Case Western Reserve Journal of International Law

Volume 23 | Issue 2

1991

Eavesdropping on the Compromising Emanations of Electronic Equipment: The Laws of England and the United States

Christopher J. Seline

Eavesdropping On the Compromising Emanations of Electronic Equipment: The Laws of England and the United States

We in this country, in this generation, are — by destiny rather than choice — the watchmen on the walls of world freedom. [1]

INTRODUCTION

For less than two hundred dollars it is possible to *see* what someone is typing on their computer screen from several hundred yards away. The device that makes this possible can be built from easily-available parts for under two hundred dollars. The device is passive and does not require the placement of a listening device in or near the screen. There is little chance of detection or apprehension. Although the Government has acted to prevent dissemination of technical data related to these devices, schematics are available from the computer underground. The Government's efforts have served only to limit the availability of counter-measures, rather than to prevent the device's use. Except for military activities handling national security information, few computer sites are protected from this type of surveillance. The ease with which this technology may be implemented, coupled with the impossibility of detection and the lack of adequate counter-measures, make it the perfect computer surveillance technique. It is already becoming the method of choice for hackers.

Before the advent of modern technology, spying was performed in person. To overhear a conversation the eavesdropper had to be within listening range. This is no longer true.[2] By the mid-twentieth century electronic surveillance devices were commonplace.[3] Today, technologies whose mere existence was once a closely-guarded secret are discussed openly in the print media.[4] Society has grown accustomed to the exist-

---

[1] Undelivered speech of President John F. Kennedy, Dallas Citizens Council 35-36 (Nov. 22, 1963).

[2] S. Rep. No. 1097, 90th Cong. 2d Sess., *reprinted in* 1968 U.S. CODE CONG. & ADMIN. NEWS 2112, 2154.

[3] Examples include hidden microphones and video cameras as well as more esoteric devices such as spread spectrum transmitters. *See generally*, D. POLLOCK, METHODS OF ELECTRONIC AUDIO SURVEILLANCE (1973) (surveillance measures and counter-measures).

[4] *Compare* Broad, *Every Computer 'Whispers' Its Secrets*, N.Y. Times, Apr. 5, 1983, at C-1 col. 2 (TEMPEST openly discussed) *with* NACSI 4003 Annex C (word TEMPEST deleted during redaction). *See infra*, note 13, for discussion of TEMPEST.

ence of these devices. The use of surveillance devices against criminals, foreign agents, and even ordinary citizens is well-publicized.[5]

Computers have become commonplace. They are used in business and at home. Many computers have software designed to prevent unauthorized use and unauthorized access to information.[6] These computers are still not secure. The information they contain may be obtained through electronic surveillance.

In the past, the communication lines of a computer would be tapped and information obtained as it transits the line.[7] Today, eavesdroppers can intercept the electromagnetic radiation emitted by computers and their peripherals.[8] The radiation may be picked up from cables, or passively as it moves through the aether.[9]

This technology has made Justice Brandeis, prophecy a reality "[t]he progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court. . . ."[10]

This note will explore the legality of this type of emanations surveillance in the United States and England. It will deal specifically with the legality of individuals using such surveillance to eavesdrop on the emanations of electronic equipment. Prohibitions and limitations on its use by governments, their agents, and employees will be examined only as each intersects the main topic.

The first section is an introduction to compromising emanations. It includes a discussion of how compromising emanations are used to obtain information, and how special equipment limits these emanations. The topic of compromising emanations is considered classified by the United States Government. Several of the documents used were classified and were only released to the author under a Freedom of Informa-

---

[5] *See generally* D. MARTIN, WILDERNESS OF MIRRORS (1980) (detailed accounts of CIA and KGB counter-intelligence operations); J. BAMFORD, THE PUZZLE PALACE: A REPORT OF AMERICA'S MOST SECRET INSIDE THE NATIONAL SECURITY AGENCY (1982) (detailed discussion of the National Security Agency, its organization and activities).

[6] *See generally* DEPARTMENT OF DEFENSE COMPUTER SECURITY CENTER, DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (1985) (setting forth a uniform set of requirements and classes for assessing the effectiveness of computer software security).

For a discussion of the Internet worm and counter-worm activities *see generally* D. SEELEY, A TOUR OF THE WORM (1988); M. EICHIN & J. ROCHLIS, WITH MICROSCOPE AND TWEEZERS: AN ANALYSIS OF THE INTERNET VIRUS OF NOVEMBER 1988 (1988); E. SPAFFORD, THE INTERNET WORM PROGRAM: AN ANALYSIS (1988).

[7] *See* D. POLLOCK, *supra* note 3, at 216-30.

[8] *See infra*, note 28 and accompanying text.

[9] Broad, *supra* note 4.

[10] Olmstead v. United States, 277 U.S. 438, 474 (1927) (Brandeis, J., dissenting).

tion Act Request. Although heavily sanitized, these documents contain information never before available.

Section Two examines U.S. law as it relates to this technology. Section Three discusses English law, and why English law has succeeded where U.S. law has failed. The final section explores possible solutions and sets forth recommendations to address this problem. The reader is reminded that the law routinely lags behind technology. Only through technology can technological problems be solved.

Appendix A contains the text of a memorandum (previously classified top secret) from President Harry S. Truman to the Secretary of State and Secretary of Defense regarding the communications intelligence activities of the United States. This memo created the National Security Agency. Appendix B is an Introduction to Compromising Emanations explaining the current technology in the electronic intelligence area.

It is possible to intercept the compromising emanations of electronic equipment. A compromising emanation is one that will yield useful information when analyzed. Both electromagnetic radiation and signals that *escape* through cables can be considered emanations. The technique of electronic intelligence gathering using the compromising emanations of target equipment will be referred to as ELINT/CE in this note.[11] The use of ELINT/CE is not illegal under the laws of the United States or England.

In the United States the possession of computer equipment that does not emit compromising emanations is limited to the U.S. Government and government contractors utilizing national security information.[12] This leads to the conundrum that it is legal for individuals and the government to invade the privacy of others, but illegal for individuals to take steps to protect their privacy.

The author suggests that the solution is straightforward. The government has a standard for limiting compromising emanations. The standard, known as TEMPEST,[13] is set forth in NACSIM 5100A[14] and

---

11 The actual short name used by the National Security Agency to refer to ELINT/CE has not been released. We will use our own short name: ELINT/CE. ELINT is the acronym for ELectronic INTelligence and CE is the acronym for Compromising Emanations. For a more detailed introduction to compromising emanations the reader is directed to Appendix B.

12 A contract is signed when the contractor is approved for access to TEMPEST information. Releasing the equipment is a violation of the contract. Further, releasing the equipment is tantamount to selling secrets since the design techniques are secret. A contractor would therefore be liable under any number of unspecified laws ranging from treason to export violations.

13 TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used as a synonym for 'compromising emanations.' DEFENSE COMMUNICATIONS AGENCY, SECURITY REQUIREMENTS FOR AUTOMATIC DATA PROCESSING (ADP) SYSTEMS, DCA Instruction No. 630-230-19, at A-5 (1985) [ADP SECURITY].

14 NATIONAL SECURITY AGENCY, NATIONAL COMMUNICATIONS SECURITY INFORMATION MEMORANDUM (NACSIM) 5100A: COMPROMISING EMANATIONS LABORATORY TEST REQUIRE-

is not available to the public.[15] The only way to prevent this type of eavesdropping is through the use of equipment meeting TEMPEST standards. Such equipment is referred to as TEMPEST Certified.

To promote general use and availability of TEMPEST Certified equipment, information on protecting privacy under TEMPEST should be made freely available. TEMPEST Certified equipment should be legally available. All computer equipment should be labeled with its emanations profile, and whether it meets the TEMPEST spectral limits.

To promote the protection of personal information, a tort should be created against data bureaus that fail to take reasonable precautions in protecting personal data. Should a data bureau fail to adequately protect such information, the person to whom the data relates would have a cause of action against the bureau. This will encourage those who hold the information of others to protect that data.

I. INTELLIGENCE GATHERING

The Transition from HUMINT to ELINT

Spying is divided by professionals into two main types: human intelligence gathering (HUMINT) and electronic intelligence gathering (ELINT). As the names imply, HUMINT relies on human operatives, and ELINT relies on technological operatives. For centuries HUMINT was the sole method for collecting intelligence.[16] The HUMINT operative would steal important papers, observe troop and weapon movements,[17] lure people into his confidences to extract secrets, and stand

---

MENTS, ELECTROMAGNETICS (1981)[hereinafter NACSIM 5100A] (supersedes National Communications Security/Emanations Security Information (NACSEM) 5100).

[15] Unclassified information concerning compromising emanations shall not be discussed or made available to persons without a need-to-know, especially when the aggregate of unclassified information could be combined to reveal classified information. No person is entitled to knowledge or possession of, or access to, information concerning compromising emanations solely because of his office, position or type of clearance. No information related to compromising emanations shall be released for public consumption through the press, advertising, radio, TV or other public media.

NATIONAL SECURITY AGENCY, NATIONAL COMMUNICATIONS SECURITY INFORMATION (NACSI) 4003: CLASSIFICATION GUIDELINES FOR COMSEC INFORMATION at C-2 (1978)[hereinafter NASCI 4003].

[16] HUMINT has been used by the United States since the Revolution. CENTRAL INTELLIGENCE AGENCY, INTELLIGENCE IN THE WAR OF INDEPENDENCE 9 (1976).

> The necessity of procuring good intelligence is apparent & need not be further urged — All that remains for me to add is, that you keep the whole matter as secret as possible. For upon Secrecy, Success depends in Most Enterprises of the kind, and for want of it, they are generally defeated, however well planned & promising a favorable issue.

Id. at preface (*citing* Letter of George Washington (July 26, 1777)).

[17] I wish you to take every possible pains in your powers, by sending trusty persons to Staten Island in whom you can confide, to obtain Intelligence of the Enemy's situation & numbers — what kind of Troops they are, and what Guards they have — their strength & where posted.

under the eavesdrip[18] of houses, eavesdropping on the occupants.

As technology has progressed, tasks that once could only be performed by humans have been taken over by machines. Spying has also become automated. Modern satellite technology allows troop and weapons movements to be observed with greater precision and from greater distances than a human spy could ever hope to accomplish.[19] The theft of documents and eavesdropping on conversations may now be performed electronically. This means greater safety for the human operative, whose only involvement may be the placing of the initial ELINT devices. This has led to the ascendancy of ELINT over HUMINT because the placement and monitoring of ELINT devices may be performed by a technician who has no training in the art of spying. The gathered intelligence may be processed by an intelligence expert, perhaps thousands of miles away, with no need of field experience.[20]

ELINT has a number of other advantages over HUMINT. If a spy is caught, her existence could embarrass the employing state and she could be forced into giving up the identities of her compatriots or other important information. By its very nature, a discovered ELINT device cannot give up any information; the ubiquitous nature of bugs provides the principal state with the ability to plausibly deny ownership or involvement.[21]

Trespassatory ELINT versus Passive ELINT

ELINT devices (bugs) fall into two broad categories: trespassatory and non-trespassatory. Trespassatory bugs require some type of trespass in order for them to function. A transmitter might require the physical invasion of the target premises for placement, or a microphone might be surreptitiously attached to the outside of a window. A telephone transmitter can be placed anywhere on the phone line, including at the central switch. Trespass occurs either when the device is physically attached to the phone line, or if inductive, when placed in close proximity to the phone line.[22] Even microwave bugs require the placement of a resonator

---

Id.

[18] Eavesdrip is an Anglo-Saxon word, and refers to the wide overhanging eaves used to prevent rain from falling close to a house's foundation. The eavesdrip provided "a sheltered place where one could hide to listen clandestinely to conversation within the house." W. MORRIS & M. MORRIS, MORRIS DICTIONARY OF WORD AND PHRASE ORIGINS 198 (1st ed. 1977).

[19] Blair, *Reconnaissance Satellites* in OUTER SPACE: A NEW DIMENSION OF THE ARMS RACE 125 (B. Jasani ed. 1982); Smith, *Evolution of the Soviet Space Program from Sputnik to Salyut and Beyond*, in INTERNATIONAL SECURITY DIMENSIONS OF SPACE 295 (1984).

[20] *See generally* BAMFORD, *supra* note 5.

[21] *Id.*

[22] *See generally* D. POLLOCK, *supra* note 3, at 216, 226.

cone within the target premises.[23]

Non-trespassatory (passive) ELINT devices operate by receiving electromagnetic radiation (EMR) as it radiates through the aether, and do not require the placement of bugs. Methods include the interception[24] of information transmitted by satellite, microwave, and radio, including mobile and cellular phone transmissions. This information is purposefully transmitted with the intent that some intended person or persons would receive it.[25]

Non-trespassatory ELINT also includes the interception of information that was never intended to be transmitted. All electronic devices emit electromagnetic radiation. Some of the radiation, as with radio waves, is intended to transmit information. Much of this radiation is not intended to transmit information and is merely incidental to whatever work the target device is performing. This information can be intercepted and reconstructed into a coherent form.

Introduction to Compromising Emanations[26]

According to the National Security Agency[27] (NSA), "information . . . which is generated, processed, or transferred by electrical, electronic, and electromechanical equipments is subject to compromise because of unintentional electromagnetic radiated and conducted emanations."[28] These "[c]ompromising emanations [CE] are unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose . . . information transmitted, received, handled, or otherwise processed by any infor-

---

23 Pursglove, *How Russian Spy Radios Work*, Radio Electronics, Jan. 1962, at 89-91.

24 *Interception* is an espionage term of art and should be differentiated from its more common usage. When information is intercepted, the interceptor as well as the intended recipient receive the information. Interception when not used as a term of art refers to one person receiving something intended for someone else; the intended recipient never receives what he was intended to receive.

25 For example, when you make a phone call you intend for the recipient of that call to be able to hear your voice. It is your intent to communicate some information. Even though you may not know the exact route your call will take (wire, microwave, fiber, or satellite) you are transmitting information with the intent that at some time some authorized person will receive this information, your phone call.

When you type on your computer it is not your intention that what you are typing be transmitted to the surrounding neighborhood. If your computer is not TEMPEST Certified it is transmitting this information, though you did not intend for this to happen.

26 For a more technical discussion of the subject see Appendix B

27 The National Security Agency is charged with protecting United States government communications and intercepting the communications of other nations. Memorandum from President Harry S. Truman to the Secretary of State and the Secretary of Defense (Oct. 24, 1952) (establishing the National Security Agency). This memorandum, never before released to the public in its entirety, is set out in Appendix A.

28 NACSIM 5100A, *supra* note 14, at iii.

mation-processing equipment."[29]

Intercepting the compromising emanations from electronic equipment is referred to as ELINT/CE.[30] The term ELINT/CE does not describe one particular circuit, or even one particular interception technique. Instead, it encompasses the range of all ELINT devices that eavesdrop on compromising emanations.

With current ELINT/CE technology it is possible to reconstruct the contents of computer video display unit (VDU) screens from up to one kilometer away; reconstructing the contents of a computer's memory or the contents of its mass storage devices is more complicated and must be performed from a smaller distance.

The reconstruction of information from CE is not limited to computers and digital devices but is applicable to all electronic devices.[31] However, ELINT/CE is especially effective against VDUs because they produce a very high level of electromagnetic radiation which may be received without expensive amplifiers or antennas.[32] The circuit necessary to eavesdrop on a VDU is simple to build. Circuit diagrams are available from the computer underground; the parts may be purchased from any electronics dealer for less than two-hundred dollars.

Emanations which cannot be detected cannot be analyzed to obtain information; they are therefore not a security threat.[33] An item of equipment that gives off very low emanations is secure against this form of eavesdropping.

The NSA has established an emanations standard for electrical equipment. Equipment whose emanations are below the levels set by this standard are considered secure against this form of eavesdropping. The document setting forth this standard is NACSIM 5100A.[34]

Equipment that is tested and certified as conforming to NACSIM

---

[29] *Id.* at 2-1.

In laymen's terms, compromising emanations are signals that will yield information when analyzed. To over-simplify, if an electronic typewriter emanates a specific signal when the "A" key is pressed, and emanates another specific signal when the "B" key is pressed, and so forth for all the keys, then these emanations are compromising because a circuit designed to eavesdrop on electronic typewriters would be able to determine what was being typed. The information typed on the typewriter would be compromised by the typewriter's emanations.

[30] *See supra*, note 11, for the definition of ELINT/CE.

[31] J. Schultz, *Defeating Ivan with TEMPEST*, in C3I HANDBOOK: COMMAND CONTROL COMMUNICATIONS INTELLIGENCE 181 (Defense Electronics 1st ed. 1986).

[32] For a thorough discussion of VDU ELINT/CE *see* Van Eck, *Electromagnetic Radiation from Video Display units: An Eavesdropping Risk?*, 4 COMPUTERS & SECURITY 269 (1985).

[33] Threat: Any circumstance or event with the potential to cause harm . . . in the form of . . . disclosure . . . of data. A threat is a potential for harm. The presence of a threat does not mean that it will necessarily cause actual harm. Threats exist because of the very existence of the system or activity and not because of any specific weakness.

ADP SECURITY, *supra* note 13, at A-14.

[34] "Equipment meeting the limits (set forth in NACSIM 5100A) provide an acceptable degree

5100A is referred to as TEMPEST certified equipment. Producing TEMPEST Certified equipment is expensive; to encourage the availability of off-the-shelf TEMPEST Certified equipment the NSA maintains a list of equipment that is TEMPEST certified. When a government agency or activity requires TEMPEST Certified equipment they may purchase directly from this list rather than contracting to have the equipment redesigned to meet NACSIM 5100A.[35]

Information regarding compromising emanations is restricted.[36] The information is available strictly on a need-to-know basis.

> Unclassified information concerning compromising emanations shall not be discussed or made available to persons without a need-to-know, especially when the aggregate of unclassified information could be combined to reveal classified information. No person is entitled to knowledge or possession of, or access to, information concerning compromising emanations solely because of his office, position or type of clearance.[37]

Limited information is available to firms producing TEMPEST equipment for the government. These firms must be owned by U.S. citizens and pass a review by the Defense Investigation Service.[38] Contractors are required to submit to prepublication review.[39] In addition, they

---

of conducted and radiated (emanations) security at the equipment level." NACSIM 5100A, *supra* note 14, at 2-1.

[35] Shearin, *TEMPEST: Let's Do More Than Talk About It*, J. ELECTRONIC DEF., Apr. 1985, at 55. In 1985, Mr. Shearin was the Executive Manager for TEMPEST Security Engineering at the National Security Agency.

[36] NACSI 4003, *supra* note 15, at C-1, C-2.

[37] *Id.* at C-2.

[38] Shearin, *supra* note 35, at 55.

[39] All TEMPEST assistance is rendered by the contracting agency, including technical support and the prepublication review of any proposed dissemination of TEMPEST information. The control and distribution of classified TEMPEST information is a contractual requirement.

Id.

For a discussion of prior restraint and national security as they relate to the First Amendment, *see* United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979), *reh'g. denied*, 486 F. Supp. 5, *motion denied*, 443 U.S. 709 (mandamus), *motion denied*, 5 Media L.R. (7th Cir.), *dismissed without op.*, 610 F.2d 819 (7th Cir.) (magazine intended to publish plans for nuclear weapon; prior restraint injunction issued), *see also* New York Times Co. v. United States, 403 U.S. 713 (1971) (per curium) (Pentagon Papers case: setting forth prior restraint standard which government was unable to meet).

For a general discussion of the First Amendment and national security, *see* T. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION (1970); Cheh, *Government Control of Private Ideas — Striking a Balance Between Scientific Freedom and National Security*, 23 JURIMETRICS J. 1 (1982) (concluding "[c]urrent laws and regulations limiting scientific and technical expression" exceed the legitimate needs of national security); M. Feldman, *Why the First Amendment Is Not Incompatible With National Security Interest: Maintaining a Constitutional Perspective*, in THE HERITAGE LECTURES 90 (1987). *Cf.* Bork, *Neutral Principles and Some First Amendment Problems*, 47 IND. L. J. 1

are discouraged from discussing TEMPEST with anyone, especially the press.[40]

Even the document defining the TEMPEST standards is restricted. NACSIM 5100A is considered COMSEC material; access by contractor personnel is therefore limited to U.S. citizens holding final government clearances.[41] NACSIM 5100A may not be "disclosed or released by any holder without approval of the Director, NSA [or the] Chief, CSS [(Central Security Service)]."[42] Nor may it be released to foreign nationals without "PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NATIONAL SECURITY AGENCY."[43]

This virtual press blackout has left the public completely unaware of compromising emanations or how to protect against them. Even public sector computer security managers are unaware of how simple it is to build a ELINT/CE device. If the public is completely unaware of the threat they are effectively prevented from acting to stop it. Security managers are blissfully unaware that their computer security is being undermined by compromising emanations. The public is unable to form an opinion, let alone lobby their elected representatives for a solution.

Even if the public was aware, they are prevented from acting to limit their compromising emanations. TEMPEST equipment is not available to the public. It is available only to government agencies that can demonstrate a definite security need.[44] The only way to prevent emanations is with TEMPEST equipment. If the public is denied this equipment, they can not act to defend themselves.

The lack of information is more dangerous than the restriction on owning TEMPEST equipment because the public does not even know they are at risk. If they knew they were at risk but were denied TEMPEST certified equipment, they could at least take the minor precaution

---

(1971) (First Amendment applies only to political speech) *with* Lewy, *Can Democracy Keep Secrets*, 26 POL. REV. 17 (1983) (endorsing draconian secrecy laws mirroring the English system).

40 "[W]e are very sensitive to TEMPEST exposure in the media, educational seminars, or industrial trade shows . . . We must continue to work toward . . . ensuring the inviolability of [TEMPEST information]. Shearin, *supra* note 35, at 75.

"[W]e challenge both Government and industry to restrict TEMPEST inquiries and information to established classified channels." *Id.* at 55.

"No information related to compromising emanations shall be released for public consumption through the press, advertising, radio, TV or other public media." NACSI 4003, *supra* note 15, at C-2.

41 NACSIM 5100 A., *supra* note 14, at title page.

42 *Id.*

43 *Id.* at i (emphasis in original).

44 The Drug Enforcement Agency was able to demonstrate such a need when "major drug smugglers" mastered ELINT/CE. *TEMPEST Market Lolls in Doldrums*, 5 ADVANCED MILITARY COMPUTING, July 17, 1989, at 1.

of not storing sensitive information on a computer system.[45]

II. UNITED STATES LAW

The Communications Act of 1934

Section 605 of the Communications Act of 1934[46] (1934 Act) was intended to criminalize the unauthorized interception of wire and radio communications.[47] In 1968, section 605 was amended[48] to shift control of wire communications to Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[49] Section 605 is now primarily limited to the interception of radio and television communications. However, the section still prohibits communications workers from intercepting and divulging communications to unauthorized persons.

Section 605 as amended explicitly allows the public to intercept public broadcast transmissions:

> [Section 605] shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is transmitted by a station for the use of the general public, which relates to ships, aircraft, vehicles, or persons in distress, or which is transmitted by an amateur radio station or by a citizens band radio operator.[50]

The Section specifically prohibits the interception and divulging of radio or wire transmissions by unauthorized persons. No communications worker may "divulge or publish"[51] the "existence, contents, substance, purpose, effect, or meaning"[52] of a radio or wire communications to anyone but authorized persons. Authorized persons include:

(1) "the addressee, his agent, or attorney,"[53]
(2) "a person employed or authorized to forward such communication

---

[45] Not storing important information on a computer is an oft overlooked security technique. Although rarely used, it is the best possible security precaution because no computer is completely secure. In fact, taking the realities of computer security into account, the only secure computer is a mason's brick. You cannot get any information into it and therefore miscreants cannot get information back out.

[46] 47 U.S.C.S. § 605 (Law. Co-op. 1962).

[47] The single largest violator of the Act was the U.S. Government, under Operation Shamrock. From September 1, 1945 through May 15, 1975 the U.S. Government received copies of all the cable traffic entering or leaving the United States. The cables were provided to the National Security Agency and its predecessor, the Signals Security Agency, for thirty years. The Government received complete cooperation from ITT Communications (now ITT World Communications), Western Union Telegraph Company, and RCA Communications (now RCA Global). BAMFORD, *supra* note 5, at 302-05.

[48] Pub. L. 90-351, 82 Stat. 197 (1968).

[49] 18 U.S.C. §§ 2510-2520 (1970).

[50] 47 U.S.C. § 605(a) (1982).

[51] *Id.*

[52] *Id.*

[53] *Id.*

to its destination,"[54]

(3) "proper accounting or distributing officers of the various communicating centers over which the communication may be passed,"[55] or

(4) "to the master of a ship under whom [the communications worker] is serving."[56]

The communications worker may also divulge the message or information about the message "in response to a subpoena issued by a court of competent jurisdiction, or . . . on demand of other lawful authority."[57]

Further, unauthorized individuals are prohibited from intercepting any radio communication using the message, or any information contained therein[58] for his own benefit, or the benefit of another.[59] Unauthorized individuals are also prohibited from interception radio communication and divulge[ing] or publish[ing][60] the existence, contents, substance, purpose, effect, or meaning[61] of the message.

The Act was intended to criminalize surveillance techniques as they were known in 1934. It is impossible to tell if the act had its intended effect. It is in fact impossible to tell if most laws have their intended effect because successful criminals do not get caught. This is especially true for information crimes like surveillance. With surveillance, nothing is stolen except privacy. The parties to an eavesdropped conversation are unaware of the eavesdropping. Unless the parties actively seek out and locate the eavesdropping devices, they will never know they are being eavesdropped on. Sophisticated eavesdropping equipment is almost impossible to detect. Passive equipment is impossible to detect; the only method of prevention is the use of counter-measures to prevent interception. A successful eavesdropper is never detected. Therefore, the Act would only effect those who were so clumsy as to be caught.

Information on whether the U.S. government had mastered ELINT/CE in 1934 is secret. Even though ELINT/CE is used mainly against VDUs, it is also used in combination with an trespassatory tap to intercept wire communications. It was used in this manner in the Berlin Tunnel in 1954.[62] It is possible that this technique was in its infancy when the 1934 Act was drafted. For whatever reasons, Congress made no mention of it in the legislative history and it is not covered by the Act.

---

54 *Id.*
55 *Id.*
56 *Id.*
57 *Id.*
58 *Id.*
59 *Id.*
60 *Id.*
61 *Id.*
62 D. MARTIN, *supra* note 5, at 75-76 (1980).

The Act's failure to cover ELINT/CE is not a problem because making ELINT/CE illegal would not prevent its use. Assuming *arguendo* that ELINT/CE were criminalized, what then? How would ELINT/CE malefactors be caught? The answer is they would not be. ELINT/CE is completely passive. There are no tell-tale signs that it is being used, nor does the person under surveillance receive any indication she is being surveilled. Unlike trespassatory ELINT devices, ELINT/CE does not require the entry and surreptitious placement of the device in the premises under surveillance. There is, therefore, no chance of the ELINT/CE malefactor being caught in the act of placing the bug. Nor is there any chance of his use of the ELINT/CE device being detected. There is, therefore, no possible way in which the ELINT/CE malefactor can be caught.

If the malefactor cannot be caught, then why have a law? It could be argued that making it illegal would discourage people from using ELINT/CE. Unfortunately, this is short-sighted. Perhaps the very timid would be dissuaded. Considering how unlikely it is that the ELINT/CE malefactor would be caught it is hard to argue that anyone would be *scared off* by an unenforceable law.

To explore the ramifications of Section 605 fully, four hypotheticals will be used.

Hypothetical One. D1 eavesdrops on V's conversations by planting a small radio transmitter on V's office. This would be not be a criminal act under section 605. Section 605 is limited to wire and radio communications, but in this case V was not intending to communicate by radio so the interception falls outside the Act.[63]

Hypothetical Two. D2 listens to V's phone conversation by physically tapping the wires of a common carrier. This would be a criminal act under section 605 as originally codified. D2 has intercepted a wire communication within the definition in the section.[64] However, this would not be a violation of section 605 as amended because control of wire communications has been switched to Title III.

Hypothetical Three. D3 uses a radio receiver to listen passively in on a private radio transmission. He overhears private information exchanged between a politician and his mistress. D3 sells this information to the *National Enquirer*. This would be a criminal act under section 605 which makes it a crime for any "person having received or intercepted

---

[63] Lee v. United States, 343 U.S. 747 (1952) (undercover agent wearing hidden microphone and transmitter did not violate section 605 since other person conversation was transmitted was not using a Section 605 communication system); United States v. Coplon, 88 F. Supp. 921 (D.C.N.Y. 1950) (evidence gathered by police Detectaphone admissible since there was no wire or radio communication involved).

[64] *See* Weiss v. United States, 308 U.S. 321 (1939); United States v. Sullivan, 116 F. Supp. 480 (D.C. cir. 1953), *aff'd*, 219 F.2d 760 (D.C. Cir. 1955).

radio communication . . . [to] divulge or publish the . . . contents . . . of such communication. . . ."[65]

D3's act is criminalized even though it is passive. However, the Act adds the requirement of personal profit. This serves two purposes. First, it does not penalize amateur radio enthusiasts, or emergency personnel, who may accidentally intercept a private communication while tuning for a legitimate transmission. Second, it limits sanctions to instances where there has been some type of overt, non-passive act. Had D3 merely listened, but not acted, he would not have been detected. It was his overt act that led to his demise.

Hypothetical Four. D4 uses ELINT/CE to eavesdrop on the word processor belonging to the senior partner in a mergers and acquisitions firm. He uses this information to invest in the stock market.[66] D4 has committed no crime under the Act. The information was not transmitted via wire as criminalized in the original version of the Act. Neither was the information transmitted by radio. It therefore falls outside the Act.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968

The Communications Act of 1934 was not satisfactory[67] because technology had outstripped the law[68] and the Supreme Court had prohibited warranted searches of Section 605 communication.[69] Accordingly, Congress amended the Communications Act of 1934 and introduced Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[70] Title III was designed to restore communications privacy.[71] It had as its dual purpose (1) protecting the privacy of wire and oral

---

65 47 U.S.C. § 605(a) (1982). *See also* Edwards v. State Farm Ins. Co., 833 F.2d 535 (5th Cir. 1987).

66 For the sake of simplicity we will ignore applicable security and exchange laws.

67 Both proponents and opponents of wiretapping and electronic surveillance agreed that the then present state of the law in this area was extremely unsatisfactory and that the Congress should act to clarify the resulting confusion. S. REP. NO. 1097, 90th Cong. 2d Sess., *reprinted in* 1968 U.S. CODE CONG. & ADMIN. NEWS 2112, 2154.

68 *Id.* at 2154-60.

69 Nardone v. United States, 308 U.S. 338 (1939).

70 18 U.S.C. §§ 2510-2520 (1970) (hereinafter [Title III].

Title III is essentially a combination of S. 675, the Federal Wire Interception Act . . . and S. 2050, the Electronic Surveillance Control Act of 1967 . . . Subsequent to the introduction of S. 675, the U.S. Supreme Court, on June 12, 1967, handed down the decision in Berger v. New York, 87 S. Ct. 1873, 338 U.S. 41, which declared unconstitutional the New York statute authorizing electronic eavesdropping (bugging) by law-enforcement officers in investigating certain types of crimes. The Court held that the New York stature on its face, failed to meet certain constitutional standards. In the course of the opinion, the Court delineated the constitutional criteria that electronic surveillance legislation should contain. Title III was drafted to meet these standards and to conform with Katz v. United States, 389 U.S. 347 (1967).

communications,[72] and (2) delineating on a uniform basis the circumstances and conditions under which the interpretation of wire and oral communications may be authorized.[73]

Section 2511 of Title III prohibits the interception,[74] use,[75] or disclosure[76] of any wire or oral communication. Interception is the aural acquisition of the contents of any wire or oral communication, through the use of any electronic, mechanical, or other device.[77] Violators are subject to criminal[78] and civil penalties.[79]

A wire communication is any communication made on wire or cable provided by a common carrier.[80] Wire communication is protected even if partially transmitted by microwave or satellite.[81]

The protection of oral communication is specifically limited to situa-

---

S. REP. NO. 1097, 90th Cong., 2d Sess., REPRINTED IN 1968 U.S. CODE CONG. & ADMIN. NEWS at 2153.

[71] The tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques. As a result of these developments, privacy of communication is seriously jeopardized by these techniques of surveillance. Commercial and employer-labor espionage is becoming widespread. It is becoming increasingly difficult to conduct business meetings in private. Trade secrets are betrayed. Labor and management plans are revealed. No longer is it possible, in short for each man to retreat into his home and be left alone.

Id. at 2154.

[72] Virtually all concede that the use of wiretapping or electronic surveillance techniques by private unauthorized hands has little justification where communications are intercepted without the consent of one of the participants.

Id. at 2156.

[73] *Id.* at 2153.

[74] 18 U.S.C. § 2511(1)(a) (1970).

[75] *Id.* at § 2511(1)(d).

[76] *Id.* at § 2511(1)(c).

[77] 18 U.S.C. § 2510(4) (1970). *See also* Application of the United States for an Order Authorizing Installation & Use of a Pen Register, 546 F.2d 243 (8th Cir. 1976), *cert. denied*, 434 U.S. 1008 (1978) (what cannot be heard falls outside the aural acquisition prohibition); United States v. Senditz, 589 F.2d 153 (4th Cir. 1978), *cert. denied*, 441 U.S. 922 (1978) (aural acquisition does not include computer transmissions).

[78] Violators shall be fined not more than $10,000 or imprisoned not more than five years, or both. 18 U.S.C. § 2511(1) (1970).

[79] Civil damages include actual damages (minimum $1000), punitive damages, and reasonable attorney and litigation costs. 18 U.S.C. § 2520 (1970).

[80] [W]ire communication means any communication 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 furnished or operated by any person engaged as a common carriers in providing or operating such facilities for the transmission of interstate or foreign communications.

18 U.S.C. § 2510(1) (1970).

[81] United States v. Gregg, 629 F. Supp. 958, 963 (W.D. Mo. 1986) *aff'd*, 829 F.2d 1430 (10th Cir. 1987), *cert. denied*, 486 U.S. 1022 (1988). United States v. Clegg, 509 F.2d 605, 611 (5th Cir. 1975).

tions where there is a justified expectation of privacy.[82] The expectation of privacy test has been established in a series of Supreme Court cases defining the relation between the warrant requirement of the Fourth Amendment[83] and government's use of electronic surveillance devices.[84]

The exact definition of reasonable expectation of privacy is still a mystery today. Professor Katz argues that the Supreme Court has whittled the expectation of privacy doctrine down to the nub.[85] According to Katz there is no expectation of privacy for anything other than oral communication.[86]

Warranted searches, foreign intelligence warrantless searches,[87] and

---

[82] "[O]ral 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." 18 U.S.C. § 2510(2) (1970).

[83] The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated; and no warrants shall issue but upon probable cause, support by oath or affirmation and particularly describing the place to be searched and the persons or things to be seized.

U.S. CONST. Amend. IV.

[84] In Olmstead v. United States, 277 U.S. 438 (1927), the Supreme Court held that warrantless wiretapping was not a violation of the Fourth Amendment because it was not a search of a physical premises and did not seize anything tangible. *Id.* at 464.

Forty years later, in Katz v. United States, 389 U.S. 347 (1967), the Supreme Court held that warrantless wiretapping was an unreasonable search and therefore violated the Fourth Amendment. *See also* Berger v. New York, 389 U.S. 41 (1967) (capturing conversation with an eavesdropping device is a search under the Fourth Amendment). Silverman v. United States, 365 U.S. 505 (1961) (recording of oral statements is a seizure). Under *Katz*, the Fourth Amendment is violated where the individual has a "reasonable expectation of privacy." 389 U.S. at 360.

[85] Katz, *In Search of A Fourth Amendment for the Twenty-first Century*, 65 IND. L.J. 549 (1990).

[86] *Id.* at 555.

[87] 18 U.S.C. § 2511(3)(1970). It was never the intention of Congress to limit the Executive branch's ability to surveil foreign nationals, both at home and abroad:

It is obvious that whatever means are necessary should and must be taken to protect the national interest. Wiretapping and electronic surveillance techniques are proper means for the acquisition of counterintelligence against the hostile action of foreign powers. Nothing in the proposed legislation seeks to disturb the power of the President to act in this area. Limitations that may be deemed proper in the field of domestic affairs of a nation become artificial when international relations and internal security are at stake.

S. REP. NO. 1097, 90th Cong., 2d Sess., *reprinted in* 1968 U.S. CODE CONG. & ADMIN. NEWS at 2157.

The Foreign Intelligence Surveillance Act of 1978 (FISA) has expanded upon Title III's blanket permission for foreign intelligence and counter-intelligence gathering within the United States. 50 U.S.C. §§ 1801-1811 (1982). *See also* S. REP. NO. 604, 95th Cong., 2d Sess. 1, *reprinted in*, 1978 U.S. CODE CONG. & ADMIN. NEWS 3904.

A detailed discussion of the FISA is beyond the scope of this work. For a more detailed discussion see Brown & Cinquegrana, *Warrantless Physical Searches For Foreign Intelligence Purposes: Executive Order 12,333 and the Fourth Amendment*, 35 CATH. U.L. REV. 97 (1985); Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PENN. L. REV. 793 (1989); Giesy, *Jurisdictional Limitations on the Foreign Intelligence Surveillance Court*, 8 SUFFOLK TRANSNAT'L L.J. 259 (1984); Kornblum,

line monitoring for diagnosis and repair[88] are specifically excluded from section 2511's prohibitions. Section 2512 prohibits the sale, manufacture, or advertisement of eavesdropping devices.[89] Common carriers, their agents and employees, acting within the normal course of business are excluded,[90] as are government employees and persons acting under contract with the government.[91]

Title III successfully updated anti-surveillance law to match the surveillance technology of 1968. However, there is no reference to ELINT/CE in its history and Title III does not cover ELINT/CE. As with the 1934 Act there is no information available as to whether this was omission or commission.

To explore fully the ramifications of Title III, the four previous hypotheticals will be used, as well as one new hypothetical.

Hypothetical One. D1 eavesdrops on V's conversations by planting a small radio transmitter on V's office. This would be a criminal act under section 2511(1)(a) which criminalizes the interception of oral communication. Under 2510(2) the oral communication must have an expectation of privacy. Since V's conversations took place within V's private office, D1 has intercepted an oral communication where there was a valid expectation of privacy.

Hypothetical Two. D2 listens to V's phone conversation by physically tapping the wires of a common carrier. This would be a criminal act under section 2511(1)(a), criminalizing the interception of wire communications. Under 2510(1) wire communication includes only wires belonging to a common carrier. D2 has intercepted the V's wire communication using a common carrier.

Hypothetical Three. D3 uses a radio receiver to listen passively in on a private radio transmission. He overhears private information exchanged between a politician and his mistress. D3 sells this information to the *National Enquirer*. This would not be a criminal act under Title III because radio transmissions do not have a reasonable expectation of privacy.[92] It is criminalized under the 1934 Act.[93]

Hypothetical Four. D4 uses ELINT/CE to eavesdrop on the word

America's Secret Court: Listening In On Espionage and Terrorism, 24 JUDGES J., Summer 1985, at 14 (1985); Saltzburg, *National Security and Privacy: Of Governments and Individuals Under the Constitution and the Foreign Intelligence Surveillance Act*, 28 VA. J. OF INT'L. L. 129 (1987).

88 18 U.S.C. § 2511(2) (1970).

89 18 U.S.C. § 2512(1) (1970). *See* United States v. Pritchard, 773 F.2d 873 (7th Cir. 1985), *cert. denied*, 474 U.S. 1085 (1986) (illegal possession of wiretap); United States v. Bast, 495 F.2d 138 (D.C. Cir. 1974) (possession, distribution, and advertisement of wiretaps).

90 18 U.S.C. § 2512(2)(a) (1970).

91 18 U.S.C. § 2512(2)(b) (1970).

92 United States v. Rose, 669 F.2d 23 (1st Cir.), *cert. denied*, 459 U.S. 828 (1982).

93 *See supra* note 65 and accompanying text (hypothetical three).

processor belonging to the senior partner in a mergers and acquisitions firm. He uses this information to invest in the stock market.[94] D4 has committed no crime under Title III. The information was not transmitted via a common carrier. Neither was the information transmitted by radio. It therefore falls outside the scope of Title III.

Hypothetical Five. D5 listens to the information transmitted between two computers by physically tapping the wires of a common carrier. This is not a criminal act because Title III only extends to aural communication and computer communication is not considered aural.[95]

The Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986[96] amended Title III to include non-wire communication. The Act was designed to update Title III and bring it in line with current technologies. The Act was specifically designed to include electronic mail, inter-computer communications, and cellular telephones while excluding cordless telephones.[97]

The Act did not modify the main concerns of Title III: protecting conversations and telecommunications.[98] It merely updated Title III to match current technology.[99] An effort was made to phrase the amendments in broad enough terms that they would cover future advances in telecommunications technology.

As before, ELINT/CE was excluded from the Act and its history. By 1986, however, the NSA was using ELINT/CE and had a countermeasures program in place. Either the NSA had not informed Congress of its TEMPEST program and Congress failed to criminalize ELINT/CE through ignorance, or Congress intentionally chose not to criminalize it. In either case ELINT/CE was not, and has not, been criminalized.

No American author has suggested that ELINT/CE be criminalized. Nor does this author think it should be criminalized. ELINT/CE is a completely passive technology; there is no way to detect its use. ELINT/CE leaves no tell-tale sign that it was used. If its use cannot be detected then the ELINT malefactors cannot be apprehended. This means that if it is criminalized, there is no way to enforce the law.

Criminalization could have an unintended effect of increasing the

---

94 We will ignore applicable security and exchange laws for the sake of simplicity.

95 United States v. Senditz, 589 F.2d 153 (4th Cir. 1978), *cert. denied*, 441 U.S. 922.

96 18 U.S.C.S. §§ 2510-2710 (Law. Co-op. 1989).

97 18 U.S.C.S. § 2510(1) (Law. Co-op. 1989); 18 U.S.C.S. § 2510(12)(A) (Law. Co-op. 1989).

98 S. REP. No. 541, 99th Cong., 2d Sess., *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS 3555.

99 *Id.* at 3557.

loss of information via ELINT/CE. If ELINT/CE is illegal then the public may be led to believe (erroneously) that the threat has been dealt with. This could lead to a false sense of safety. The public would not purchase TEMPEST Certified equipment because the they would rely to the law to protect them when, in fact, the law is incapable either of detecting or stopping ELINT/CE. To explore fully the ramifications of ECPA, the five previous hypotheticals will be used.

Hypothetical One. D1 eavesdrops on V's conversations by planting a small radio transmitter on V's office. This would be a criminal act under section 2511(1)(a), which criminalizes the interception of oral communication. Under 2510(2) the oral communication must have an expectation of privacy. Since V's conversations took place within his V's private office, D1 has intercepted an oral communication where there was a valid expectation of privacy.

Hypothetical Two. D2 listens to V's phone conversation by physically tapping the wires of a common carrier. This would be a criminal act under section 2511(1)(a) criminalizing the interception of wire communications. Under 2510(1) wire communication includes only wires belonging to a common carrier. D2 has intercepted the V's wire communication using a common carrier.

Hypothetical Three. D3 uses a radio received to passively listen in on a private radio transmission. He overhears private information exchanged between a politician and his mistress. D3 sells this information to the *National Enquirer*. This would not be a criminal act under the ECPA because radio transmission do not have a reasonable expectation of privacy.[100] It is criminalized under the 1934 Act.[101]

Hypothetical Four. D4 uses ELINT/CE to eavesdrop on the word processor belonging to the senior partner in a mergers and acquisitions firm. He uses this information to invest in the stock market.[102] D4 has committed no crime under the ECPA. The information was not transmitted via a common carrier. Neither was the information transmitted by radio.

As just demonstrated, there is no effective change for these hypotheticals between the original Title III and Title III as amended by the Electronic Communications Privacy Act. The ECPA does, however, protect computer communications. This is especially important considering the large amount of information that is now transmitted by computer.

Hypothetical Five. D5 listens to the information transmitted between two computers by physically tapping the wires of a common car-

---

100 United States v. Rose, 669 F.2d 23 (1st Cir., *cert. denied*, 459 U.S. 828 (1982).

101 *See supra* note 65 and accompanying text (hypothetical three).

102 For the sake of simplicity we will ignore applicable security and exchange laws.

rier. This is a criminal act under section 2511(1)(a) which criminalizes intercepting electronic communications. Electronic communications 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, photoelectric or photo-optical system.[103] D5 has violated the ECPA by eavesdropping on the electronic communication between two computers.

It should be noted that the definition of electronic communication is overly broad. It would, for example, include a person using his eyes (a photo-optical system) to see neon sign (which by definition transmits information using a photoelectric system). The viewing of a sign could, then, be a violation of 2511(1)(A).

This example illustrates the problem of trying to write legislation that is broad enough to encompass future, unimagined, technologies. In attempting to write a statute broad enough to encompass the unknown technological future, Congress wrote one that was broad enough to include almost all communication. But, at the same time, they failed to make it broad enough to include ELINT/CE.

Technology will always be years ahead of the law. Instead of writing an overly broad statute, Congress should have undertaken to amend the ECPA twice every year. In this case, the definitions and language would be written narrowly, not broadly. This would allow the statute to pinpoint current technology without being over-inclusive. By amending it twice a year, Congress would be able to apply the statute to new technological developments as they occurred, pinpointing the problems as they developed.[104]

III. ENGLISH LAW

In England, the Home Office has set forth drafting principles controlling how and why criminal legislation is created.[105] Under these principles, a criminal statute *will not* be written if there is a less onerous way to address the problem. The statute will be written *if and only if* criminalization is the only way to limit the targeted behavior.[106] "This helps to maintain public respect for the criminal law."[107] The English law, both existing statutory law and proposed law, adhere to these principles.

---

103 18 U.S.C.S. § 2510(12) (Law. Co-op. 1989).

104 In arguing this, the author does not want to appear to be supporting the criminalization of ELINT/CE. The author is merely advocating a legislative technique more in harmony with the ever changing technological world than the technique currently in use.

105 THE LAW COMMISSION, WORKING PAPERS 1988, No. 110: COMPUTER MISUSE ¶ 1.11 (1988) [hereinafter THE LAW COMMISSION].

106 *Id.*

107 *Id.*

Under the principles, a new offense may not be created unless it is enforceable.[108] To this end, the legislation must be "clear in its scope and effect."[109] Further, criminal sanctions are "reserved for dealing with undesirable behaviour for which other, less drastic means of control would be ineffective, impracticable or insufficient.[110] If tort law is an adequate remedy, then criminal sanctions are prohibited. The behavior in questions [must be] so serious that it goes beyond what . . . is proper to deal with on the basis of compensation as between one individual and another and concerns the public interest in general."[111]

There are no computer crime offenses in England; the English do not have a specific set of statutes aimed at crimes involving computers. Instead, computer crime is dealt with in the same manner as traditional offenses.[112] "For example . . . it is not a crime to use someone else's lawnmower without their permission, so long as it is returned undamaged. By analogy, it is not an offense to make unauthorized use of a computer."[113]

The Interception of Communications Act 1985[114] criminalizes the intentional interception of communications sent over public telecommunications lines.[115] The communications may be voice or data.[116] The Secretary of State for Home Affairs determines which communication systems are part of the public telecommunications system.[117]

The interception of communications on a telecommunication line can take place with a physical tap on the line, or the passive interception of microwave or satellite links.[118] It is not an offense to intercept com-

---

[108] *Id.*

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *Id.* at ¶ 1.5.

[113] *Id.*

[114] An Act to make new provision for and in connection with the interception of communication sent by post or by means of telecommunications systems and to amend section 45 of the Telecommunications Act, 1984. Interception of Communications Act, 1985, ch. 56.

[115] (1) Subject to the following provisions of this section, a person who intentionally intercepts a communication in the course of its transmission by post or by means of a public telecommunication system shall be guilty of an offence and liable—

(a) on summary conviction, to a fine not exceeding the statutory maximum;

(b) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

Id. at § 1.

[116] Telecommunications Act, 1984, ch. 12, § 4(1)(c); Interception of Communications Act, 1985, ch. 56, § 10 (1)(a) & (b).

[117] Telecommunications Act, 1984, ch. 12, § 9(1).

[118] Trespassatory eavesdropping is patently in violation of the statute.

The offense created by section 1 of the Interception of Communications Act 1985 covers those forms of eavesdropping on computer communications which involve 'tapping' the wires along which messages are being passed. One problem which may arise, however, is

munications if the eavesdropper has a reasonable belief that one of the parties to the communication has consented.[119] In addition, it is not an offense if the interception is done under a warrant issued by the Home Secretary.[120] Nor is there an offense if the interception was done pursuant to the provision of telecommunication service.[121]

The Communications Act of 1985 is roughly equivalent to U.S. law as amended by the Electronic Communications Privacy Act.[122] Both cover interception of communications whether transmitted by wire, satellite, fiber, or microwave. The English law, however, is limited to common carriers; U.S. law has no such limitation. Neither law differentiates between computer communications and voice communications; interception of either is a criminal act. This means that the current law finally protects computer communications.

The advantage of the English law over U.S. law lies in the method of design. The English law was written by a group of academics and is thereby mostly removed from the grip of lobbyists. The United States was not so fortunate. ECPA, and its predecessors, were written by various government officials, rewritten by lobbyists, and amended by politicians. Where the English gave long and thoughtful analysis, the U.S. effort was less reasoned.

ELINT/CE is not prohibited by the Act. The English Law Commission is the authoritative body in England regarding legislation. It is the official opinion of the Law Commission that eavesdropping on the compromising emanations of computer equipment is not prohibited by the Interception of Communications Act 1985:

> There are . . . forms of eavesdropping which the Act does not cover. For example, eavesdropping on a VDU screen by monitoring the radiation field which surrounds it in order to display whatever appears on the legitimate user's screen on the eavesdropper's screen. This activity would not seem to constitute any criminal offense (unless the information gained was specifically protected under, for example, the Official Secrets Act 1911).[123]

In its official review of computer misuse[124] the Law Commission

---

the question of whether the communication in question was intercepted in the course of its transmission *by means of a public telecommunication system*. It is technically possible to intercept a communication at several stages in its transmission, and it may be a question of fact to decide the stage at which it enters the 'public' realm.

THE LAW COMMISSION, *supra* note 105, at § 3.30 (emphasis added).

119 Interception of Communications Act, 1985, ch. 56, § 1(2)(B).

120 *Id.*, at ch. 56, § 1(2)(A).

121 *Id.* § 1(3)(A).

122 18 U.S.C.S. §§ 2510-2710 (Law. Co-op. 1989).

123 THE LAW COMMISSION, *supra* note 105, § 3.31.

124 THE LAW COMMISSION, *supra* note 105.

evaluated whether English law was sufficient to deal with so called computer crime, including ELINT/CE.[125] The Commission, in its official report, provisionally decided that the general criminal law was sufficient to deal with most forms of computer misuse:[126]

> In the light of our study of the present law, our provisional conclusion is that the general criminal law is sufficient to deal with most of the computer misuse which we have identified . . . Our provisional view is that a comprehensive computer crime statute is neither necessary nor appropriate in England . . . The present scheme of criminal offenses relating to theft, fraud and criminal damage encompass a broad range of factual circumstances and, in general, avoid distinctions based on the kind of property stolen and damaged . . . Our provisional view is that there is no reason to change this policy in relation to computers.[127]
>
> * * *
>
> [T]o justify legislative action and particularly the creation of any new criminal offense, we believe that it is essential to be able to identify the nature and extent of any risks involved.[128]

The English decided not to add ELINT/CE to their Communications Act, or to include it in a computer crime bill, because they felt ELINT/CE should not be a separate crime. The argument for inclusion is that ELINT/CE, in and of itself, should be a crime. The English response is that the act of eavesdropping may not be a crime but if someone commits a crime with the information they will be punished. Since they will already be punished for breaking the law there is no need for adding an extra penalty for using ELINT/CE. For example, if D uses ELINT/CE to obtain information about P and blackmails P then the crime of blackmail has been committed and will be punished accordingly. It is the resulting action that is punished. If the resulting action is not a crime, goes the argument, then why make obtaining the information a crime?

The American response is that anything bad should be a crime. Since eavesdropping is by definition bad it should be a crime. This argument fails to address the intent of the legislation. Why was ECPA enacted? To limit eavesdropping. The goal of limiting eavesdropping?

---

[125] In discussing the pros and cons of creating a hacker offense, the Law Commission noted:

> A further argument against the creation of a hacking offense is that the offense may be very difficult to enforce. We understand that it is possible for a hacker to obtain access to data on a computer and to ensure that the fact that he has obtained access remains undetected.

Id. § 6.16.

[126] Neither the English nor the Scottish law commissions have found sufficient evidence "of the scale and consequences of computer misuse to conclude that it would of itself suggest an impending crisis of a kind that demanded prompt legislative action." *Id.* § 6.18.

[127] *Id.* § 8.2

[128] *Id.* § 6.18.

Protecting privacy. The English have a much better way to protect privacy. The English realize that criminalizing ELINT/CE and other forms of data theft will not prevent the theft because data thieves are rarely caught. The way to prevent the theft is shift the burden of the person most able to protect the data: the person who controls the computer. With this in mind, the English enacted the Data Protection Act of 1984.

Reducing Compromise of Data By Penalizing Those Who Fail To Reasonably Protect Data

In England the Data Protection Act of 1984[129] imposes sanctions against anyone who stores the personal information[130] of others on a computer and fails to take reasonable measures to prevent disclosure of that information. The act mandates that personal data may not be stored in any computer unless the computer bureau or data user[131] has registered under the act.[132] This provides for a central registry and the tracking of which companies or persons maintain databases of personal information. Data users and bureaus must demonstrate a need and purpose behind their possession of personal data.

The Act requires data users and computer bureaus to adhere to eight Data Protection Principles.[133] The eighth principle requires the

---

129 "An Act to regulate the use of automatically processed information relating to individuals and the provision of services in respect of such information." Data Protection Act, 1984, ch. 35, preamble.

130 "Personal data" means data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user), including any expression of opinion about the individual but not any indication of the intentions of the data user in respect of that individual.

Id. § 1(3).

131 'Data user' means a person who holds data, and a persons Holds data if —

(a) the data form part of a collection of data processed or intended to be processed by or on behalf of that person as mentioned in subsection (2) above; [subsection (2) defines data] and

(b) that person (either alone or jointly or in common with other persons) controls the contents and use of the data comprised in the collection; and

(c) the data are in the form in which they have been or are intended to be processed as mentioned in paragraph (a) above or (though not for the time being in that form) in a form into which they have been converted after being so processed and with a view to being further so processed on a subsequent occasion.

Id. §§ 1(5).

132 *Id.* §§ 4, 5.

133 *Id.* Schedule One.

Personal data held by data users

1. The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.
2. Personal data shall be held only for one or more specified and lawful purposes.
3. Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.

data users and bureaus to take security measures against the compromise of personal data:

> Appropriate security measures shall be taken against unauthorized access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data. [In interpreting the Eighth Principle], regard shall be had (a) to the nature of the personal data and the harm that would result from such access, alteration, disclosure, loss or destruction as are mentioned in this principle; and (b) to the place where the personal data are stored, to security measures programmed into the relevant equipment and to measures taken for ensuring the reliability of staff having access to the data.[134]

The Act provides tort remedies to any person who is damaged by disclosure of the personal data.[135] Reasonable care to prevent the disclosure is a defense.[136] English courts have not yet ruled what level of computer security measures constitute reasonable care under the Act. However, the courts have determined that due diligence is the same as reasonable care.[137] Due diligence is a question of fact.[138] The failure of company directors to exercise due diligence is imputed to the corpora-

---

4. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.
5. Personal data shall be accurate and, where necessary, kept up to date.
6. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
7. An individual shall be entitled—
   (a) at reasonable intervals and without undue delay or expense—
      (i) to be informed by any data user whether he holds personal data of which that individual is the subject; and
      (ii) to access to any such data held by a data user; and
   (b) where appropriate, to have such data corrected or erased.

Personal data held by data users or in respect of which services are provided by persons carrying on computer bureaux

8. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction or personal data.

Id. Schedule One.

134 *Id.*

135 An individual who is the subject of personal data held by a data user . . . and who suffers damage by reason of - (c) . . . the disclosure of the data, or access having been obtained to the data without such authority as aforesaid shall be entitled to compensation from the data user . . . for any distress which the individual has suffered by reason of the . . . disclosure or access.

Id. § 23.

136 "[I]t shall be a defense to prove that [the data user] had taken such care as in all the circumstances was reasonably required to prevent the . . . disclosure or access in question." *Id.* § 23(3).

137 Riverstone Meat Co., Ltd. v. Lancashire Shipping Co. Ltd., 1 Q.B. 536, 581 (1960).

138 Hammett (R.C.) Ltd. v. Crabb, 145 L.T.R. 638 (K.B. 1931).

tion.[139] Given the serious threat from ELINT/CE towards compromising information, due diligence must include the use of TEMPEST Certified equipment.

There is no method to determine just how well the Act works. Data theft leaves no fingerprints or broken windows. The data is just copied, not removed so there is little evidence a break-in ever occurred. With little chance to detect break-ins (a break-in would include acquisition of data via ELINT/CE) it is impossible to determine the Act's success.

However, it is clear that a protected computer system must be harder to acquire information from than a non-protected system. Therefore, less data is being compromised now that systems must be protected than before when systems were only haphazardly protected.

The United States has no similar law. Even if ELINT/CE was a crime it would be impossible to detect its use. If it can not be detected then ELINT malefactors can not be apprehended. This leaves data open to anyone who can build a ELINT/CE unit. The plans for these devices are available from the computer underground;[140] the parts to build one cost less than two hundred dollars. This makes it very easy for anyone to use ELINT/CE.

Only certain Department of Defense activities and federal investigatory bodies use TEMPEST Certified equipment. It is not used by the private sector. In fact, most security managers are completely unaware of the threat. This leaves the door wide open to ELINT/CE operators.

At this time all detected computer break-ins come from some type of direct access. The hacker, cracker, or phone phreak (hereinafter collectively referred to as hackers) break directly into the computer. This is accomplished either by breaking access security, or by intercepting communications and stealing passwords. Because these methods require a phone or network connection to the computer they can be traced. As the police and FBI become more adept at tracking down computer hackers, the hackers will shift to passive collection systems to obtain information. ELINT/CE, the ultimate passive collection system, will become the method of choice. It is cheap, efficient, undetectable, and best of all, counter-measures.

---

139 Pearce v. Cullen, 96 Sol. J. 132 (Q.B. 1952).

140 There is no exact definition of the computer underground because, unlike the French Underground of the Second World War or the Weather Underground of the 1970's, the computer underground is not organized. The underground can best to termed as those individuals who are operating outside the mainstream of accepted computer use. For a discussion of the computer underground *see* J. BRUNNER, SHOCKWAVE RIDER (1975) (fictional account). For a discussion of what it means to be an individual and rebel against regimentation and thought control, *see* M. WHITE & J. ALI, THE OFFICIAL PRISONER COMPANION (1988). For a discussion of the cyberpunk computer underground see W. GIBSON, NEUROMANCER (1985)(fictional account); Markoff, *Cyberpunks Seek Thrills in Computerized Mischief*, N.Y. Times, Nov. 26, 1988, at 1, col. 1.

IV. SOLUTIONS

ELINT/CE is a threat to keeping information secret. The most direct way to prevent someone from eavesdropping on compromising emanations is to prevent the emanations. This can be accomplished through use of TEMPEST Certified equipment. The question then becomes, how best to encourage the use of TEMPEST Certified equipment?

Criminalization is not the answer. ELINT/CE is a completely passive technology; there is no way to detect its use. ELINT/CE leaves no telltale sign that it was used. If its use cannot be detected then the ELINT malefactors cannot be apprehended. If it is criminalized, there is no way to enforce the law.

Criminalization could have an unintended effect of increasing the loss of information via ELINT/CE. If ELINT/CE is illegal then the public may be led to believe (erroneously) that the threat has been stopped. This could lead to a false sense of security. The public would not purchase TEMPEST Certified equipment because it would rely to the law for protection when, in fact, the law is incapable either of detecting or stopping ELINT/CE.

If the goal is to limit the compromise of data the question that must be asked in: how best to limit the loss of data? The answer is: make the person who controls the data responsible for its protection.

The only way to prevent the loss of data through compromising emanations is to prevent those emanations. To limit compromising emanations we must encourage the use of equipment that does not produce them. This requires the use TEMPEST Certified equipment.

Businesses have no incentive to protect people's personal information. It is in the business' interest to protect its corporate secrets, but there is little incentive to protect information whose compromise will not cost the firm lost revenues.

A disincentive must be created to make firms protect data. By creating a private tort between the person whose data was compromised and the company, the Data Protection Act creates this disincentive. Should the firm fail to take reasonable steps to protect the information then it may be sued by the person whose data was compromised.

In deciding how much to spend on protecting such data the firm will make an economic decision. The firm will balance its possible liability under the Act with the cost of protecting the information. Should the liability be high enough, the firm will invest in TEMPEST Certified equipment. If the liability are not so high then the firm will choose to use a more cost effective but less secure protection mechanism. In this manner economic efficiency is achieved.

Implementing a U.S. version of the Data Protection Act will only secure personal information held by firms where the cost of protecting it

is less than the cost of leaving it unprotected. This does not address the total spectrum of information that society might wish to protect. Each person or company should be able to determine on their own whether they want to protect information that is not covered by the Data Protection Act. This requires education.

The public is grossly unaware of the threat presented by ELINT/CE. To solve this, government and industry must begin an education program to provide information on ELINT/CE and TEMPEST suppression. This will serve to alert computer users to the ELINT/CE threat. Once aware, each computer owner can make his own decision about the cost of compromise versus the cost of installing TEMPEST Certified equipment.

To further this goal, all electronic equipment should be labeled as either "TEMPEST Certified or as Emitting Compromising Emanations." This will remind users of the security provided by the equipment before they purchase it.[141]

V. CONCLUSION

United States law does not criminalize ELINT/CE. It was never the intention of Congress to prohibit ELINT/CE, nor has Congress ever discussed criminalizing the interception of compromising emanations. The English Law Commission has addressed the topic of Compromising Emanations. The Commission determined that ELINT/CE should not be made illegal.

Criminalizing ELINT/CE in the United States is not an effective way to prevent the compromise of information. Making ELINT/CE a crime will serve only to give the public a false sense of safety because ELINT/CE equipment is passive in nature and hence undetectable. If the equipment cannot be detected then the malefactors cannot be caught; and if they cannot be caught then the syllogism follows that they cannot be tried or convicted. If the malefactors cannot be tried or convicted then the law will fail to either deter or punish those who use ELINT/CE.

Under the English Data Protection Act data users and computer bureaus must take reasonable precautions in protecting the personal data they hold.[142] Failure to take reasonable precautions will result in the data holder or bureaus being liable in tort to those whose data was compromised. The use of TEMPEST Certified equipment is reasonable where the possible liability in tort is greater than the cost of purchasing

---

[141] TEMPEST Certified equipment must be modified every few years as surveillance devices become more sensitive and the TEMPEST standard is updated. This is not a onerous burden, since computer equipment has a very short useful life and is generally replaced/updated every few years.

[142] *See supra* note 129 and accompanying text.

the equipment. By balancing these economic interests the Acts achieves economic efficiency.

The solution to ELINT/CE is to encourage the use of non-compromising equipment, *i.e.* TEMPEST Certified equipment. Only equipment that does not emit compromising emanations is secure against ELINT/CE. To encourage the use of TEMPEST Certified equipment a two-pronged program is necessary. Prong one is the enactment of legislation similar to the English Data Protection Act. This will force data users and computer bureaus to determine which is more economically efficient: controlling compromising emanations by purchasing TEMPEST Certified equipment, or paying out claims to persons whose personal information has been compromised.

Prong two is education. Only through education will the public be able to determine whether TEMPEST Certified equipment is cost-effective for protecting their information. Once they have been educated computer purchasers will be able to determine whether they need TEMPEST Certified equipment, and whether they are will to pay the high price tag for security.

*Christopher J. Seline**

* J.D. Candidate, Case Western Reserve School of Law (1991).

APPENDIX A

5/4/54/OS[143]
A 20707 NSA TS CONTL. NO 73-00405
COPY: D321

Oct 24 1952

MEMORANDUM FOR: The Secretary of State
The Secretary of Defense

SUBJECT: Communications Intelligence Activities

The communications intelligence (COMINT) activities of the United States are a national responsibility. They must be so organized and managed as to exploit to the maximum the available resources in all participating departments and agencies and to satisfy the legitimate intelligence requirements of all such departments and agencies.

I therefore designate the Secretaries of State and Defense as a Special Committee of the National Security Council for COMINT, which Committee shall, with the assistance of the Director of Central Intelligence, establish policies governing COMINT activities, and keep me advised of such policies through the Executive Secretary of the National Security Council.

I further designate the Department of Defense as executive agent of the Government, for the production of COMINT information.

I direct this Special Committee to prepare and issue directives which shall include the provisions set forth below and such other provisions as the Special Committee may determine to be necessary.

1. A directive to the United States Communication Intelligence Board (USCIB).

This directive will replace the National Security Council Intelligence Directive No. 9, and shall prescribe USCIB's new composition, responsibilities and procedures in the COMINT fields. This directive shall include the following provisions.

a. USCIB shall be reconstituted as a body acting for and under the Special Committee, and shall operate in accordance with the provisions of the new directive. Only those departments or agencies represented in USCIB are authorized to engage in COMINT activities.

b. The Board shall be composed of the following members:

(1) The Director of Central Intelligence, who shall be the Chairman of the Board.

---

[143] This memorandum was originally classified TOP SECRET. It has been downgraded and released to the author following a Freedom of Information Act request.

(2) A representative of the Secretary of State.

(3) A representative of the Secretary of Defense.

(4) A representative of the Director of the Federal Bureau of Investigation.

(5) The Director of the National Security Agency.

(6) A representative of the Department of the Army.

(7) A representative of the Department of the Navy.

(8) A representative of the Department of the Air Force.

(9) A representative of the Central Intelligence Agency.

c. The Board shall have a staff headed by an executive secretary who shall be appointed by the Chairman with the approval of the majority of the Board.

d. It shall be the duty of the Board to advise and make recommendations to the Secretary of Defense, in accordance with the following procedure, with respect to any matter relating to communications intelligence which falls within the jurisdiction of the Director of the NSA.

(1) The Board shall reach its decision by majority vote. Each member of the Board shall have one vote except the representatives of the Secretary of State and of the Central Intelligence Agency who shall each have two votes. The Director of Central Intelligence, as Chairman, will have no vote. In the event that the Board votes and reaches a decision, any dissenting member of the Board may appeal from such decision within 7 days of the Special Committee. In the event that the Board votes but fails to reach a decision, any member of the Board may appeal within 7 days to the Special Committee. In either event the Special Committee shall review the matter, and its determination thereon shall be final. Appeals by the Director of NSA and/or the representatives of the Military Departments shall only be filed with the approval of the Secretary of Defense.

(2) If any matter is voted on by the Board but -

(a) no decision is reached and any member files an appeal;

(b) a decision is reached in which the representative of the Secretary of Defense does not concur and files an appeal; no action shall be taken with respect to the subject matter until the appeal is decided, provided that, if the Secretary of Defense determines, after con-

sultation with the Secretary of State, that the subject matter presents a problem of an emergency nature and requires immediate action, his decision shall govern, pending the result of the appeal. In such an emergency situation the appeal may be taken directly to the President.

(3) Recommendations of the Board adopted in accordance with the foregoing procedures shall be binding on the Secretary of Defense. Except on matter which have been voted on by the Board, the Director of NSA shall discharge his responsibilities in accordance with his own judgment, subject to the direction of the Secretary of Defense.

(4) The Director of NSA shall make such reports and furnish such information from time to time to the Board, either orally or in writing, as the Board my request, and shall bring to the attention of the Board either in such reports or otherwise any major policies or programs in advance of their adoption by him.

e. It shall also be the duty of the Board as to matters not falling within the jurisdiction of NSA;

(1) To coordinate the communications intelligence activities among all departments and agencies authorized by the President to participate therein;

(2) To initiate, to formulate policies concerning, and subject to the provision of NSCID No. 5, to supervise all arrangements with foreign governments in the field of communications intelligence; and

(3) to consider and make recommendations concerning policies relating to communications intelligence of common interest to the departments and agencies, including security standards and practices, and, for this purpose, to investigate and study the standards and practices of such departments and agencies in utilizing and protecting COMINT information.

f. Any recommendation of the Board with respect to the matters described in paragraph e above shall be binding on all departments or agencies of the Government if it is adopted by the unanimous vote of the members of the Board. Recommendations approved by the majority, but not all, of the members of the Board shall be transmitted by it to the Special Committee for such action as the Special Committee may see fit to take.

g. The Board will meet monthly, or oftener at the call of the Chairman or any member, and shall determine its own procedures.

2. *A directive to the Secretary of Defense*. This directive shall include the following provisions:

a. Subject to the specific provisions of this directive, the Secretary of Defense may delegate in whole of in part authority over the Director of NSA within his department as he sees fit.

b. The COMINT mission of the National Security Agency (NSA) shall be to provide an effective, unified organization and control of the communications intelligence activities of the United States conducted against foreign governments, to provide for integrated operational policies and procedures pertaining thereto. As used in this directive, the terms communications intelligence or COMINT shall be construed to mean all procedures and methods used in the interception of communications other than foreign press and propaganda broadcasts and the obtaining of information from such communications by other than intended recipients, but shall exclude censorship and the production and dissemination of finished intelligence.

c. NSA shall be administered by a Director, designated by the Secretary of Defense after consultation with the Joint Chiefs of Staff, who shall serve for a minimum term of 4 years and who shall be eligible for reappointment. The Director shall be a career commissioned officer of the armed services on active or reactivated status, and shall enjoy at least 3-star rank during the period of his incumbency.

d. Under the Secretary of Defense, and in accordance with approved policies of USCIB, the Director of NSA shall be responsible for accomplishing the mission of NSA. For this purpose all COMINT collection and production resources of the United States are placed under his operational and technical control. When action by the Chiefs of the operating agencies of the Services or civilian departments or agencies is required, the Director shall normally issue instruction pertaining to COMINT operations through them. However, due to the unique technical character of COMINT operations, the Director is authorized to issue direct to any operating elements under his operational control task assignments and pertinent instructions which are within the capacity of such elements to accomplish. He shall also have direct access to, and direct communication with, any elements of the Service or civilian COMINT agencies on any other matters of operational and technical control as may be necessary, and he is authorized to obtain such information and intelligence material from them as he may require. All instruction issued by the Director under the authority provided in this

paragraph shall be mandatory, subject only to appeal to the Secretary of Defense by the Chief of Service or head of civilian department of agency concerned.

e. Specific responsibilities of the Director of NSA include the following:

(1) Formulating necessary operational plans and policies for the conduct of the U.S. COMINT activities.

(2) Conducting COMINT activities, including research and development, as required to meet the needs of the departments and agencies which hare authorized to receive the products of COMINT.

(3) Determining, and submitting to appropriate authorities, requirements for logistic support for the conduct of COMINT activities, together with specific recommendations as to what each of the responsible departments and agencies of the Government should supply.

(4) Within NSA's field of authorized operations prescribing requisite security regulations covering operating practices, including the transmission, handling and distribution of COMINT material within and among the COMINT elements under his operations or technical control; and exercising the necessary monitoring and supervisory control, including inspections if necessary, to ensure compliance with the regulations.

(5) Subject to the authorities granted the Director Central Intelligence under NSCID No. 5, conducting all liaison on COMINT matters with foreign governmental communications intelligence agencies.

f. To the extent he deems feasible and in consonance with the aims of maximum over-all efficiency, economy, and effectiveness, the Director shall centralize or consolidate the performance of COMINT functions for which he is responsible. It is recognized that in certain circumstances elements of the Armed Forces and other agencies being served will require close COMINT support. Where necessary for this close support, direct operational control of specified COMINT facilities and resources will be delegated by the Director, during such periods and for such tasks as are determined by him, to military commanders or to the Chiefs of other agencies supported.

g. The Director shall exercise such administrative control over COMINT activities as he deems necessary to the effective performance of his mission. Otherwise, administrative control of

personnel and facilities will remain with the departments and agencies providing them.

h. The Director shall make provision for participation by representatives of each of the departments and agencies eligible to receive COMINT products in those offices of NSA where priorities of intercept and processing are finally planned.

i. The Director shall have a civilian deputy whose primary responsibility shall be to ensure the mobilization and effective employment of the best available human and scientific resources in the field of cryptographic research and development.

j. Nothing in this directive shall contravene the responsibilities of the individual departments and agencies for the final evaluation of COMINT information, its synthesis with information from other sources, and the dissemination of finished intelligence to users.

3. The special nature of COMINT actives requires that they be treated in all respects as being outside the framework of other or general intelligence activities. Order, directives, policies, or recommendations of any authority of the Executive Branch relating to the collection, production, security, handling, dissemination, or utilization of intelligence, and/or classified material, shall not be applicable to COMINT actives, unless specifically so stated and issued by competent departmental of agency authority represented on the Board. Other National Security Council Intelligence Directive to the Director of Central Intelligence and related implementing directives issued by the Director of Central Intelligence shall be construed as non-applicable to COMINT activities, unless the National Security Council has made its directive specifically applicable to COMINT.

/s/ HARRY S TRUMAN

APPENDIX B

Introduction to Compromising Emanations

Intercepting the compromising emanations from electronic equipment is referred to as ELINT/CE.[144] With current ELINT/CE technology it is possible to reconstruct the contents of computer video display terminal (VDU) screens from up to a kilometer away; reconstructing the contents of a computer's memory or the contents of its mass storage devices is more complicated and must be performed from a lesser distance.[145]

The reconstruction of information from CE is not limited to computers and digital devices but is applicable to all electronic devices.[146] However, ELINT/CE is especially effective against VDUs because they produce a very high level of EMR.[147]

According to the National Security Agency, which is charged with

---

144 The actual short name used by the National Security Agency to refer to ELINT/CE has not been released. We will use our own short name: ELINT/CE. ELINT is the acronym for ELectronic INTelligence and CE is the acronym for Compromising Emanations.

145 TEMPEST is concerned with the transient electromagnetic pulses formed by digital equipment. All electronic equipment radiates electro magnetic radiation ("EMR") which may be reconstructed. Digital equipment processes information as 1's and 0's — *on's or off's*. Because of this, digital equipment gives off pulses of EMR. These pulses are easier to reconstruct at distance than the non-pulse EMR given off by analog equipment. For a thorough discussion of the radiation problems of broadband digital information *see* D. WHITE & M. MARDIGUIAN, EMI CONTROL METHODOLOGY AND PROCEDURES, § 10.2 (4th ed. 1985). [hereinafter WHITE & MARDIGUIAN].

"[E]mission levels are expressed in the time and frequency domain, broadband or narrowband in terms of the frequency domain, and in terms of conducted or radiated emissions." *Id.* at § 10.1.

146 Of special interest to ELINT collectors are CE from computers, communications centers and avionics. S. Schultz, *supra* note 31, at 181.

147 The picture on a CRT screen is built up of picture elements (pixels) organized in lines across the screen. The pixels are made of material that fluoresces when struck with energy. The energy is produced by a beam of electrons fired from an electron gun in the back of the picture tube. The electron beam scans the screen of the CRT in a regular repetitive manner. When the voltage of the beam is high the pixel it is focused upon emits photons and appears as a dot on the screen. By selectively firing the gun as it scans across the face of the CRT, the pixels form characters on the CRT screen.

The pixels glow for only a very short time and must be routinely struck by the electron beam to stay lit. To maintain the light output of all the pixels that are supposed to be lit, the electron beam traverses the entire CRT screen sixty times a second. Every time the beam fires it causes a high voltage EMR emission. This EMR can be used to reconstruct the contents of the target CRT screen.

ELINT/CE equipment designed to reconstruct the information on a CRT screen intercepts the EMR from the target's video circuitry. The synchronization (sync) signals from the target CRT are normally too faint to be detected at a distance. Therefore, the ELINT/CE unit injects fresh sync signals into the intercepted EMR. These sync signals are tuned until the ELINT/CE's electron gun is in sync with the electron gun of the target CRT.

When the ELINT/CE unit detects EMR indicating that the target CRT fired on a pixel, the unit fires the electron gun of its CRT. The ELINT/CE CRT is in perfect synchronism with the target CRT; when the target lights a pixel, a corresponding pixel on the ELINT/CE CRT is lit. The

protecting United States government communications and intercepting the communications of other nations[148], information . . . which is generated, processed, or transferred by electrical, electronic, and electromechanical equipments is subject to compromise because of unintentional electromagnetic radiated and conducted emanations.[149] Emanations which cannot be detected cannot be analyzed to obtain information; they are therefore not a security threat.[150]

---

exact picture on the target CRT will appear on the ELINT/CE CRT. Any changes on the target screen will be instantly reflected in the surveillance screen.

For a thorough discussion of CRT ELINT/CE *see* Van Eck, *supra* note 32.

[148] The COMINT mission of the National Security Agency (NSA) shall be to provide an effective, unified organization and control of the communications intelligence activities of the United States conducted against foreign governments, to provide for integrated operational policies and procedures pertaining thereto. As used in this directive, the terms "communications intelligence" or "COMINT" shall be construed to mean all procedures and methods used in the interception of communications other than foreign press and propaganda broadcasts and the obtaining of information from such communications by other than intended recipients, [] but shall exclude censorship and the production and dissemination of finished intelligence . . . the Director of NSA shall be responsible for accomplishing the mission of NSA. For this purpose all COMINT collection and production resources of the United States are placed under his operational and technical control.

Memorandum from President Harry S. Truman to the Secretary of State and the Secretary of Defense, 5-6 (Oct. 24, 1952) (establishing the National Security Agency).

This memorandum has never before been released to the public in its entirety. It is set out in Appendix A.

[149] NACSIM 5100A, *supra* note 145, at iii.

There are two types of emissions, conducted and radiated. Radiated emissions are formed when components or cables act as antennas for transmitting the EMR; when radiation is conducted along cables or other connections but not radiated it is referred to as conducted. Sources include cables, the ground loop, printed circuit boards, internal wires, the power supply to power line coupling, the cable to cable coupling, switching transistors, and high-power amplifiers.

WHITE & MARDIGUIAN, *supra* note 145, at § 10.1.

[C]ables may act as an antenna to transmit the signals directly or even both receive the signals and re-emit them further away from the source equipment. It is possible that cables acting as an antenna in such a manner could transmit the signals much more efficiently than the equipment itself . . . A similar effect may occur with metal pipes such as those for domestic water supplies . . . If an earthing [grounding] system is not installed correctly such that there is a path in the circuit with a very high resistance (for example where paint prevents conduction and is acting as an insulator), then the whole earthing system could well act in a similar fashion to an antenna . . . [For a VDU] the strongest signals, or harmonics thereof, are usually between 60-250 MHz approximately. There have however been noticeable exception of extremely strong emissions in the television bands and at higher frequencies between 450-800 MHz.

Potts, *Emissions Security*, 3 COMPUTER L. & SEC. REP. 27 (1988). TEMPEST emanations are assumed to be either direct baseband emanations, impulsive emanations, or double sideband amplitude modulation. NACSIM 5100A, *supra* note 14, at 1-1.

[150] Threat: Any circumstance or event with the potential to cause harm . . . in the form of . . . disclosure . . . of data. A threat is a potential for harm. The presence of a threat does not mean that it will necessarily cause actual harm. Threats exist because of the very existence of the system or activity and not because of any specific weakness.

ADP SECURITY, *supra* note 13, at A-14.

Detected emanations may be classed into two broad groups, those that are correlatable (CORR E) and those that are non-correlatable. Emanations which yield information after analysis are correlatable, those that yield no information are non-correlatable.[151]

Correlatable emanations consist of three sub-groups: Data related emanations, compromising emanations, and undesired signal data emanations. Data related emanations (DRE) are limited to correlated emanations which are not compromising. That is, analysis of DRE will not yield useful information.[152] "Compromising emanations [CE] are unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose . . . information transmitted, received, handled, or otherwise processed by any information-processing equipment."[153]

CE limits are set forth in NACSIM 5100A.[154] "[The] document specifies test procedures for identifying the conducted and electromagnetic radiation emanations characteristics of individual equipments in a laboratory environment."[155] Equipments meeting the limits [set forth in NACSIM 5100A] provide an acceptable degree of conducted and radiated TEMPEST security at the equipment level."[156]

> The emanation limits [set forth in NACSIM 5100A, Appendix H] constitute a set of reference curves which are intended for use:
>
> a. As a guide for determining a contractual measure for acceptability, or as a performance objective in preparing specifications for newly developed equipments, and
>
> b. As a standard to compare the TEMPEST profiles of different equipments.[157]

CE above the limits set forth in NACSIM 5100A is considered undesired signal data emanations (USDE).[158]

---

151 NACSIM 5100A, *supra* note 14, at 5-1.

In laymen's terms, correlatable emanations are ones from which information can be extracted through analysis. To oversimplify, if your electronic typewriter puts out one type of signal when you type "a" and another for "b" and so forth for all the keys, then these emanations are correlatable because they can be used to determine what you were typing.

152 *Id.*

153 *Id.* at 2-1.

In laymen's terms, compromising emanations that will yield information is analyzed. We used an electronic type writer in a previous example; *see supra* note 153. The emanations in that example were compromising because analysis would reveal what was being typed.

154 "Equipments and systems to which the requirements of this document are levied shall not emit compromising emanations that exceed the applicable limits specified herein." NACSIM 5100A, *supra* note 14, at 2-1.

155 *Id.*

156 *Id.*

157 *Id.*

158 *Id.* at 6-3.

In laymen's terms, USDE are bad because they are strong enough to be picked up by

Specifically, USDE includes electromagnetic radiation and BLACK line[s][159] which exceed the applicable limits. "For RED signal line[s] . . . USDE refers to any portion of the measured signal spectrum which exceeds the RED signal line limits and from which the RED data can be recovered."[160]

Equipment that is tested and certified as conforming to NACSIM 5100A is referred to as TEMPEST certified equipment.[161] Producing TEMPEST Certified equipment is expensive; to encourage the availability of off-the-shelf TEMPEST Certified equipment the NSA maintains a list of equipment that is TEMPEST certified. When a government agency or activity requires TEMPEST Certified equipment they may purchase directly from this list rather than contracting to have the equipment redesigned to meet NACSIM 5100A.[162]

ELINT/CE surveillance equipment. If the signals are compromising but are too weak to be detected at a distance they are not a threat—if they cannot be detected they cannot be analyzed.

This has led to a revision of the TEMPEST standard as detection equipment has become more sophisticated. This could be considered akin to the arms race. As more sophisticated ELINT equipment is built, the TEMPEST standard must be updated to limit CE below the limits the new equipment can detect; as the TEMPEST standard is updated, installed TEMPEST Certified equipment must be retrofitted to harmonize with the updated standard and new equipment must be manufactured. As this happens, new and more sensitive ELINT equipment is built to eavesdrop on the updated equipment.

159 *Id.* at 5-1. BLACK lines contain only enciphered information (cyphertext). UNITED STATES DEPARTMENT OF DEFENSE: DATA NETWORK, BLACKER INTERFACE CONTROL DOCUMENT § 1.0.1 (1989)[hereinafter BLACKER].

160 NACSIM 5100A, *supra* note 14, at 5-1. RED lines carry plain text information. BLACKER, *supra* note 159, at § 1.0.1.

> Primary RED lines are those which intentionally carry RED signals. Secondary RED lines are non-RED signals lines (clock, control) which originate or terminate in the same electrical interfaces as or share the same cable with any RED signal line . . . RED Signal Source [is] [a]ny circuit or circuit element, through which a RED signal is fed, which causes a change in signal current with respect to time (di/dt). . . . RED Signal Type [is] [t]he characterization of a RED signal by the following features: code, format, parity, whether serial or parallel, whether repetitive or non-repetitive, the number of bytes simultaneously processed, and whether baseband or a form of modulation or multiplexing.

NACSIM 5100A, *supra* note 14, at 4-2.

161 The limits set forth in NACSIM 5100A apply solely to individual pieces of equipment. TEMPEST certified equipment may produce USDE when placed with other equipment or under certain environmental conditions. [This] may have a significant effect on TEMPEST security when judged at the system or field-site level. Such considerations are beyond the scope of [NACSIM 5100A].

Id. at 1-1.

162 Shearin, *supra* note 35, at 55.

> The Industrial TEMPEST Program (ITP) was established to allow industry to respond to Government's need for off-the-shelf TEMPEST equipment. It provides an alternative to awarding specific contracts for each individual TEMPEST equipment required. First, a company completes an ITP application indicating its intent to invest company funds in the production of TEMPEST equipment and if the application is accepted, a voluntary agreement called a Memorandum of Understanding (MOU) is signed which forms the corner-

Information regarding compromising emanations is restricted.[163] The information is available strictly on a need-to-know basis.

---

stone of the ITP. Once the MOU is signed and the company has met U.S. ownership and security clearance qualifications, the ITP provides the National TEMPEST Standard and other supporting documentation.

Id.

The goal of each ITP company is to combine its technical expertise with the classified documentation to design an equipment that receives government accreditation and is listed on the Preferred Products List (PPL). The PPL contains equipment which has met the criteria of NACSIM 5100A and has been reviewed and approved by the TEMPEST Qualification Special Committee (TQSC).

Id. at 56.

In April 1988 the National Security Agency's Industrial TEMPEST Program (ITP) was restructured into the TEMPEST Endorsement Program which comprises the Endorsed TEMPEST Products Program (ETPP), the Endorsed TEMPEST Test Services Program (ETTSP), and the Endorsed TEMPEST Test Instrumentation Program (ETTIP). The decision to restructure the ITP was based on increasing concern regarding the security integrity of the products placed on the Preferred Products Lists (PPL). The new emphasis will be individual product or service endorsement, vice company membership, and active involvement of NSA technical resources in the evaluation and subsequent post endorsement product assurance processes.

Letter from National Security Agency Public Affairs Office to author (Feb. 1990).

NSA endorsement is a statement that the company has successfully demonstrated to NSA that its product complies with the requirements of the National TEMPEST Standard, NACSIM 5100A and that the product manufacturer has in place and applies to the product, the manufacturing capability and product assurance controls necessary to ensure the continued TEMPEST integrity of the product subsequent to endorsement.

Id.

A new National TEMPEST policy, NTISSP 300, was enacted in October 1988. The thrust of this classified policy is to provide government departments and agencies with a series of options to solve their TEMPEST security needs. This new policy mandates that government departments and agencies only buy TEMPEST protection proportionate to the security requirements of that department of agency. It is anticipated that the policy will result in a significant reduction in the overall cost of TEMPEST to the government.

Id.

[163] The Director, National Security Agency, has responsibility for providing guidance on security classification and control of information pertaining to compromising emanations including the releasibility of this information to foreign nations. . . .

It may be necessary to assign higher levels of classification to specific categories of compromising emanations information depending on such factors as: (a) the widespread usage of a particular equipment or system used to process classified information; (b) the geopolitical location of a specific operational site used to process classified information; (c) the level or sensitivity of the traffic being processed by a particular equipment, system or site; and (d) the severity of the [TEMPEST] problem associated with a particular equipment, system or site.

NATIONAL SECURITY AGENCY, NATIONAL COMMUNICATIONS SECURITY INFORMATION (NACSI) 4003: CLASSIFICATION GUIDELINES FOR COMSEC INFORMATION C-1, C-2 (1978)[hereinafter NACSI 4003].

NACSIM 5100A is COMSEC (communications security) material. "Access by contractor personnel is limited to U.S. citizens holding final government clearances." NACSIM 5100A, *supra* note 14, at title page. NACSIM 5100A may not be disclosed or released by any holder without approval of the "Director, NSA [or the] Chief, CSS [(Central Security Service)]." *Id.* Nor may it be released

> Unclassified information concerning compromising emanations shall not be discussed or made available to persons without a need-to-know, especially when the aggregate of unclassified information could be combined to reveal classified information. No person is entitled to knowledge or possession of, or access to, information concerning compromising emanations solely because of his office, position or type of clearance.[164]

Limited information is available to firms producing TEMPEST equipment for the government. These firms must be owned by United States citizens and pass a review by the Defense Investigation Service.[165] Contractors are required to submit to prepublication review.[166] In addition, they are discouraged from discussing TEMPEST with anyone, especially the press.[167]

---

to foreign nationals without "PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NATIONAL SECURITY AGENCY." *Id.* at i (emphasis in original).

164 NACSI 4003, *supra* note 163, at C-2.

165 TEMPEST information can be obtained either through a classified government contract or under the auspices of the National Security Agency's Industrial TEMPEST Program (ITP).

* * *

> [D]istribution of [NACSIM 5100A] is made through the sponsoring agency's contracting officer. The proper clearances and storage capability are obtained when the contracting agency sponsors a company to the U.S. Defense Investigation Service (DIS), which issues a facility clearance for the company and individual clearances for employees who will be involved with the classified contract. When TEMPEST requirements have been levied in a contract and clearances have been issued, classified TEMPEST information is released to the contractor.

Shearin, *supra* note 35, at 55.

166 All TEMPEST assistance is rendered by the contracting agency, including technical support and the prepublication review of any proposed dissemination of TEMPEST information. The control and distribution of classified TEMPEST information is a contractual requirement.

Id.

For a discussion of prior restraint and national security as they relate to the First Amendment, *see* cases cited *supra* note 39.

For a general discussion of the First Amendment and national security, *see* sources cited *supra* note 39.

167 "[W]e are very sensitive to TEMPEST exposure in the media, educational seminars, or industrial trade shows . . . we must continue to work together . . . towards ensuring the inviolability" of the newest frontiers of [TEMPEST information]." Shearin, *supra* note 35, at 75.

"[W]e challenge both Government and industry to restrict TEMPEST inquiries and information to established classified channels." Shearin, *supra* note 35, at 55.

"No information related to compromising emanations shall be released for public consumption through the press, advertising, radio, TV or other public media." NACSI 4003, *supra* note 163, at C-2.