Eavesdropping On the Electromagnetic Emanations of Digital Equipment: The Laws of Canada, England and the United States

This document is a rough draft. The Legal Sections are overviews. They will be significantly expanded in the next version.

> We in this country, in this generation, are -- by destiny rather than choice -- the watchmen on the walls of world freedom. [1]
>
> -- President John F. Kennedy

In the novel 1984, George Orwell foretold a future where individuals had no expectation of privacy because the state monopolized the technology of spying. The government watched the actions of its subjects from birth to death. No one could protect himself because surveillance and counter-surveillance technology was controlled by the government.

This note explores the legal status of a surveillance technology ruefully known as TEMPEST [2]. Using TEMPEST technology the information in any digital device may be intercepted and reconstructed into useful intelligence without the operative ever having to come near his target. The technology is especially useful in the interception of information stored in digital computers or displayed on computer terminals.

The use of TEMPEST is not illegal under the laws of the United States [3], or England. Canada has specific laws criminalizing TEMPEST eavesdropping but the laws do more to hinder surveillance countermeasures than to prevent TEMPEST surveillance. In the United States it is illegal for an individual to take effective counter-measures against TEMPEST surveillance. 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 would like to suggest that the solution to this conundrum is straightforward. Information on protecting privacy under TEMPEST should be made freely available; TEMPEST Certified equipment should be legally available; and organizations possessing private information should be required by law to protect that information through good computer security practices and the use of TEMPEST Certified equipment.

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 opera-

tives, and ELINT relies on technological operatives. In the past HUMINT was the sole method for collecting intelligence. [4] The HUMINT operative would steal important papers, observe troop and weapon movements [5], lure people into his confidences to extract secrets, and stand under the eavesdrip [6] 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. So it has been with spying. 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. 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.

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

ELINT devices 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. The trespass comes either when it is physically attached to the phone line, or if it is inductive, when placed in close proximity to the phone line. Even microwave bugs require the placement of the resonator cone within the target premises. [7]

Non-trespassatory ELINT devices work by receiving electromagnetic radiation (EMR) as it radiates through the aether, and do not require the placement of bugs. Methods include intercepting [8] information transmitted by satellite, microwave, and radio, including mobile and cellular phone transmissions. This information was purposely transmitted with the intent that some intended person or persons would receive it.

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. [9] This information can be intercepted and reconstructed into a coherent form. With current TEMPEST technology it is possible to reconstruct the contents of computer video display terminal (VDU) screens from up to a kilometer distant [10]; 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 closer distance. [11] The reconstruction of information via EMR, a process for which the United States government refuses to declassify either the exact technique or even its name [12], is not limited to computers and digital devices but is applicable to all devices that generate electromagnetic radiation. [13] TEMPEST is especially effective against VDUs because they produce a very high level of EMR. [14]

"[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, Emission Security, 3 COMPUTER LAW AND SECURITY REPORT 27 (1988).

ELINT is not limited to governments. It is routinely used by individuals for their own purposes. Almost all forms of ELINT are available to the individual with either the technological expertise or the money to hire someone with the expertise. Governments have attempted to criminalize all use of ELINT by their subjects -- to protect the privacy of both the government and the population.

In the United States, Title III of the Omnibus Streets and Crimes Act of 1968 [15] criminalizes trespassatory ELINT as the intentional interception of wire communications. [16] As originally passed, Title III did not prohibit non-trespassatory ELINT, [17] because courts found that non-wire communication lacked any expectation of privacy. [18] The Electronic Communications Privacy Act of 1986 [19] amended Title III to include non-wire communication. ECPA was specifically designed to include electronic mail, inter-computer communications, and cellular telephones. To accomplish this, the expectation of privacy test was eliminated. [20]

As amended, Title III still outlaws the electronic interception of communications. The word "communications" indicates that someone

is attempting to communicate something to someone; it does not refer to the inadvertent transmission of information. The reception and reconstruction of emanated transient electromagnetic pulses (ETEP), however, is based on obtaining information that the target does not mean to transmit. If the ETEP is not intended as communication, and is therefore not transmitted in a form approaching current communications protocols, then it can not be considered communications as contemplated by Congress when it amended Title III. Reception, or interception, of emanated transient electromagnetic pulses is not criminalized by Title III as amended.

In England the Interception of Communications Act 1985 [21] criminalizes the tapping of communications sent over public telecommunications lines. [22] 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. [23] These forms of passive interception differ from TEMPEST ELINT because they are intercepting intended communication; TEMPEST ELINT intercepts unintended communication. Eavesdropping on the emanations of computers does not in any way comport to tapping a telecommunication line and therefore falls outside the scope of the statute. [24]

Canada has taken direct steps to limit eavesdropping on computers. The Canadian Criminal Amendment Act of 1985 criminalized indirect access to a computer service. [25] The specific reference to an "electromagnetic device" clearly shows the intent of the legislature to include the use of TEMPEST ELINT equipment within the ambit of the legislation.

The limitation of obtaining "any computer service" does lead to some confusion. The Canadian legislature has not made it clear whether "computer service" refers to a computer service bureau or merely the services of a computer. If the Canadians had meant access to any computer, why did they refer to any "computer service". This is especially confusing considering the all-encompassing language of (b) 'any function of a computer system'.

Even if the Canadian legislation criminalizes eavesdropping on all computers, it does not solve the problem of protecting the privacy of information. The purpose of criminal law is to control crime. [26] Merely making TEMPEST ELINT illegal will not control its use. First, because it is an inherently passive crime it is impossible to detect and hence punish. Second, making this form of eavesdropping illegal without taking a proactive stance in controlling compromising emanations gives the public a false sense of security. Third, criminalizing the possession of a TEMPEST ELINT device prevents public sector research into countermeasures. Finally, the law will not prevent eavesdropping on private information held in company computers unless disincentives are given for companies that do not take sufficient precautions against eavesdropping and simple, more common, information crimes. [27]

TEMPEST ELINT is passive. The computer or terminal emanates compromising radiation which is intercepted by the TEMPEST device and reconstructed into useful information. Unlike conventional ELINT there is no need to physically trespass or even come near the target. Eavesdropping can be performed from a nearby office or even a van parked within a reasonable distance. This means that there is no classic scene of the crime; and little or no chance of the criminal being discovered in the act. [28]

If the crime is discovered it will be ancillary to some other investigation. For example, if an individual is investigated for insider trading a search of his residence may yield a TEMPEST ELINT device. The device would explain how the defendant was obtaining insider information; but it was the insider trading, not the device, that gave away the crime.

This is especially true for illegal TEMPEST ELINT performed by the state. Unless the perpetrators are caught in the act there is little evidence of their spying. A trespatory bug can be detected and located; further, once found it provides tangible evidence that a crime took place.

A TEMPEST ELINT device by its inherent passive nature leaves nothing to detect. Since the government is less likely to commit an ancillary crime which might be detected there is a very small chance that the spying will ever be discovered. The only way to prevent eavesdropping is to encourage the use of countermeasures: TEMPEST Certified [29] computers and terminals.

In merely making TEMPEST ELINT illegal the public is given the false impression of security; they lulled into believing the problem has been solved. Making certain actions illegal does not prevent them from occurring. This is especially true for a TEMPEST ELINT because it is undetectable. Punishment is an empty threat if there is no chance of being detected; without detection there can be no apprehension and conviction. The only way to prevent some entity from eavesdropping on one's computer or computer terminal is for the equipment not to give off compromising emanation; it must be TEMPEST Certified.

The United States can solve this problem by taking a proactive stance on compromising emanations. The National Institute of Standards and Technology (NIST [30]) is in charge of setting forth standards of computer security for the private sector. NIST is also charged with doing basic research to advance the art of computer security. Currently NIST does not discuss TEMPEST with the private sector. For privacy's sake, this policy must be changed to a proactive one. The NIST should publicize the TEMPEST ELINT threat to computer security and should set up a rating system for level of emanations produced by computer equipment. [31]

Further, legislation should be enacted to require the labeling of all computer equipment with its level of emanations and whether it

is TEMPEST Certified. Only if the public knows of the problem can it begin to take steps to solve it.

Title III makes possession of a surveillance device a crime, unless it is produced under contract to the government. This means that research into surveillance and counter-surveillance equipment is monopolized by the government and a few companies working under contract with the government. If TEMPEST eavesdropping is criminalized, then possession of TEMPEST ELINT equipment will be criminal. Unfortunately,this does not solve the problem. Simple TEMPEST ELINT equipment is easy to make. For just a few dollars many older television sets can be modified to receive and reconstruct EMR. For less than a hundred dollars a more sophisticated TEMPEST ELINT receiver can be produced. [32]

The problem with criminalizing the possession of TEMPEST ELINT equipment is not just that the law will have little effect on the use of such equipment, but that it will have a negative effect on counter-measures research. To successfully design counter-measures to a particular surveillance technique it is vital to have a complete empirical understanding of how that technique works. Without the right to legally manufacture a surveillance device there is no possible way for a researcher to have the knowledge to produce an effective counter-measures device. It is axiomatic: without a surveillance device, it is impossible to test a counter-measures device.

A number of companies produce devices to measure the emanations from electrical equipment. Some of these devices are specifically designed for bench marking TEMPEST Certified equipment. This does not solve the problem. The question arises: how much radiation at a particular frequency is compromising? The current answer is to refer to NACSIM 5100A. This document specifies the emanations levels suitable for Certification. The document is only available to United States contractors having sufficient security clearance and an ongoing contract to produce TEMPEST Certified computers for the government. Further, the correct levels are specified by the NSA and there is no assurance that, while these levels are sufficient to prevent eavesdropping by unfriendly operatives, equipment certified under NACSIM 5100A will have levels low enough to prevent eavesdropping by the NSA itself.

The accessibility of supposedly correct emanations levels does not solve the problem of preventing TEMPEST eavesdropping. Access to NACSIM 5100A limits the manufacturer to selling the equipment only to United States governmental agencies with the need to process secret information. [33] Without the right to possess TEMPEST ELINT equipment manufacturers who wish to sell to the public sector cannot determine what a safe level of emanations is.

Further those manufacturers with access to NACSIM 5100A should want to verify that the levels set out in the document are, in fact, low enough to prevent interception. Without an actual

eavesdropping device with which to test, no manufacturer will be able to produce genuinely uncompromising equipment.

Even if the laws allow ownership of TEMPEST Certified equipment by the public, and even if the public is informed of TEMPEST's threat to privacy, individuals' private information will not necessarily by protected. Individuals may choose to protect their own information on their own computers. Companies may choose whether to protect their own private information. But companies that hold the private information of individuals must be forced to take steps to protect that information.

In England the Data Protection Act 1984 [34] imposes sanctions against anyone who stores the personal information [35] 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 [36] has registered under the act. [37] 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 provides tort remedies to any person who is damaged by disclosure of the personal data. [38] Reasonable care to prevent the disclosure is a defense. [39] English courts have not yet ruled what level of computer security measures constitute reasonable care. Considering the magnitude of invasion possible with TEMPEST ELINT it should be clear by now that failure to use TEMPEST Certified equipment is prima facie unreasonable care.

The Remedies section of the act provides incentive for these entities to provide successful protection of person data from disclosure or illicit access. Failure to protect the data will result in monetary loss. This may be looked at from the economic efficiency viewpoint as allocating the cost of disclosure the persons most able to bear those costs, and also most able to prevent disclosure. Data users that store personal data would use TEMPEST Certified equipment as part of their computer security plan, thwarting would-be eavesdroppers.

The Data Protection Act 1984 allocates risk to those who can bear it best and provides an incentive for them to keep other individuals' data private. This act should be adopted by the United States as part of a full-spectrum plan to combat TEMPEST eavesdropping. Data users are in the best position to prevent disclosure through proper computer security. Only by making them liable for failures in security can we begin to rein in TEMPEST ELINT. Do not criminalize TEMPEST ELINT. Most crimes that TEMPEST ELINT would aid, such a insider trading, are already illegal; the current laws are adequate.

The National Institute of Standards and Technology should immediately begin a program to educate the private sector about TEMPEST.

Only if individuals are aware of the threat can they take appropriate precautions or decide whether any precautions are necessary.

Legislation should be enacted to require all electronic equipment to prominently display its level of emanations and whether it is TEMPEST Certified. If individuals are to choose to protect themselves they must be able to make a informed decision regarding how much protection is enough.

TEMPEST Certified equipment should be available to the private sector. The current ban on selling to non-governmental agencies prevents individuals who need to protect information from having the technology to do so.

Possession of TEMPEST ELINT equipment should not be made illegal. The inherently passive nature and simple design of TEMPEST ELINT equipment means that making its possession illegal will not deter crime; the units can be easily manufactured and are impossible to detect. Limiting their availability serves only to monopolize the countermeasures research, information, and equipment for the government; this prevents the testing, design and manufacture of counter-measures by the private sector.

Legislation mirroring England's Data Protection Act 1984 should be enacted. Preventing disclosure of personal data can only be accomplished by giving those companies holding the data a reason to protect it. If data users are held liable for their failure to take reasonable security precautions they will begin to take reasonable security precautions, including the use of TEMPEST Certified equipment.

---

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

2. TEMPEST is an acronym for Transient Electromagnetic Pulse Emanation Standard. This standard sets forth the official views of the United States on the amount of electromagnetic radiation that a device may emit without compromising the information it is processing. TEMPEST is a defensive standard; a device which conforms to this standard is referred to as TEMPEST Certified. The United States government has refused to declassify the acronym for devices used to intercept the electromagnetic information of non-TEMPEST Certified devices. For this note, these devices and the technology behind them will also be referred to as TEMPEST; in which case, TEMPEST stands for Transient Electromagnetic Pulse Surveillance Technology. The United States government refuses to release details regarding TEMPEST and continues an organized effort to censor the dissemination of information about it. For example the NSA succeeded in shutting down a Wang Laboratories presentation on TEMPEST Certified equipment by classifying the contents of the speech and threat-

ening to prosecute the speaker with revealing classified information. [cite coming]

3. This Note will not discuses how TEMPEST relates to the Warrant Requirement under the United States Constitution. Nor will it discuss the Constitutional exclusion of foreign nationals from the Warrant Requirement.

4. HUMINT has been used by the United States since the Revolution. "The necessity of procuring good intelligence is apparent and 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 and promising a favorable issue." Letter of George Washington (Jul. 26, 1777).

5. "... 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 and numbers -- what kind of Troops they are, and what Guards they have -- their strength and where posted." Id.

6. 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 (1977).

7. Pursglove, How Russian Spy Radios Work, RADIO ELECTRONICS, 89-91 (Jan 1962).

8. 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.

9. There are two types of emissions, conducted and radiated. Radiated emissions are formed when components or cables act as antennas for transmit 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.

10. The TEMPEST ELINT operator can distinguish between different VDUs in the same room because of the different EMR characteristics of both homo and heterogeneous units. "[T]here is little comparison between EMR characteristics from otherwise comparable equipment. Only if the [VDU] was made with exactly the same components is there any similarity. If some of the components have come from a different batch, have been updated in some way, and especially if they are from a different manufacturer, then completely different results are obtained. In this way a different mark or version of the same [VDU] will emit different signals. Additionally because of the variation of manufacturing standards between counties, two [VDUs] made by the same company but sourced from different counties will have entirely different EMR signal characteristics... From this it way be thought that there is such a jumble of emissions around, that it would

not be possible to isolate those from any one particular source. Again, this is not the case. Most received signals have a different line synchronization, due to design, reflection, interference or variation of component tolerances. So that if for instance there are three different signals on the same frequency ... by fine tuning of the RF receiver, antenna manipulation and modification of line synchronization, it is possible to lock onto each of the three signals separately and so read the screen information. By similar techniques, it is entirely possible to discriminate between individual items of equipment in the same room." Potts, supra note 9. For a discussion of the TEMPEST ELINT threat see e.g., Memory Bank, AMERICAN BANKER 20 (Apr 1 1985); Emissions from Bank Computer Systems Make Eavesdropping Easy, Expert Says, AMERICAN BANKER 1 (Mar 26 1985); CRT spying: a threat to corporate security, PC WEEK (Mar 10 1987).

11. TEMPEST is concerned with the transient electromagnetic pulses formed by digital equipment. All electronic equipment radiates 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 a distance than the non-pulse EMR given off by analog equipment. For a thorough discussion the radiation problems of broadband digital information see e.g. military standard MIL-STD-461 REO2; White supra note 9, 10.2.

12. See supra note 2.

13. Of special interest to ELINT collectors are EMR from computers, communications centers and avionics. Schultz, Defeating Ivan with TEMPEST, DEFENSE ELECTRONICS 64 (June 1983).

14. The picture on a CRT screen is built up of picture elements (pixels) organized in lines across the screen. The pixels are made of materi- al 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 then 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. TEMPEST ELINT equipment designed to reconstruct the information synchronizes its CRT with the target CRT. First, it uses the EMR to synchronize its electron gun with the electron gun in the target CRT. Then, when the TEMPEST ELINT unit detects EMR indicating that the target CRT fired on a pixel, the TEMPEST ELINT unit fires the electron gun of its CRT. The ELINT CRT is in perfect synchronism with the target CRT; when the target lights a pixel, a corresponding pixel on the TEMPEST ELINT CRT is lit. The exact picture on the target CRT will appear on the TEMPEST ELINT CRT. Any changes on the target screen will be instantly reflected in the TEMPEST ELINT screen. TEMPEST Certified equipment gives off emissions levels that are too faint to be readily detected. Certification levels are set out in National Communications Security Information Memorandum 5100A (NACSIM 5100A). "[E]mission levels are expressed in the time and frequency domain, broadband or narrow band in terms of the frequency

domain, and in terms of conducted or radiated emissions." White, supra, note 9, 10.1. For a thorough though purposely misleading discussion of TEMPEST ELINT see Van Eck, Electromagnetic Radiation from Video Display units: An Eavesdropping Risk?, 4 Computers & Security 269 (1985).

15. Pub. L. No. 90-351, 82 Stat. 197. The Act criminalizes trespassatory ELINT by individuals as well as governmental agents. cf. Katz v. United States, 389 U.S. 347 (1967) (Fourth Amendment prohibits surveillance by government not individuals.)

16. 18 U.S.C. 2511(1)(a).

17. United States v. Hall, 488 F.2d 193 (9th Cir. 1973) (found no legislative history indicating Congress intended the act to include radio-telephone conversations). Further, Title III only criminalized the interception of "aural" communications which excluded all forms of computer communications.

18. Willamette Subscription Television v. Cawood, 580 F.Supp 1164 (D. Or. 1984) (non-wire communications lacks any expectation of privacy).

19. Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. 2510-710) [hereinafter ECPA]. 9

20. 18 U.S.C. 2511(1)(a) criminalizes the interception of "any wire, oral or electronic communication" without regard to an expectation of privacy.

21. Interception of Communications Act 1985, Long Title, An Act to make new provision for and in connection with the interception of communications sent by post or by means of public telecommunications systems and to amend section 45 of the Telecommunications Act 1984.

22. Interception of Communications Act 1985 1, Prohibition on Interception: (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 telecommunications 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.

23. Tapping (aka 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 the question of whether the communication in question was intercepted in the course of its transmission by means of a public telecommunications 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,WORKING PAPER NO. 110: COMPUTER MISUSE, 3.30 (1988).

24. "There are also forms of eavesdropping which the Act does not cover. For example. eavesdropping on a V.D.U. [referred to in this text as a CRT] 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 crimi-

nal offence..." THE LAW COMMISSION, WORKING PAPER NO. 110: COMPUTER MISUSE, 3.31 (1988).

25. 301.2(1) of the Canadian criminal code states that anyone who without color of right, (a) obtains, directly or indirectly, any computer service, (b) by means of an electromagnetic ... or other device, intercepts or causes to be intercepted, either directly or indirectly, any function of a computer system ... [is guilty of an indictable offence].

26. UNITED STATES SENTENCING COMM'N, FEDERAL SENTENCING GUIDELINES MANUAL (1988) (Principles Govern- ing the Redrafting of the Preliminary Guidelines "g." (at an unknown page))

27. There has been great debate over what exactly is a computer crime. There are several schools of thought. The more articulate school, and the one to which the author adheres holds that the category computer crime should be limited to crimes directed against computers; for example, a terrorist destroying a computer with explosives would fall into this category. Crimes such as putting ghost employees on a payroll computer and collecting their pay are merely age-old accounting frauds; today the fraud involves a computer because the records are kept on a computer. The computer is merely ancillary to the crime. This has been mislabeled computer crime and should merely be referred to as a fraud perpetrated with the aid of a computer. Finally, there are information crimes. These are crimes related to the purloining or alteration of information. These crimes are more common and more profitable due to the computer's ability to hold and access great amounts of information. TEMPEST ELINT can best be categorized as a information crime.

28. Compare, for example, the Watergate breakin in which the burglars were discovered when they returned to move a poorly placed spread spectrum bug.

29. TEMPEST Certified refers to the equipment having passed a testing and emanations regime specified in NACSIM 5100A. This classified document sets forth the emanations levels that the NSA believes digital equipment can give off without compromising the information it is processing. TEMPEST Certified equipment is theoretically secure against TEMPEST eavesdropping. NACSIM 5100A is classified, as are all details of TEMPEST. To obtain access to it, contractor must prove that there is demand within the government for the specific type of equipment that intend to certify. Since the standard is classified, the contractors can not sell the equipment to non-secure governmental agencies or the public. This prevents reverse engineering of the standard for its physical embodiment, the Certified equipment. By preventing the private sector from owning this anti- eavesdropping equipment, the NSA has effectively prevented them from protecting the information in their computers.

30. Previously the Bureau of Standards. The NIST is a division of the Commerce Department.

31. In this case computer equipment would include all peripheral computer equipment. There is no use is us- ing a TEMPEST Certified computer if the printer or the modem are not Certified.

32. The NSA has tried to limit the availability of TEMPEST information to prevent the spread of the devices. For a discussion of the First Amendment and prior restraint see, e.g. The United States of America v.

Progressive, Inc. 467 F.Supp 990 (1979, WD Wis.)(magazine intended to publish plans for nuclear weapon; prior restraint injunction issued), reh. den. United States v. Progressive Inc. 486 F.Supp 5 (1979, WD Wis.), motion den Morland v. Sprecher 443 US 709 (1979) (mandamus), motion denied United States v. Progressive, Inc. 5 Media L R (1979, 7th Cir.), dismd. without op. U.S. v. Progressive, Inc 610 F.2d 819 (1979, 7th Cir.); 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); T. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION (1970); Balance Between Scientific Freedom and NAtional Security, 23 JURIMETRICS J. 1 (1982) (current laws and regulations limiting scientific and technical expression exceed the legitimate needs of national security); Hon. M. Feldman, Why the First Amendment is not Incompatible with National Security, HERITAGE FOUNDATION REPORTS (Jan. 14, 1987). Compare Bork, Neutral Principles and Some First Amendment Problems, 47 IND. L. J. 1 (First Amendment applies only to political speech); G. Lewy, Can Democracy Keep Secrets, 26 POLICY REVIEW 17 (1983) (endorsing draconian secrecy laws mirroring the English system).

33. For example, the NSA has just recently allowed the Drug Enforcement Agency (DEA) to purchase TEMPEST Certified computer equipment. The DEA wanted secure computer equipment because wealthy drug lords had were using TEMPEST eavesdropping equipment.

34. 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, Long Title.

35. "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. Data Protection Act 1984 1(3)

36. "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. Data Protection Act 1(5).

37. Data Protection Act 1984, 4,5.

38. An individual who is the subject of personal data held by a data user... and who suffers damage by reason of (1)(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 ...