511(3)(b)(ii) (1988)(emphasis added). Another circumstance is when a party is authorized to "forward such a communication *to its destination*." 18 U.S.C. § 2511(3)(b)(iii) (1988)(emphasis added). The language in these provisions clearly indicates that a communication covered by the *ECPA* must be transmitted from a sender to an intended recipient.

Furthermore, interception of an electronic communication is not prohibited where "*one of the parties* to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(c) (1988)(emphasis added). This language implies that communications covered by the *ECPA* occur between two or more parties. All of these provisions make it clear that an "electronic communication" involves information transferred from the sender to an intended recipient. Because Petitioner's emanations were not transfers of information to an intended recipient, the emanations were not covered by the *ECPA*.

3. Because the purpose of the *ECPA* is to prohibit interception of communications and because electromagnetic emanations are not capable of interception, Petitioner's emanations are not covered by the *ECPA*.

The *ECPA* sets forth penalties for anyone who "intercepts" an "electronic communication." 18 U.S.C. § 2511(4)(a) (1988). "Intercept" means the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (1988). To "acquire" generally means to come into ownership or possession of something. The flow of the emanations into the Respondent's antenna range while they "drifted out" in all directions from Petitioner's computer monitor cannot constitute an "interception." While the emanations could create an image on Respondent's television screen, they are not capable of being held in Respondent's possession. The emanations will continue to flow in all directions beyond Respondent's range until their energy has dissipated into the air.

Additionally, while 18 U.S.C. § 2511(1)(a) states that it is unlawful to intercept an electronic communication, 18 U.S.C. § 2511(g)(i) states that it shall not be unlawful to intercept or access certain communications. 18 U.S.C. § 2511(g)(i) (1988). The addition of the word "access" in § 2511(g)(i) shows that the drafters considered interception to be something different than access, which is simply making contact with a signal. Therefore, because Respondent merely accessed the signal rather than intercepting it, his actions would not be prohibited by the *ECPA*. Because the emanations are only capable of access and are not capable of the interception prohibited by the *ECPA*, the emanations are not covered by the plain language of the *ECPA*.

Moreover, even if the plain language of the *ECPA* was ambiguous so that it might be construed to cover the emanations, because the *ECPA* is a criminal statute, it must be narrowly construed and any ambiguity resolved in favor of leniency. *United States v. Enmons*, 410 U.S. 396, 411 (1973); *see also State v. Howard*, 679 P.2d 197, 205 (Kan.

1984)(stating that the *ECPA* is a penal statute requiring strict construction); *United States v. Herring*, 933 F.2d 932 (11th Cir. 1991), *vacated*, 977 F.2d 1435 (1992), *rev'd on other grounds*, 993 F.2d 784 (1993), *cert. denied*, 114 S. Ct. 347 (1993)(stating that the doctrine of leniency applies to the *ECPA*). Therefore, the trial court properly dismissed the Petitioner's claim, and the Marshall Appellate Court properly affirmed the dismissal.

B. *The legislative history of the ECPA shows that Congress did not intend that the ECPA cover electromagnetic radiation emanating from a computer monitor displaying a customer list.*

The *ECPA* amended Title III of the existing Omnibus Crime Control and Safe Street Act by adding, among other things, the word "electronic" to describe the methods of communication protected by the statute. 18 U.S.C. § 2511 (1988). The legislative history of the *ECPA* demonstrates that while Congress expanded the coverage of the original statute to include more methods of communication evolving from advancing technology, it did not change the original purpose of the statute. *Manufacturers Int'l, LTDA v. Manufacturers Hanover Trust Co.*, 792 F. Supp. 180, 191 (E.D.N.Y. 1992); Seline, *supra*, at 375. Thus, the *ECPA* was intended to protect new methods of making the same type of communications already protected under existing law. S. Rep. No. 541, 99th Cong., 2d Sess. (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

Title III of the original statute was enacted in 1968 as a reaction to public concern over wiretapping and a concomitant need for government investigative agencies to intercept communications. Fred W. Weingarten, *Communications Technology: New Challenges to Privacy*, 21 J. Marshall L. Rev. 735, 743 (1988). Title III was intended to protect the privacy of wire and oral communications from unauthorized surveillance and delineate when interception of those communications may be authorized. Seline, *supra*, at 371-2. The primary methods of communication at that time were telephone calls and face-to-face conversations between parties. Richard C. Turkington et al., *Privacy: Cases and Materials* 168 (1992).

Because the *ECPA* was only intended to recognize new methods of making the same type of communications already protected by existing law, such as telephone calls and face-to-face conversations, interpreting the *ECPA* to cover any conduct that is not similar to these communications would be contrary to the legislative intent. Petitioner's emanations, which were only a reaction to information displayed on a computer monitor, were unlike communications protected by existing

law. Therefore, Congress did not intend that they be covered by the *ECPA*.

The report of the Senate Judiciary Committee states that the purpose of the *ECPA* is to prohibit unauthorized interception of electronic communications and clarify the law in light of changes in computer and telecommunications technology. S. Rep. No. 541. The report listed examples of the new types of technology and methods of communication Congress intended to cover. This list includes electronic mail, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing. S. Rep. 541. All of these examples of communications to be covered by the *ECPA* involve a transfer of information from one party to an intended recipient. They are all interactive in nature.

Additionally, the report states that Congress intended to give these new methods of communication protection comparable to that given to a first class letter or a telephone call via a common carrier because these new methods of communication were coming to be used in lieu of or side by side with letters and telephone calls. S. Rep. No. 541. Letters and common carrier telephone calls, like the new methods of communication listed in the report, involve a transfer of information from one party to an intended recipient and are also interactive in nature. Because the report shows a clear intent to cover the methods of communication used in place of mail or telephone calls via a common carrier, only those situations involving the similar transfers of information should be covered by the *ECPA*. Petitioner's emanations do not involve such transfers of information but instead are a reaction to the display of information on Petitioner's computer monitor. Therefore, Congress did not intend to cover Petitioner's emanations in the *ECPA*.

Although Congress broadly stated that it intended to cover those communications not carried by sound waves or characterized as containing the human voice, S. Rep. No. 541, its statement demonstrates that a communication in the nature of those covered by existing law is still required to trigger the statute. The *ECPA* only broadened the existing statute to include new methods of making these same types of communications. The Petitioner's emanations are unlike these communications. Rather than a transfer of information to an intended recipient, they are a reaction to the energy necessarily generated by the display of Petitioner's customer list on his computer monitor. Therefore, including the emanations in the definition of an "electronic communication" would be contrary to legislative intent.

Decisions of courts examining the legislative history of the *ECPA* are consistent with the view that electromagnetic emanations were not intended to be covered by the *ECPA*. In *Manufacturers International*, the court found that the 1986 amendments did not change the nature of

the coverage provided by the statute. 792 F. Supp. at 191. The amendments substituted "intentionally" for "willfully" and added "electronic" to the types of communications covered. *Herring*, 933 F.2d at 934. The legislative history also indicates that Congress intended to protect "personal and business 'point-to-point' communications." *Id.* at 935. The amendments were not intended to change the basic purpose of the statute which was to prohibit the unauthorized interception of communications similar to those protected by existing law.

The emanations here are distinguishable from all of the examples of communications Congress intended to cover because there is no point-to-point transfer of information from a sender to an intended recipient. Furthermore, the basic nature of communications the Congress intended to cover has not changed with the enactment of the *ECPA*. Hence, including the Petitioner's electromagnetic emanations in the coverage of the *ECPA* would be contrary to legislative intent. Therefore, Petitioner's claim was properly dismissed.

C. *Court decisions considering whether analogous signals constitute an "electronic communication" indicate that Petitioner's emanations are not covered by the ECPA.*

No court has yet considered whether electromagnetic emanations like the Petitioner's constitute an "electronic communication" covered by the *ECPA*. However, decisions determining whether analogous signals are "electronic communications" buttress the conclusion that Petitioner's electromagnetic emanations are not within the *ECPA*'s definition of an "electronic communication."

1. Because the emanations in this case are similar to the signal between the base and handset of a cordless telephone, which is not covered by the *ECPA*, the emanations were not intended to be covered by the *ECPA*.

Electromagnetic emanations from a computer monitor are analogous to the radiation flowing between the base and handset of a cordless telephone. Terri A. Cutrera, Note, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60 U.M.K.C. L. Rev. 139, 163 (1991). The radio signal flowing between the base and handset of a cordless telephone is not covered by the *ECPA*. 18 U.S.C. § 2510(12)(A) (1988). One reason for this exclusion is that the signal between the base and handset of a cordless telephone, unlike the signals between cellular telephones and other instruments covered by the *ECPA*, is not capable of being transmitted in a particular direction. *United States v. Carr*, 805 F. Supp. 1266, 1270 (E.D.N.C. 1992). Additionally, Congress was unwilling to cover that which is easily intercepted such as the signal between

the base and handset of a cordless telephone. Timothy R. Rabel, Comment, *The Electronic Communications and Privacy Act: Discriminatory Treatment for Similar Technology, Cutting the Cord of Privacy*, 23 J. Marshall L. Rev. 661, 673-4 (1990).

In *United States v. Carr*, the defendant tried to suppress the contents of a conversation intercepted from a cordless telephone call. *Carr*, 805 F. Supp. at 1266. The court found that interception of the signal flowing between the base and handset of the cordless telephone was not prohibited by the *ECPA*. *Id.* at 1269 (citing 18 U.S.C. § 2510(12)(A)). The court compared the signal between the base and the handset of a cordless telephone to a stone being dropped in the water, the reaction being concentric circles moving outward until the energy generated by the stone has dissipated. *Id.* at 1270. The cordless telephone signal, as it flows out like the concentric circles in the water, can be picked up by anyone with a scanner, compatible cordless phone, or other radio receiver within 1000 feet. *Id.* Because of the ease of accessibility to this signal and the impossibility of directing the signal to an intended recipient, Congress did not intend to include the signal in the coverage of the *ECPA*.

The emanations from a computer monitor have the same essential characteristics as a cordless telephone signal. Cutrera, *supra*, at 164. The emanations are a reaction to the energy generated by the display of Petitioner's customer list on the computer monitor. They are not and cannot be sent in a particular direction, but instead emanate in all directions like circles in the water when a stone is dropped in. Any person within range of the emanations having a television or other receptor with a cathode ray tube on a compatible frequency could not avoid picking up the emanations.

Additionally, both cordless telephones and computer monitors must be accompanied by FCC warnings stating that they radiate radio frequency energy. 47 C.F.R. § 15.105(b) (1990); Cutrera, *supra*, at 164. These similar warnings show that the FCC, the federal agency charged with regulating wire and radio transmissions, recognizes that VDT emanations raise a similar level of concern about easy access as is the case with cordless telephone signals. Therefore, an examination of the applicability of the *ECPA* to the closely analogous situation of cordless telephones shows that Petitioner's emanations are not an "electronic communication" within the intended coverage of the *ECPA*.

While it is true that Congress made a specific exception for cordless telephone signals and not for electromagnetic emanations, technology was not sufficiently advanced at the time of the 1986 amendments to enable Congress to anticipate the applicability of the *ECPA* to the Petitioner's situation. It was the late 1980's before the FBI began

investigating the possibility of using CRT Microspy technology as a means of surveillance. Cutrera, *supra*, at 143.

Furthermore, although the general rule of statutory construction states when Congress explicitly enumerates exceptions to a general scheme, exceptions not explicitly made should not be implied, this rule is only true when there is no contrary legislative intent. *Andrus v. Glover Constr. Co.*, 446 U.S. 608, 616-17 (1980); *see also Moskal v. United States*, 498 U.S. 103, 111 (1990)(declaring that the United States Supreme Court has never required every permissible application of a statute to be expressly referred to in its legislative history).

Here, there is contrary legislative intent because Congress specifically excluded similarly known technology. Congress could not exclude that which it could not foresee. Thus, the only way to determine whether a particular new technology should be covered is to compare it to technology that Congress specifically addressed. The cordless telephone signal is the type of technology Congress did not intend to cover, and because the emanations here are very similar to the cordless telephone signal, it is clear Congress did not intend to cover such emanations.

Even if Congress had been aware of electromagnetic radiation and CRT Microspy technology, Congress could not have anticipated that an explicit exception was needed for electromagnetic emanations as was the case for the cordless telephone. With a cordless telephone, the signal is generated by a telephone call from one party to another. Absent an express exception, such a telephone call is clearly covered by the statute. Because the signal was a part of such a telephone call covered by the *ECPA*, application of the *ECPA* could be foreseen, thus making an express exception necessary.

However, the electromagnetic radiation in this case was not generated by a communication covered by the *ECPA* such as a telephone call. Instead, it was generated by the display of a customer list on a computer screen. Because there was no recognized communication involved in the display of the customer list, Congress could not anticipate that application of the *ECPA*. Hence, Congress would not have found it necessary to make an explicit exception for the emanations. Therefore, the rationale behind the specific exception of the cordless telephone signal, as reflected in *United States v. Carr*, indicates that the electromagnetic radiation emanating from Petitioner's computer monitor does not fall within the *ECPA*.

2. Because the emanations from the Petitioner's computer monitor can be distinguished from satellite signals which have been found to be "electronic communications," the emanations are not covered by the *ECPA*.

Courts have considered the definition of an "electronic communication" in determining its applicability to satellite television signals. Courts have found that the *ECPA* prohibits the interception of scrambled satellite signals that enable non-subscribers to access pay-per-view television. *United States v. Herring*, 993 F.2d 784, 787 (11th Cir. 1993); *United States v. Lande*, 968 F.2d 907, 909-10 (9th Cir. 1992), *cert. denied*, 113 S. Ct. 1299 (1993); *Oceanic Cablevision, Inc. v. M.D. Electronics*, 771 F. Supp. 1019, 1028 (D. Neb. 1991). Electromagnetic emanations from computers have been likened to television signals. (R. 3.) In both cases, an omni-directional signal is moved outward through the atmosphere. However, satellite signals are distinguishable from Petitioner's emanations because satellite signals are intended for specific destinations, including broadcast stations and cable head ends. Weingarten, *supra*, at 745. Additionally, the signals are scrambled for the specific purpose of preventing unauthorized interception.

On the other hand, there is no intended recipient for the Petitioner's emanations. Moreover, no effort had been made to prevent the signals from reaching anyone in the accessible radius having certain basic equipment. Because the Petitioner's emanations are distinguishable from signals covered by the *ECPA*, the emanations are not an "electronic communication." Therefore, the court properly dismissed the Petitioner's claim.

D. *Even if the electromagnetic emanations from Petitioner's computer monitor can be considered an "electronic communication," they are excluded from the ECPA because they are "readily accessible to the general public."*

Even if the electromagnetic emanations can be considered an "electronic communication," Respondent's reception of the emanations is not prohibited by the *ECPA*. The *ECPA* identifies specific exceptions to the prohibition on the interception of electronic communications. The statute states that it shall not be unlawful to intercept or access an electronic communication "that is configured so that such electronic communication is readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i) (1988).

The *ECPA* defines "readily accessible to the general public" with respect to radio communications by listing means of preventing such a communication from becoming "readily accessible to the general public." 18 U.S.C. § 2510(16) (1988). Electromagnetic emanations, like radio

signals flowing through the atmosphere, can be accessed by anyone within their reach having basic equipment operating on the same frequency. Therefore, in order to avoid these emanations being "readily accessible to the general public" and exempt from the *ECPA*, one of the methods listed in 18 U.S.C. § 2510(16) must be used to avoid the exception. Of the methods listed, scrambling or encrypting is the only method Petitioner might have arguably employed.

Although Petitioner's emanations were not on the same frequency as Respondent's television, thus requiring a device to synchronize the frequencies, this mismatch of frequencies is not the same as scrambling or encrypting the signal. First, Petitioner did nothing to cause the emanations to be on a different frequency. Luck simply worked in Petitioner's favor. Second, the Senate Judiciary Committee Report states that to scramble or encrypt a signal means to convert the signal into unintelligible form by means intended to protect the contents from unintended reception. S. Rep. No. 541.

Here, Petitioner did not show any intent and did not take any action to protect against the reception of the emanations from his computer monitor. Because the nature of the emanations, like radio signals, makes them readily accessible to the general public, and because Petitioner made no effort to protect against such accessibility as required by the statute, the emanations fall within the "readily accessible" exception to the *ECPA*. Thus, the trial court properly dismissed the Petitioner's claim.

E. *Including electromagnetic emanations within the coverage of the ECPA would contravene public policy.*

Public policy supports the view that electromagnetic emanations should not be covered by the *ECPA*.

1. Including CRT Microspy reception of electromagnetic emanations within the *ECPA*'s prohibition would crete an unenforceable law.

The CRT Microspy is a completely passive technology that leaves no sign that it was used. As a result, detection of the CRT Microspy's use is virtually impossible. Seline, *supra*, at 375. Since detection is so difficult, enforcing a prohibition of its use would be extremely difficult. For example, in the case at hand, no one would have known that Respondent used the CRT Microspy if Respondent's employee had not told Petitioner. (R. 5.) Therefore, if electromagnetic emanations are included within the coverage of the *ECPA*, it would be virtually impossible for authorities or citizens to enforce the prohibition of CRT Microspy through prosecution or civil suits.

2. Including electromagnetic emanations in the coverage of the *ECPA* would provide computer users with a false sense of security.

By including Petitioner's electromagnetic emanations within the coverage of the *ECPA*, authorities could lull computer users into a false sense of security. If the law includes electromagnetic emanations in the definition of an "electronic communication," then computer users could be led to believe that the threat of devices such as CRT Microspy is non-existent because the law prohibits its use to intercept electromagnetic emanations. However, because such a law could not be enforced due to the great difficulty in detecting use of the CRT Microspy, computer users would not be protected at all. Thus, the only effective result of including Petitioner's electromagnetic emanations in the *ECPA* would be to create a false sense of security among computer users which would discourage them from making efforts to protect themselves against CRT Microspy use.

3. Computer users have other methods of protection from the use of the CRT Microspy.

Computer users can protect themselves from the CRT Microspy's use in a couple of ways. First, the United States government has developed TEMPEST equipment which reduces radio frequency leakage and prevents eavesdropping. Cutrera, *supra*, at 143-44; Seline, *supra*, at 362. Second, computer users can insulate their rooms with copper foil to protect themselves from the use of the CRT Microspy. Cutrera, *supra*, at 144. In the case at hand, Petitioner could have used either of these protective measures to prevent the emanations from reaching Respondent. Because including electromagnetic emanations in the definition of "electronic communication" would create an unenforceable law that would lull computer users into a false sense of security, and because means are available for users to protect themselves from devices such as the CRT Microspy, the *ECPA* should not be applied to the facts of this case. Therefore, public policy supports the trial court's dismissal of the Petitioner's claim.

II. RESPONDENT'S USE OF A CRT MICROSPY TO REPRODUCE IMAGES FREELY EMANATING FROM PETITIONER'S VIDEO DISPLAY TERMINAL DID NOT GIVE RISE TO A CLAIM FOR INTRUSION UPON SECLUSION.

In *Barstel v. Frepton*, the Supreme Court of Marshall recognized a common law tort for intrusion upon seclusion. 987 M.2d 345, 348 (Marshall 1980). The court adopted the language of the Restatement (Second) of Torts § 652B (1977), stating that "one who intentionally

intrudes, physically or otherwise, upon the solitude or *seclusion* of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." 987 M.2d 345, 348 (Marshall 1980)(citing Restatement (Second) of Torts § 652B (1977))(emphasis added).

The facts established in this case are insufficient to state a claim for intrusion upon seclusion for three reasons: (1) the customer list data-bank on Petitioner's VDT did not constitute an area of seclusion for Petitioner; (2) Respondent's use of a CRT Microspy to receive images freely emanating from Petitioner's VDT did not constitute an intrusion into Petitioner's affairs; and (3) any perceived "intrusion" by Respondent did not meet Marshall's "highly offensive" standard, and thus was not actionable. In light of these facts, the Marshall Appellate Court correctly affirmed the circuit court's dismissal of Petitioner's invasion of privacy claim for failure to state a cause of action.

A. *The customer list data-bank on Petitioner's VDT did not constitute an area of seclusion for the Petitioner.*

The common law action for intrusion upon seclusion is one branch of a larger body of tort law aimed at protecting an individual's right of privacy. *See* William L. Prosser, *Privacy*, 48 Calif. L. Rev. 383, 389 (1960). In order to determine when an individual may assert an interest in privacy, or seclusion, it is helpful to recall what is protected by the right of privacy. In the 1890 article, *The Right to Privacy*, by Louis D. Brandeis and Samuel D. Warren - traditionally viewed as the origin of the common law's recognition of an independent right of privacy[1] - Brandeis and Warren classified the right to privacy "as a part of the more general right to the immunity of the person - the right to *one's personality*." 4 Harv. L. Rev. 193, 207 (1890)(emphasis added). A more recent analysis defined privacy as "that aspect of social order by which persons control access to information *about themselves*." Charles Fried, *Privacy*, 77 Yale L.J. 475, 493 (1968)(emphasis added).

As a specific subdivision of the law of privacy, the tort for intrusion upon seclusion naturally reflects privacy law's focus on the protection of one's own personality. Accordingly, one court has characterized the intrusion tort as a means of protecting "one's emotional sanctum." *Phillips v. Smalley Maintenance Services, Inc.*, 435 So. 2d 705, 711 (Ala. 1983). Thus, a cause of action for intrusion upon seclusion must be consistent with the underlying principle that the right of privacy pertains to information about one's own personality and emotions. In determining whether a plaintiff may claim an expectation of seclusion in a particular area or source of information, one must first resolve the more

1. Prosser, *supra*, at 383.

basic issue of whether that area or source of information bears any relationship to the plaintiff's privacy interest in controlling access to information about himself.

Comment (c) to Section 652I of the Restatement (Second) of Torts states: "A corporation, partnership or unincorporated association has no personal right of privacy. It has therefore no cause of action for any [type] of invasion [of privacy]." Restatement (Second) of Torts § 652I cmt. c (1981). In finding this Restatement position consistent with the underlying concerns of privacy law, one state court explained, "[t]he tort of invasion of privacy focuses on the humiliation and intimate personal distress suffered by an individual as a result of intrusive behavior. While a corporation may have its reputation or business damaged as a result of intrusive activity, it is not capable of emotional suffering." *N.O.C., Inc. v. Schaefer*, 484 A.2d 729, 730-31 (N.J. Super. Ct. Law Div. 1984).

As the foregoing authority indicates, there is no basis for privacy law protection where the plaintiff is not at risk of experiencing intimate personal distress or emotional suffering. Although the plaintiff in the present case is not a corporation, this fundamental line of analysis is still helpful in deciding whether a plaintiff can claim an expectation of seclusion in a specific source of information. If the relevant source of information does not pose any threat to the plaintiff's emotional sanctum, then there is no basis for a privacy interest or privacy protection. Again, in order for a privacy or seclusion interest to exist, there must be some potential threat to that plaintiff's own personality or emotions.

In *Pearson v. Dodd*, the Court of Appeals for the D.C. Circuit found that a senator-plaintiff's office files constituted an area of seclusion, and that the unauthorized removal of such files constituted an intrusion upon the Senator's seclusion. 410 F.2d 701 (D.C. Cir. 1969), *cert. denied*, 395 U.S. 947 (1969). One must keep in mind the specific facts that justified this holding. In *Pearson*, the information in the relevant files described various aspects of the Senator's public career. *Id.* at 703. As such, these office files were inextricably linked to the Senator's interest in controlling access to information about himself. Unauthorized disclosure of the information in these files was a source of humiliation and emotional distress for the Senator. In other words, the plaintiff in *Pearson* had a strong privacy interest in the relevant files, and this privacy interest provided the foundation for the court's determination that the files constituted an area of seclusion.

In the present case, however, Petitioner's complaint contradicts the foundations of the right of privacy by attempting to assert a privacy interest in information not about himself, but rather about Longshore Cosmetics' customers. The computer data-bank in which the Petitioner is attempting to claim an expectation of seclusion contains the names

and addresses of Longshore Cosmetics' customers. While Petitioner, as sole proprietor of Longshore Cosmetics, may claim a proprietary business interest in the customer list data-bank, this data-bank bears no relationship to the Petitioner's privacy interest in controlling access to information about himself. Although the names and addresses of Longshore Cosmetics' customers are closely related to the company's business interests, they are irrelevant to Petitioner's personal emotional sanctum. In the absence of any potential privacy interest in the customer list data-bank, Petitioner cannot use the customer list data-bank as the basis for a claim of invasion of privacy.

Indeed, the only potential privacy claim associated with a company's customer list rests with the customers themselves. For example, in *Shibley v. Time, Inc.*, a magazine subscriber sued the magazine's publisher, alleging that the publisher's practice of renting and selling subscription lists was a violation of the subscribers' right of privacy. 341 N.E.2d 337 (Ohio Ct. App. 1975). This claim was dismissed by the Ohio Court of Appeals, however, on grounds that "the right of privacy does not extend to the mailbox." *Id.* at 339. Given that an individual cannot claim a seclusion interest in his own mailing address, the address certainly cannot give rise to a privacy claim on behalf of the commercial party who is merely the file holder of this address. Keeping in mind the interests which are protected by the right of privacy, it is reasonable to conclude, "[t]he proper party plaintiff in an intrusion upon informational seclusion case would be the individual *about whom the information concerns*, not necessarily the party storing the information." John A. McLaughlin, Note, *Intrusions Upon Informational Seclusion in the Computer Age*, 17 J. Marshall L. Rev. 831, 842 n.68 (1984)(emphasis added).

Since the customer list data-bank on Petitioner's VDT merely served as a location where Petitioner stored information about other people, this data-bank had no relation to Petitioner's personal privacy interests. As a result, the customer list data-bank did not constitute an area of seclusion for Petitioner.

B. *Respondent's use of a CRT Microspy to receive images freely emanating from Petitioner's VDT did not constitute an intrusion into the Petitioner's affairs.*

Even assuming that the customer list data-bank constituted an area of seclusion for Petitioner, Petitioner's complaint for intrusion upon his seclusion must fail because Respondent's conduct did not amount to an intrusion. Respondent merely sat in his own office and received images that were freely emanating from Petitioner's VDT. By suggesting that such conduct constitutes an intrusion, Petitioner ignores the plain

meaning of the term, "intrusion." Furthermore, even if one assumes that this conduct could amount to an intrusion, it certainly did not meet the "highly offensive" standard set forth in the Restatement (Second) of Torts § 652B and *Barstel v. Frepton*, 987 M.2d at 348. Consequently, Respondent's "intrusion" could not give rise to an action for invasion of privacy.

In order to constitute an intrusion, "the defendant's conduct must involve some entry, penetration, trespass, or acquisition, as in a physical entry into an area or curtilage, or wiretapping or eavesdropping, or watching through lens or camera, or opening and reading private mail." 1 George B. Trubow, *Privacy Law and Practice* § 1.06[3] (1991). Some courts emphasize the physical aspect of intrusion upon seclusion, stating that this common law tort "is directed to protecting the integrity and sanctity of physical areas a person would naturally consider private and off limits to uninvited, unwelcomed, prying persons." *Cummings v. Walsh Constr. Co.*, 561 F. Supp. 872, 884 (S.D. Ga. 1983). In light of this emphasis, courts in the state of Georgia "require that the intrusion must be physical, analogous to a trespass." *Kobeck v. Nabisco, Inc.*, 305 S.E.2d 183, 185 (Ga. App. 1983).

A number of courts have dispensed with the requirement that an intrusion plaintiff must show a physical trespatory invasion. See *Phillips v. Smalley Maintenance Services, Inc.*, 435 So. 2d 705 (Ala. 1983); *Dietemann v. Time, Inc.*, 449 F.2d 245 (9th Cir. 1971); *Pearson v. Dodd*, 410 F.2d 701 (D.C. Cir. 1969). Still, even without looking for a technical trespass, many of the leading intrusion cases focus upon the defendant's utilization of an intruding or prying device. In *Dietemann v. Time, Inc.*, the court held that defendants' use of hidden microphones and cameras amounted to an intrusion, even though the defendants were invited into the plaintiff's home. 449 F.2d 245 (9th Cir. 1971). In *Hamberger v. Eastman*, the court found that a landlord's installation of hidden listening devices in his tenants' bedroom amounted to an intrusion. 206 A.2d 239 (N.H. 1964). Finally, in *Harkey v. Abate*, the court found that a business owner's installation of hidden viewing panels in the restroom of his premises constituted an intrusion. 346 N.W.2d 74 (Mich. App. 1983). All of these cases deal with devices that allow the defendant to *pry into* the plaintiff's area of seclusion.

In *Barstel v. Frepton*, the Supreme Court of Marshall held that the defendant's unauthorized reading of the plaintiff's diary, while the defendant was a guest in the plaintiff's home, constituted an actionable intrusion upon the plaintiff's seclusion. 987 M.2d 345 (Marshall 1980). Like the court in *Dietemann*, the Marshall Supreme Court found that, even though the defendant was a guest in the plaintiff's home and there was no technical trespass, the defendant's active efforts to pry into the plaintiff's private life amounted to an intrusion.

The opinion of the Marshall Appellate Court in the present case emphasizes the physical element of the intrusion tort, yet it remains consistent with the holdings in *Dietemann*, *Hamberger*, *Harkey*, and *Barstel*. In *Barstel*, the appellate court held that the facts alleged by Petitioner "do not constitute an invasion of privacy based on intrusion upon seclusion because Hackner never entered *or intruded* into Longshore's premises." (R. 7)(emphasis added). Indeed, Respondent merely sat in his own office and used the CRT Microspy to receive images that were freely radiating out from Petitioner's VDT. (R. 4). Obviously, this does not constitute a physical trespass on Petitioner's property. More importantly, however, Respondent's conduct does not come within the broader class of intrusion addressed in the *Barstel*, *Dietemann*, *Hamberger*, and *Harkey* holdings.

Unlike the defendant's actions in *Barstel* of opening and prying into the contents of the plaintiff's diary, Respondent in the present case simply received wavelengths that were already being radiated into the atmosphere by Petitioner's VDT. Although Respondent made use of a technical device - specifically, the CRT Microspy - this is not a device that inserts an electronic "eye" or "ear" into anyone's area of seclusion. Instead of prying into the sights or sounds of a person's private world, the CRT Microspy picks up the signals that another person is freely projecting and which reach Respondent as he sits in his own office.

In *Pearson v. Dodd*, the Court of Appeals for the D.C. Circuit held that a defendant could not be liable for intrusion upon seclusion, where the defendant merely received information from an intruder, knowing that the information had been obtained by improper intrusion. 410 F.2d at 705. The court reasoned:

> A person approached by an eavesdropper with an offer to share in the information gathered through the eavesdropping would perhaps play the nobler part should he spurn the offer and shut his ears. However, it seems to us that at this point it would place too great a strain on human weakness to hold one liable in damages who merely succumbs to temptation and listens.

Id.

Like the defendant in *Pearson*, Respondent merely sat in his office and viewed information that was brought to him by the CRT Microspy. The facts of the present case should be distinguished from *Pearson* in the sense that the CRT Microspy, unlike the eavesdropper in *Pearson*, did not improperly intrude upon or pry into the Petitioner's affairs. Nevertheless, the Respondent's simple act of viewing information projected into his own office is closely analogous to the behavior which the court in *Pearson* classified as beyond the realm of tort law. In short, by viewing images freely emanating from Petitioner's VDT, Respondent's conduct did not constitute an intrusion.

C. *Any perceived "intrusion" by the Respondent did not meet the "highly offensive" standard adopted by Marshall, and thus was not actionable.*

In order for an intrusion to give rise to an action for invasion of privacy under the standard adopted by the Supreme Court of Marshall, the intrusion must be "highly offensive to a reasonable person." *Barstel*, 987 M.2d at 348. Even if a court decided to classify Respondent's conduct of sitting in his office and receiving VDT emanations as an intrusion, this conduct, as a matter of law, does not reach the "highly offensive" standard adopted by Marshall.

When one views the unobtrusiveness of Respondent's conduct in conjunction with the fact that Respondent's only aim was to freely compete with Longshore Cosmetics in the mail order cosmetics industry, it becomes evident that Respondent's actions were reasonable under the circumstances. In short, this conduct does not give rise to a claim for intrusion upon seclusion.

1. Respondent's conduct was not actionable under a balancing of interests analysis.

Various state courts have crafted a balancing test to determine when an invasion of privacy provides the basis for a tort claim. Under such a test, "[a]n invasion of privacy is 'actionable' when the defendant's conduct is unreasonable and seriously interferes with the plaintiff's privacy interest. To determine the reasonableness of the defendant's conduct, this court must balance defendant's interest in pursuing his course of conduct against plaintiff's interest in protecting his privacy." *Gerard v. Parish of Jefferson*, 424 So. 2d 440, 445 (La. Ct. App. 1982), *cert. denied, Brister v. Parish of Jefferson*, 464 U.S. 822 (1983).

While it is already clear that Respondent's conduct did not seriously, or even minimally, interfere with any privacy interest of Petitioner's, the absence of any actionable intrusion becomes even more apparent when one evaluates the simple, free market interests underlying Respondent's actions. These capitalist objectives, while more laudable to some than others, posed no threat whatsoever to the *privacy* interests of Petitioner or anyone else.

In the present case, Respondent's sole interest was to compete in the mail order cosmetics industry on an equal footing with Longshore Cosmetics. Respondent's plan was simply to alert the broadest range of customers that they could purchase cosmetics from H&C for less money than from Longshore. Once Respondent made consumers aware of H&C and its prices, it was the consumers who decided to switch from Longshore to H&C. (R. 4). Thus, it is worth noting that Respondent's success was due to the fact that his interest in strengthening his cosmet-

ics business simultaneously furthered the general public's interest in buying goods for the lowest prices available.

On the other hand, Petitioner's interest in the present case was not to protect his privacy, but rather to maintain exclusive contact with his customers. With the availability of a captive market, Petitioner could charge higher prices for his products without competition.

Courts have held in certain cases that a plaintiff's privacy interest may be outweighed by particular benefits to the public that result from an intrusion. In *Cohan v. River Park Place Condominium Ass'n*, for example, the court held there was no claim for intrusion where the condominium association entered the plaintiff's unit in order to check for unsafe conditions. 333 N.W.2d 574 (Mich. App. 1983), *appeal denied*, 365 N.W.2d 201 (1985). The court concluded that "plaintiff's interest in privacy must yield to the defendant's interest in monitoring unsafe conditions." *Id.* at 576.

Although the economic benefit to the public in the present case is only incidental to the Respondent's interest in strengthening his own business, this beneficial off-shoot for consumers is real and should be entered into the mix of any balancing test employed by the court. In sum, Respondent's interest in using the CRT Microspy was a legitimate business interest that simultaneously benefitted cosmetics consumers by providing them with lower prices. When weighed against Petitioner's interest in blocking competition - a proprietary interest which is removed from Petitioner's right of privacy - Respondent's interest is reasonable and does not give rise to a claim for invasion of privacy.

2. Respondent's conduct was not actionable in light of the broad availability of the Petitioner's VDT emanations.

Respondent's actions in this case serve as proof that the images freely radiating from Petitioner's VDT could have been received by anyone, within range, who possessed the proper antennae equipment. In deciding that an intrusion is reasonable and not "highly offensive" as a matter of law, courts have taken note of the actual availability of information which the plaintiff claims to be private. For example, in *McLain v. Boise Cascade Corp.*, the Oregon Supreme Court held that a grant of nonsuit was proper where:

> In the first place, the surveillance and picture taking were done in such an unobtrusive manner that plaintiff was not aware that he was being watched and filmed. In the second place, plaintiff conceded that his activities which were filmed could have been observed by his neighbors or passers-by. Undoubtedly the [workmen's compensation claims] investigators trespassed . . . but it is also clear that the trespass . . . did not constitute an unreasonable surveillance 'highly offensive to a reasonable man.'

533 P.2d 343, 346 (Or. 1975).

In the present case, it is established that Respondent's conduct was so unobtrusive that Petitioner was not aware of it until he was informed by Casey three months after-the-fact. (R. 4). In *Dietemann v. Time, Inc.*, the Ninth Circuit Court of Appeals noted that the common law provided a cause of action for intrusions that cause the plaintiff emotional distress. 449 F.2d 245, 247 (9th Cir. 1971). In the present case, Petitioner was unaware of the Respondent's acquisition of the relevant information, and, as a result, Respondent's conduct had no effect on the Petitioner's state of emotions. Instead, Petitioner was only concerned by the decline in his business performance that followed Respondent's offering lower prices to previous Longshore customers.

The complete unobtrusiveness of Respondent's conduct, combined with the fact that Respondent was receiving images which were freely emanating from Petitioner's VDT to surrounding antennae, conclusively shows that Respondent's conduct cannot, as a matter of law, rise to the level of a "highly offensive" intrusion. Consequently, even if Respondent's conduct is termed an intrusion, the Marshall Appellate Court would still have been correct in affirming the circuit court's dismissal of Petitioner's invasion of privacy claim for failure to state a cause of action.

CONCLUSION

The electromagnetic radiation emanating from Petitioner's computer monitor does not constitute an "electronic communication" within the plain language of the *ECPA*. Both the legislative history of the *ECPA* and court decisions considering the application of the *ECPA* to analogous radiations indicate the emanations are not an "electronic communication." Moreover, expanding the *ECPA* to cover these emanations would be contrary to public policy.

In addition, the facts established in this case are insufficient to state a claim for intrusion upon seclusion. First, the customer list data-bank on Petitioner's VDT did not constitute an area of seclusion for Petitioner. Second, Respondent's conduct of receiving images freely emanating from Petitioner's VDT did not constitute an intrusion. Third, even if Respondent's conduct was considered an intrusion, it was reasonable and unobtrusive, and thus was not actionable.

For the reasons stated herein, Respondent respectfully requests that the Supreme Court of the State of Marshall affirm the dismissal of Petitioner's claims.

APPENDIX

18 U.S.C. § 2510

§ 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 for communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

(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 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) 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) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

(B) any wire or oral communication'

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

(D) any communication from a tracking device (as defined in section 3117 of this title);

(13) "user" means any person or entity who—

(A) uses 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 electronic communications, and any computer facilities or re-

lated 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; and

(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.

18 U.S.C. § 2511

§ 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; or

(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;

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 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 a 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 the 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 the State or any political subdivision of a State, as my 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 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 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 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 and oral 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 fre-

quency 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.

(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 the 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 or encrypted, then—

(i) if the communication is not the radio portion of a cellular telephone communication, 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 public land mobile radio service communication or a paging service communication, the offender shall be fined not more than $500.

(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a statelite 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.