Privacy Issues in Computerized Communications

Thesis by
Daniel M. Zimmerman

In Partial Fulfillment of the Requirements
for the Undergraduate Minor in
Science, Ethics and Society

California Institute of Technology
Pasadena, California

1996
(Submitted 3 June 1996)

Contents

I
Introduction & Overview

Over the last few years, the use of technologies such as electronic mail and the World Wide Web has increased at an incredible rate. Millions of people, who had previously only used telephones and other conventional methods to communicate and transact business, have started to take advantage of the convenience and economic savings offered by these new computerized communication technologies. However, as the use of these technologies has increased, it has become clear that there are privacy issues associated with their use which have not yet been adequately addressed by either service providers or lawmakers.

Because there are laws protecting the privacy of telephone conversations, letters sent via U.S. Mail, and even transactions such as video rentals, a great majority of people assume that their privacy is also protected when they engage in computerized communications. Unfortunately, they could scarcely be more wrong - the privacy of computerized communications is, as we shall see, barely protected, if it is even protected at all. This has caused, among other undesirable effects, massive credit card fraud resulting from credit card numbers "intercepted" as they travel the Internet, at great cost to both individuals and credit card companies. In addition, the thousands of personal computerized communications which flow through the global telecommunications network every day are subject to interception by any number of third parties, unbeknownst to the majority of Internet users who simply wish to take advantage of new technology to communicate with

each other.

It is, therefore, critical to the setting of future communications policy to determine whether or not the privacy of these newly widespread computerized communications *should* be protected, and, if so, what actions can be taken to protect them. The following three chapters, which present descriptions of the concept of privacy in general, the development of the concept of a "right to privacy" in the legal context, the concept of "private communications", and the nature of the various types of computerized communications, provide the necessary basis for answering the first question; the next two chapters, which examine the feasibility of current and future technological protection for computerized communications privacy as well as the current legal status of computerized communications privacy, provide the necessary background for answering the second.

The privacy issues associated with the use of computerized communications have recently become extremely important, and will become even more important as the use of computerized communications continues to increase. My goal is to clarify these issues, and ultimately to not only show that privacy in the various types of computerized communications is deserving of protection, but also determine how such protection can best be provided given the current state of both technological development and legislative policy.

2
The Concept of Privacy

The concept of privacy is one which is familiar, on some fundamental level, to everyone. The term "privacy" itself is used regularly when discussing many different issues, and the number of different actions which are regularly classified under the umbrella category of "invasion of privacy" is staggering. However, despite the fact that privacy is such a widely-used concept, it is extremely difficult to actually define what privacy*is*, and harder still to define a "right to privacy" or give concrete reasons for the necessity of such a right - as one author of a paper on the topic put it, "Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is."[1] In this chapter, I will present some of the definitions of privacy and the right to privacy which have been proposed over the last century, as a means of providing a basis for defining the concept of private communications and justifying the existence of a right to private communications.

2.1. Privacy as the "Right to be Let Alone"

In 1890, Samuel D. Warren and Louis D. Brandeis published "The Right To Privacy (The Implicit Made Explicit)" in the Harvard Law Review. This was the first serious attempt at a quantification of privacy for legal purposes, and, as its title implies, it explicitly laid out a definition for and limitations of a "right to privacy" and legal remedies for violations of that right.

Every individual, according to Brandeis and Warren, is entitled by common law to, "the right of determining, ordinarily, to what extent his thoughts, sentiments and emotions shall be communicated to others."[2] This right applies regardless of both the form taken by such communication and the individual initiating the communication. For example, if somebody were to print a list of individuals who share some controversial political position and post it in public view, he would be violating the right of those individuals to keep their personal beliefs from being widely known. Similarly, if this same somebody forced an individual to reveal his position on various political issues by means of coercion (either physical or psychological), he would still be violating the same right. Brandeis and Warren clearly distinguish between violations of privacy and cases of defamation, saying that defamation, "deals only to damage with reputation, with the injury done to the individual in his external relations to the community, by lowering him in the estimation of his fellows," while a violation of an individual's privacy involves an, "effect...upon his estimate of himself and upon his own feelings."[3] In other words, privacy is a more "spiritual" right, where the rights protected by slander and libel laws are "material" in nature.

Brandeis and Warren further assert that such protection applies to physical property as well as intellectual property. If an individual possesses physical property which he wants to keep private, they say, no other individual should be able to publish a description of that physical property without permission, just as no individual is entitled to publish another individual's political views without permission. The right to privacy, they conclude, is not based on property rights (whose main purpose is to prevent others from unjustly profiting from an individual's work); rather, it is a, "more general right of the individual to be let alone."[4] They go on to state that:

> *The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.*[5]

and, later, that:

> *The principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal*

> *appearance, sayings, acts, and to personal relation[s], domestic or otherwise.*[6]

In other words, common law already included privacy protection for intellectual property, and a reasonable extension of that protection to include "personal appearance, sayings, acts, and...relations" does not involve the creation of a new legal principle.

Of course, there must be limitations to this right of privacy - if there weren't, the criminal justice system would cease to function, among other undesirable consequences. Similarly, there must be legal remedies for violations of the right to privacy, or else enforcement would be impossible. Warren and Brandeis address both of these issues, listing six limitations and two remedies[7] .

The limitations to the right of privacy as stated by Warren and Brandeis are:

1. *The right to privacy does not prohibit any publication of matter which is of public or general interest.*

Information about an individual in public office, or anyone else in which the public has a legitimate interest, can still be publicly released despite the fact that it may be "private" information if it has some bearing on the individual's fitness for their position. The private lives of politicians, in general, fall into the category of "public interest" (as can be seen by looking through almost any newspaper in the country, especially during a presidential election year).

2. *The right to privacy does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel.*

An individual is allowed to reveal private information in certain circumstances. One example of this is the preparation of a defense in a criminal trial - a defendant's alibi may depend upon the fact that he met a particular person at a particular place and time, and, even if that person doesn't want his whereabouts at that time publicly known, the defendant has the right to reveal them in his own defense. Another example would be if one individual sends a private letter to another promising some future action, then fails to keep her promise - the recipient of the letter has the right to reveal the contents therein, in order to prove that the promise was broken.

3. *The law would probably not grant any redress for the invasion of privacy by*

oral publication in the absence of special damage.

As Warren and Brandeis put it, "the injury resulting from such oral communications would ordinarily be so trifling that the law might well, in the interest of free speech, disregard it altogether."[8]

4. *The right to privacy ceases upon the publication of the facts by the individual, or with his consent.*

If an individual releases information in a form which is legally considered a "publication" (which does not include such things as interoffice memos and other privately circulated communications), that individual can no longer claim that said information is protected by her right to privacy (because it is clearly no longer private).

5. *The truth of the matter published does not afford a defense.*

Clearly, a violation of privacy should be regarded the same way, whether or not the information in question is true. In fact, Warren and Brandeis state that, "[the right to privacy] implies the right not merely to prevent *inaccurate* portrayal of private life, but to prevent its being depicted at all."[9]

6. *The absence of "malice" in the publisher does not afford a defense.*

The reason for this limitation is similar to that for the fifth limitation - a violation of privacy should be regarded the same way regardless of the state of mind of the person perpetrating the violation.

The remedies for a violation of an individual's right to privacy are similar to the remedies for defamation law and property law, namely:

1. *An action of tort for damages in all cases. Even in the absence of special damages, substantial compensation could be allowed for injury to feelings as in the action of slander and libel.*

2. *An injunction, perhaps [in] a very limited class of cases.*

Brandeis and Warren go on to say that, "it would doubtless be desirable that the privacy of the individual should receive the added protection of the criminal law, but for this, legislation would be required."[10] Clearly, their position was that the law already protected an individual's right to privacy, and they were only expressing that implicit protection in an explicit manner (hence, the title of their paper). Though most people shared the views

expressed by Brandeis and Warren regarding the law's protection of personal privacy, there were some who disagreed that privacy was as obvious a concept as the "right to be let alone," as evidenced by subsequent writing on the subject.

2.2. Privacy as Four Distinct Torts

For seventy years after the publication of "The Right to Privacy" in the Harvard Law Review, articles discussing the same issues and (with very few exceptions) reaching approximately the same conclusions as Warren and Brandeis appeared in various law journals throughout the United States. The right to privacy began, slowly, to find its way into decisions in courts throughout the country, though some (such as the New York Court of Appeals) initially refused to uphold the existence of such a right due to lack of any relevant precedent, and by 1960 the right of privacy was recognized in every U.S. jurisdiction except Rhode Island, Nebraska, Texas and Wisconsin. It was in this legal climate, with the existence of a right to privacy almost universally recognized, that William L. Prosser, dean of the University of California at Berkeley's Boalt Hall Law School, published "Privacy (A Legal Analysis)" in the California Law Review. In this paper, Prosser analyzes what the right of privacy actually amounts to with respect to law, and he comes to a conclusion rather different from those previously published.

Unlike Warren and Brandeis, who maintained that privacy was basically a new tort distinct from any others already recognized under the law, Prosser says that privacy, "comprises four distinct kinds of invasion of four different interests of the plaintiff,"[11] or, more succinctly, that privacy, "is not one tort, but a complex of four…[which] have almost nothing in common except that each represents an interference with the right of the plaintiff…'to be let alone.'"[12] While this may not seem like an important distinction at first glance, it becomes quite dramatic as Prosser actually describes these four "interests". In addition to listing the four distinct torts comprising privacy,[13] Prosser relates them to the definition of privacy previously advanced by Brandeis and Warren, describes exactly what "interest of the plaintiff" he believes is protected by each one, and postulates reasonable limitations on the protection they afford:

1. *Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.*

Examples of actions which violate privacy rights under this tort are intrusion into a person's home, looking through a person's shopping bags, or tapping somebody's telephone lines. Prosser points out, correctly, that Brandeis and Warren do not seem to address this particular aspect of privacy in their article, as they were primarily concerned with the *publication* of information about or belonging to individuals, rather than intrusions which do not involve anything which could be construed as publication.

In order for an action to be a violation of privacy under this tort, "there must be something in the nature of prying or intrusion...mere noises which disturb a church congregation, or bad manners, harsh names and insulting gestures in public have been held not to be enough."[14] He also says that, "the intrusion must be something which would be offensive or objectionable to a reasonable man," and, "it is clear...that the thing into which there is prying or intrusion must be, and be entitled to be, private."[15] For instance, a defendant at a criminal trial does not suffer a violation of his privacy rights when his testimony is recorded, nor does a man whose photograph is taken while he is walking in a public park.

In summary, Prosser says that the interest protected by this tort is, "primarily a mental one," and that this tort, "has been useful chiefly to fill in the gaps left by trespass, nuisance, the intentional infliction of mental distress, and whatever remedies there may be for the invasion of constitutional rights."[16]

2. Public disclosure of embarrassing private facts about the plaintiff.

An example of an action which violates privacy rights under this tort is the publication of lewd photographs or descriptions of an individual. This aspect of privacy, Prosser states, is the one with which the article of Warren and Brandeis was primarily concerned. "Public disclosure" is basically tantamount to publication, and it is precisely the publication of private information which Warren and Brandeis addressed. Prosser, however, goes beyond Warren and Brandeis in detailing the conditions under which an action actually violates an individual's right to privacy under this tort.

Prosser says, first of all, that any disclosure which violates the right to privacy under this tort must in fact be *public*. For instance, it would be an invasion of privacy to publish, in the *Los Angeles Times* or the *California Tech*, that a particular classmate of mine did

poorly on an exam, but it would not be an invasion of privacy for me to tell the same information to a group of friends. Similarly, the disclosure must be of "private facts" - if I were to publish a description, or even a photograph, of the outside of my best friend's apartment building, it would not be a violation of her right to privacy because that information is already available publicly (by driving down her street and looking out the car window). The counterpart to this restriction (in the case of photographs) is that if a photograph is taken, "surreptitiously, or over the plaintiff's objection, in a private place," or a preexisting photograph is, "stolen, or obtained by bribery or other inducement of breach of trust,"[17] the plaintiff's right to privacy is violated. Additionally, as with the first tort, the disclosure must be one which, "would be offensive and objectionable to a reasonable man of ordinary sensibilities," because, as Prosser quite rightly points out, "all of us, to some extent, lead lives exposed to the public gaze or to the public inquiry, and complete privacy does not exist in this world except for the eremite in the desert."[18] For instance, if a man hosts a party for a group of people, that fact can be reported in a newspaper without violating his privacy under this tort, whereas (using a favorite example of many writers on the topic) a report containing details of his sexual relations *would* violate his right to privacy.

In summary, Prosser describes the interest protected by this second tort as, "that of reputation, with the same overtones of mental distress that are present in libel and slander," and goes on to say that it is, "an extension of defamation, into the field of publications that do not fall within the narrow limits of the old torts, with the elimination of the defense of truth."[19]

3. Publicity which places the plaintiff in a false light in the public eye.

Examples of actions which violate privacy rights under this tort include cases where a person's name is used on a political petition without permission, and cases where pictures of individuals are used to illustrate writings which have no connection to the individuals in question. As with the first tort, the issues addressed by this tort do not seem to have been considered by Warren and Brandeis in their article, according to Prosser.

Basically, any action which publicly places an individual in a false light constitutes a violation of privacy rights under this tort. There need not be any defamatory characteristics associated with the false light, but, as with the previous two torts, the guideline that the

violation, "must be something that would be objectionable to the ordinary reasonable man under the circumstances," applies, and, in fact, Prosser explicitly states that, "the hypersensitive individual will not be protected,"[20] by this tort. For example, assume a man is photographed while walking along Hollywood Boulevard at 6 PM on Friday. He can not claim that his privacy rights have been violated if the photograph is used to illustrate a story about people who walk along Hollywood Boulevard, even if the caption under the picture erroneously says that it was taken at 8 PM on Friday. However, if the same picture is used to illustrate a story about men who seek out prostitutes on Hollywood Boulevard on Friday nights, the man in the photograph can certainly claim a privacy violation under this tort.

In summary, the interest protected by the third tort is, according to Prosser, "clearly that of reputation, with the same overtones of mental distress as in defamation," and this interest bears, "a resemblance to disclosure; but the two differ in that one involves truth and the other lies, one private or secret facts and the other invention."[21]

4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness. An example of an action which violates privacy rights under this tort is the use of a prominent person's picture in an endorsement for some commercial product, without the permission of the person in question. Like the first and third torts, this one does not seem to have been considered by Warren and Brandeis in their article.

The main idea behind this tort is that the person's name or likeness must be used to represent the person's actual identity, rather than just as a name or a picture. For instance, using a picture of me to advertise a particular brand of canned broccoli would not be considered a violation of this tort (though it may be a violation of some other tort, particularly if the picture was of me eating broccoli at a private dinner - this would fall under the second tort, disclosure, outlined above), because I have no public reputation for being a good judge of broccoli. However, using a picture of George Bush to advertise the same can of broccoli would be considered a violation, because it would be making use of his well-known aversion to broccoli to say, "Our broccoli is so good, even George Bush will eat it!" Similarly, as Prosser goes on to say, "there is no liability for the publication of a picture of [an individual's] hand, leg and foot, his dwelling house, his automobile or his dog, with nothing to indicate whose they are,"[22] because there is no basis for the association of those pictures

with the individual in question. Additionally, in accordance with the necessity of freedom of the press, "the mere incidental mention of the plaintiff's name in a book or a motion picture ...is not an invasion of his privacy; nor is the publication of a photograph or a newsreel in which he incidentally appears."[23]

In summary, Prosser says that the interest of the plaintiff protected by this tort, "is not so much a mental as a proprietary one, in the exclusive use of the plaintiff's name and likeness as an aspect of his identity."[24] which clearly distinguishes it from the previous three torts.

The main consequence of defining privacy as four torts rather than one is that it becomes a lot more complicated to decide what is and what is not an invasion of an individual's privacy. In fact, in the section after he describes the torts in detail, Prosser writes the following complex summary of the commonalities among the four different torts:

> *Taking them in order - intrusion, disclosure, false light, and appropriation - the first and second require the invasion of something secret, secluded or private pertaining to the plaintiff; the third and fourth do not. The second and third depend upon publicity, while the first does not, nor does the fourth, although it usually involves it. The third requires falsity or fiction; the other three do not. The fourth involves a use for the defendant's advantage, which is not true of the rest. Obviously this is an area in which one must treat warily and be on the lookout for bogs. Nor is the difficulty decreased by the fact that quite often two or more of these forms of invasion may be found in the same case, and quite conceivably all four.*[25]

Prosser goes on to say that, despite all of the differences pointed out above, the rules which have been applied to privacy cases have been remarkably consistent among all four types of cases, and he seems to approve of these rules (which include the rule that an individual's right to privacy does not extend to members of his family, and that the right of privacy pertains to individuals rather than organizations, among others). He also mentions the same exceptions to the rules originally mentioned by Warren and Brandeis, namely that matters of "public interest" can be disclosed without violating an individual's right to privacy, that the truth of a disclosure or the intention of the discloser has no bearing on whether or not a violation has taken place, and that an individual's (legitimate) consent nullifies any violation of his privacy rights.

Overall, Prosser seems to be saying that there is a danger in grouping all four of his separate torts under the umbrella label of "privacy" and treating them all in the same way,

because it creates, "an independent basis of liability...[which] has been expanded by slow degrees to invade, overlap, and encroach upon a number of other fields."[26] If left unchecked, the monolithic "tort of privacy" could expand to a point where privacy considerations begin to outweigh and overwhelm well-established considerations such as freedom of the press, whereas his four distinct torts are clearly delineated and have no such dangers associated with them.

2.3. Privacy as an Aspect of "Human Dignity"

Prosser's analysis of the right to privacy seems overly complex, and his "four distinct torts" definition has the unfortunate characteristic that it defines the (now multi-faceted) right to privacy on grounds that were expressly rejected by Brandeis and Warren in their original article, among them the torts of misappropriation of property and defamation of character. In fact, Prosser is basically saying that violations of privacy are merely violations of other, older and well known torts given a new name, whereas Brandeis and Warren clearly were trying to explicitly define a *new* right in their original privacy paper. In 1964, Edward J. Bloustein, the president of Rutgers University, published "Privacy as an Aspect of Human Dignity - An Answer to Dean Prosser" in the New York University Law Review, and in this paper he makes almost exactly this argument against Prosser's theory.

Bloustein's theory of privacy revolves, as one might guess from the title of his paper, around the concept of privacy as an aspect of "human dignity". He arrives at this theory by examining the original article by Warren and Brandeis to see what they really meant by a "right to privacy", because, as he says:

> *Warren and Brandeis went very little beyond...giving 'their right' and 'their interest' a name and distinguishing it from other rights or interests. It is only in asides of characterization and passing attempts at finding a verbal equivalent of the principle of privacy that we may find any further clues to the interest or value they sought to protect.*[27]

Recall that Brandeis and Warren distinguished between the right to privacy and the rights protected by slander and libel laws, by saying that privacy was a "spiritual" right where the others were "material" rights, and that a violation of privacy involves an effect upon an individual's "estimate of himself...and his own feelings."[28] They also explicitly said that the right to privacy was based on a principle of "inviolate personality". Bloustein, examining

these words written by Brandeis and Warren in 1890, sees in them the idea that the right to privacy results from, "the individual's independence, dignity and integrity;" and that the principle of inviolate personality, "defines man's essence as a unique and self-determining being."[29] As a result, he says, Brandeis and Warren wrote their article because they felt that, "it would have been inconsistent with a belief in man's individual dignity and worth to refuse him the right to determine whether his artistic and literary efforts should be published to the world."[30] Prosser's system of four torts would seem to be at odds with this definition of privacy, as it is based solely on interests of the individual which have nothing to do with "man's individual dignity and worth," and Bloustein, in analyzing the same types of cases examined by Prosser, concludes that all four of Prosser's torts address the same interest - protection of human dignity.

With regard to the first tort, which deals with intrusion into an individual's private affairs or upon his solitude, Prosser says that the main wrong addressed by the tort is the intentional infliction of mental distress; Bloustein, on the other hand, says that the wrong addressed by this tort is an attack on human dignity, because actions like eavesdropping and wiretapping, "are wrongful because they are demeaning of individuality, and they are such whether or not they cause emotional trauma."[31] He additionally invokes the Fourth Amendment, which protects U.S. citizens from "unreasonable search and seizure", and the declaration of the Supreme Court that "the underlying purpose of such protection is the preservation of individual liberty,"[32] as a further illustration that the type of intrusion addressed by Prosser's first tort is wrong because it is a violation of individual liberty, and not because it causes mental distress.

In dealing with the second and third torts, which deal with public disclosure of private facts and portrayal in a false light, Prosser says that the interest of reputation is the main interest protected by both. However, as Bloustein points out, this completely ignores the fact that Warren and Brandeis explicitly differentiated between defamation and privacy violations, and that they explicitly said that the right to privacy existed to prevent private life from being portrayed *at all*, rather than merely to prevent it from being portrayed inaccurately, which certainly seems to indicate that protection of an individual's reputation should play no part in defining the right to privacy. In other words, as Bloustein puts it,

"defamation is founded on loss of reputation while the invasion of privacy is founded on an insult to individuality."[33] Since it is not necessary to suffer any damage to reputation as a result of an invasion of privacy, it is inconceivable that Prosser's second and third torts are adequate to describe the right to privacy in the cases to which they apply. Additionally, it seems clear that privacy cases which fall under the second and third torts involve an affront to individual dignity, as the disclosure of private facts about an individual must be a violation of individual liberty (in this case, the liberty to decide who does and who does not get to know the private facts), just as intrusions into an individual's private affairs are.

The fourth tort, which deals with commercial exploitation of an individual's name or likeness, is said by Prosser to protect the individual's proprietary interest in his name and likeness as an aspect of his identity. Bloustein, however, maintains that the interest being protected is not a proprietary one, but rather the individual's interest in preserving his dignity, because, "the use of a personal photograph or a name for advertising purposes has the same tendency to degrade and humiliate as has publishing details of personal life to the world at large."[34] In a famous case, *Pavesich v. New England Life Ins. Co*., involving a man whose photograph was used in an advertisement for life insurance without his permission, the Georgia Supreme Court declared that:

> *The knowledge that one's features and form are being used for such a purpose and displayed in such places as such advertisements are often liable to be found brings not only the person of an extremely sensitive nature, but even the individual of ordinary sensibility, to a realization that his liberty has been taken away from him, and as long as the advertiser uses him for these purposes, he cannot be otherwise than conscious of the fact that he is, for the time being, under the control of another, and that he is no longer free, and that he is in reality a slave without hope of freedom, held to service by a merciless master...*[35]

Clearly, a person in such a situation has suffered a severe blow to his human dignity. Furthermore, as Bloustein points out:

> *The only difference between [exploitation] cases and the public disclosure cases is that the sense of personal affront and indignity is provoked by the association of name or likeness with a commercial product rather than by publicity concerning intimacies of personal life.*[36]

Privacy cases which fall under Prosser's fourth tort, therefore, involve affronts to human dignity just as those which fall under the previous three torts.

According to Bloustein, then, all four types of privacy cases described by Prosser

involve a single common element - an affront to human dignity. In describing them as such, seems to capture the spirit of the right to privacy more successfully than Prosser, emphasizing, as Brandeis and Warren did, that, "the interest served in...privacy cases is in some sense a spiritual interest rather than an interest in property or reputation," and that, "moreover...the spiritual characteristic which is at issue is not a form of trauma, mental illness or distress, but rather individuality or freedom."[37]

2.4. An Economic Theory of Privacy

In addition to the legal/philosophical definitions of privacy already presented, there is one more interesting theory of privacy which can be considered, especially with respect to the exchange of information. In 1978, Richard A. Posner published an article in *Regulation* entitled "An Economic Theory of Privacy," which details this theory and its ramifications. While this theory has had little effect on privacy law or attitudes toward privacy in the United States, it is of interest specifically because of the radically different light in which it presents the issues surrounding the protection of individual privacy.

Posner does not define the word "privacy" itself - he admits, at the very beginning of his paper, that he is "sidestepping" the issue. Rather, he notes the "obvious" fact that one particular aspect of privacy involves the withholding or concealment of information, and that, with respect to this aspect, privacy can be analyzed using economic theory rather than conventional philosophical or legal arguments. He says[38] that, in considering privacy, there are two economic goods involved - "privacy" and "prying" - and that both are what economists call "intermediate goods", meaning that people desire privacy and prying not in and of themselves but rather because they can be used as "inputs into the production of income or some other broad measure of utility or welfare."[39] Privacy, then, is desired by people (among other reasons) so that they can manipulate the opinions of others by misrepresenting themselves, and prying is desired (among other reasons) so that one can uncover the misrepresentations of others.

This type of analysis, Posner maintains, has the ability to explain quite a few aspects of our society which may seem odd. For instance, the fact that newspapers like the *National Enquirer* and televisions shows like *Hard Copy*, which specialize in gossip and

rumormongering, are so popular seems unusual, and interest in such publications is frowned upon by many. However, Posner says, gossip columns and other such sources are actually informative, "open[ing] people's eyes to opportunities and dangers,"[40] and providing people with models (albeit not always good ones) on which to base their own behavior. Posner believes that this is the reason why people pay little to no attention to information regarding the lives of poor people, while eagerly reading gossip about the social elite: in his own words, "the lives of the poor do not provide as much useful information for the patterning of our own lives."[41] Economic arguments also explain the increase of press coverage of the private lives of individuals over the last century, because, as living conditions have improved, it has become more and more difficult to "pry" into others' affairs - the press has risen to play the role formerly occupied by the voyeur.

Posner goes on to consider the question of who "owns" personal information about individuals. From an economic standpoint, he concludes that in most cases it is better to assign property rights in particular pieces of information *away from* the individuals to whom the pieces of information pertain, because:

> *Much of the demand for privacy...concerns discreditable information - often information concerning past or present criminal activity or moral conduct at variance with a person's professed moral standards - and often the motive for concealment is...to mislead others. People also wish to conceal private information that, while not strictly discreditable, would if revealed correct misapprehensions that the individual is trying to exploit...*[42]

Two examples of such concealment are a worker concealing a serious health problem from his employer and a prospective husband concealing his sterility from his fiancée. In fact, under current law, both of those examples would probably be considered fraud, so the law agrees with the economic theory on that point. Making an analogy to the "world of commerce", Posner says that people should not have the right to conceal "material facts" about themselves, just as dealers of merchandise do not have the right to make false claims about the quality of their wares. A notable exception to this is in the area of "trade secrets", where commercial ideas and processes are protected in order to "encourage investment in the production of socially valuable information."[43] This sort of protection is provided in the United States by means of patent and copyright law, as well as non-disclosure agreements and other such legal instruments.

Of course, it would be ridiculous of Posner to advocate a system whereby everybody always had to tell the complete truth about themselves all of the time - such a system would never function in today's society. He admits, in fact, that "there are practical reasons for not imposing a general legal duty of full and frank disclosure of one's material personal shortcomings," but also says that, "each of us should be allowed to protect ourselves from disadvantageous transactions by ferreting out concealed facts about other individuals that are material to their implicit or explicit self-representations."[44] On the other hand, there is some non-discreditable information which people in general seem to want to conceal - the example given by Posner is that most people, in Western culture, do not like to be seen naked - and since the concealment of such information has no social cost, the property rights in this sort of information can be assigned to the individual without negative effects from an economic standpoint.

Despite the fact that property rights in private information should, from an economic standpoint, not be given to the individual to whom the information pertains, the *means* of "ferreting out concealed facts" about others must also be considered in an economic analysis of individual privacy. Obtaining information about an individual by asking him questions is totally different from obtaining the same information using a tap on the individual's telephone - if the second method is allowed, then the "cost" of conversation increases, as in this example by Posner:

> A in conversation with B disparages C. If C has a right to hear this conversation, A, in choosing the word he uses to B, will have to consider the possible reactions of C. Conversation will be more costly because of the external effects and this will result in less - and less effective - communication.[45]

If people had to take into account everybody who might be listening in on a particular conversation when choosing their words, it is doubtful that any meaningful communication would *ever* occur. This, in fact, is one of the important premises underlying the concept of private communications, to which I will return in the next chapter. This economic analysis of conversation can, of course, be extended to other forms of communication such as letters and, more interestingly (as I will show later), electronic mail. An exception to the prohibition against surveillance occurs when the communication is part of some illicit activity, such as the planning of a bank robbery or the arrangement of a narcotics deal - in

these cases, surveillance is economically justifiable because it protects society from bearing the social cost of the illicit activity in question.

There are, in summary, three "essential elements" which comprise Posner's economic theory of privacy: the privacy of trade secrets and other secrets which encourage the production of socially valuable information would be protected; facts about individuals would *not* be protected; and eavesdropping and other forms of "intrusive" surveillance would be limited (ideally) to conversations which involve the planning or execution of illegal activities. This economic theory of privacy, though many of its elements seem extremely questionable (especially the ones which deal with assigning the rights in facts about individuals away from the individuals in question), is, as it turns out, in very good agreement with current United States law on communications privacy.

2.5. Summary: So What *Is* Privacy?

Much has been written about privacy, and the right to privacy, since Samuel Warren and Louis Brandeis published "The Right To Privacy" in 1890. After over 100 years, however, it seems that, aside from some small clarifications, the accepted legal definitions for privacy and the right to privacy are basically the ones given by Warren and Brandeis. William Prosser's objections in his 1960 article, and his claim that the right to privacy involves four torts rather than one, seem to make the fact that privacy is a right in and of itself even more strikingly clear, as Edward Bloustein showed in his response to the Prosser paper. The economic definition of privacy, as devised by Posner, has had little to no effect on the commonly accepted notion of privacy and a right to privacy, and certainly no effect on the laws regarding privacy, though it does provide some fairly compelling reasons for the protection of privacy in communications.

Unfortunately, while a general consensus about legal definitions of privacy seems to have been reached over the last century, little to no consensus seems to have been reached about what, exactly, privacy *is*. Defining privacy as simply "the right to be let alone", as Brandeis did, seems inadequate - after all, as Posner very perceptively writes, "few people want to be let alone. They want to manipulate the world around them by selective disclosure of facts about themselves."[46] However, defining privacy as Bloustein does, as the state in

which an individual's "inviolate personality" is respected and in which his "dignity" is intact, also seems inadequate, because neither "inviolate personality" nor "dignity" has a clear, straightforward meaning. It would seem, then, that although we currently have a good idea about what sort of thing privacy is, and how it should be treated under the law, it is impossible to give a clear and precise definition for the term. Such a definition, however, is not necessary for the purposes of this discussion - the concepts as already presented form enough of a groundwork on which to build a definition of private communications and to establish the need for a right to communications privacy.

3
Private Communications

Having examined the general concept of privacy, it is now important to define exactly what constitutes a "private communication" and to determine whether or not individuals should have a "right" to private communications. Just like the concept of privacy, the idea of private communications is familiar on some fundamental level to everyone in our society, and nearly everyone would agree that there should be a right to at least *some* degree of privacy in communications. The basic groundwork for justifying such a right has already been laid in the previous discussion of the right to privacy itself - the goal of this chapter is to present a simple and coherent definition of the term "private communication" and to show that the right to privacy, as previously discussed, implies a right to private communications.

3.1. A Definition of "Private Communication"

In order to determine what the concept of privacy means when applied to communications, a specific definition of "communication" is necessary. I propose the following: A communication is an exchange of ideas, in any visible, audible or otherwise tangible form, between one person (the "sender" of the communication) and any number of other people (the "receivers" of the communication). This definition of communication clearly encompasses telephone conversations (spoken words), paper letters (written or typed words) and electronic mail (typed words). In addition, it does not restrict a

communication to being "point-to-point" - rather than a single sender and a single receiver, a communication, for the purposes of this discussion, can involve multiple receivers (as in an interoffice memo, or a piece of electronic mail sent to two people).

With this definition of a communication, it becomes simple to assign a meaning to the term "private communication". In order for a communication to be considered private, three conditions must hold. First, the sender must know the identities of all of the actual receivers of the communication (an "actual receiver" is any person who becomes aware of the content of the communication, through any means). Second, the sender must *intend* for the communication to be received by every actual receiver. This means, for instance, that if one of the intended receivers discloses the contents of the communication to a third party, the communication is no longer private under this definition. Third, the sender must expressly intend that the communication *not* be received by anybody other than the intended receivers. While this may seem obvious, there are actually many cases where communications which would not normally be thought of as private would be classified as such if not for the presence of this requirement.

It may seem as though this definition of a private communication is rather heavily biased in favor of the sender - for example, nothing in the definition states that any intended receiver should have knowledge of the other receivers. This "omission" is, in fact, intentional - a private communication, for the purposes of this discussion, is considered to be a "one-way" exchange of ideas between the sender and the receivers. After all, as Warren and Brandeis stated in their famous article, every individual is entitled to determine for themselves, "to what extent his thoughts, sentiments and emotions shall be communicated to others."[47] This would seem to indicate that it should be the sender who has control over which individuals receive any particular private communication, while at the same time eliminating any obligation of the sender to make an individual receiver aware of the identities of the other receivers - the sender can choose not to communicate *anything he wants* to any particular receiver, including the identities of the other receivers. The definition of a private communication as given here, therefore, seems to fit well with the definition of privacy as given in the previous chapter.

3.2. The Right to Private Communications

Now that a definition for "private communication" has been proposed, it is necessary to determine whether a *right* to private communications exists and, if such a right *does* exist, to what extent it should be protected by law. The first question is relatively easy to answer - as I will show, the definitions of privacy and the right to privacy previously discussed actually imply a right to private communications. It is much more difficult to answer the second question, however: to do so, the importance of private communications to the individual must be weighed against other social concerns, such as the cost (both financial and social) of enforcement of laws protecting the right to private communications and the effect such laws have on the government's ability to enforce other laws (mainly those prohibiting various kinds of criminal activity).

Clearly, Warren and Brandeis would say that a right to private communications *does* exist. After all, the definition of private communications is practically a direct manifestation of their statement that every individual has the right to determine "to what extent his thoughts, sentiments and emotions shall be communicated to others." If we interpret the sentence literally, it doesn't help much in justifying a right to privacy - after all, the idea that a person has the right to communicate only 15% of his thoughts to others doesn't actually mean that the person has a right to control *who* gets to receive that 15% of his thoughts. However, it seems inconceivable to me that Warren and Brandeis would have intended it this way, given the content of the rest of their paper. Rather, I believe that they intended this to mean that an individual has the right to control not only the extent to which he communicates his thoughts, but also the extent to which that communication is disseminated throughout the population - in other words, he has the right to determine who should receive the information that he is communicating. This is, of course, the essence of a "right to private communications".

Support for the existence of a right to private communications can also be found in the writings of Bloustein, who believes that such a right exists because actions like eavesdropping and wiretapping, "are demeaning of individuality," and are, therefore, affronts to human dignity. Bloustein also invokes the Fourth Amendment's prohibition of "unreasonable search and seizure" - with a broad interpretation of the words, the monitoring

of an individual's communications without some legally justifiable reason (such as suspicion of criminal activity) becomes an "unreasonable search," and the interception of such communications an "unreasonable seizure."

Even Posner's economic theory of privacy includes an implicit right to private communications, though for totally different reasons than those outlined above. If people have to constantly worry about who might be monitoring their communications, Posner believes, they are not only less likely to communicate effectively, but also less likely to communicate *at all*, because the "cost" of effective communication increases greatly with the possibility that unknown agents are receiving the communication.

It seems clear, therefore, that the right to privacy implies a right to private communications as I have defined them. It is much more difficult, however, to determine to what extent private communications should be protected by legislation. Among the issues which must be considered when making this determination are the importance to the individual of protected private communications from both "economic" and philosophical points of view, the costs involved in enforcing legislation which provides such protection, and the effect of such legislation on the government's ability to successfully enforce other laws.

3.3. The Importance of Communications Privacy

The first issue, that of the importance to the individual of some form of protection for private communications, must be examined from two separate points of view. The first of these is grounded in economics, and deals with the "cost" of communication, as mentioned by Posner in his paper. The basic idea is that if individual A communicates with individual B knowing that the communication is private, he can say anything he likes about individual C, secure in the knowledge that C will not find out what is being said. If, on the other hand, A has to worry about his remarks being overheard by (or reported to) C, he must be very careful in choosing his words when discussing C, which raises the "cost" of the communication for A. When private communications are not protected, it becomes impossible to effectively communicate in many circumstances - imagine, to take possibly one of the least "serious" examples, communicating with a friend as part of planning a

surprise party, only to find that the intended "surprisee" had been eavesdropping on your conversation. There are, of course, potentially far more serious effects of a lack of communications privacy, such as a prosecuting attorney monitoring communications between defense attorneys in preparation for a murder trial and, using the knowledge he gains about their trial strategy, convicting an innocent defendant and sending him to prison for the rest of his life.

The importance of communications privacy to the individual must also be examined from a philosophical point of view. Charles Fried, in a paper entitled "Privacy: A Moral Analysis," maintains that privacy is, "necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust," and that, "privacy is the necessary atmosphere for these [relations], as oxygen is for combustion."[48] Since we have already established that the right to privacy implies a right to private communications, this statement can be strengthened to say that private communications are essential to the fundamental human relations of respect, love, friendship and trust, all of which are very important to most people. This strengthening seems to be a reasonable one. Nobody would deny that private communications between two people are essential for the development of a love relationship, for instance - in fact, the important role of such private communication is obvious. So, from a philosophical point of view, the existence and protection of private communications is important because it allows people to form basic and fundamental human relationships with others.

3.4. Difficulties in Protecting Communications Privacy

The second issue, that of the difficulty involved in enforcing legislation which protects private communications, is actually not a terribly difficult one to deal with. In order to protect the privacy of communications, it is not necessary to *actively* enforce rules prohibiting, for example, the use of wiretapping devices to listen to telephone conversations. Rather, it is enough to *passively* enforce these rules, by establishing systems of fines and other punishments as penalties for interception or other unauthorized use of private communications. For instance, the fact that information obtained by the police through the use of an unauthorized wiretap is not admissible in court is enough to prevent

the police from using unauthorized wiretaps, because nothing is gained by obtaining evidence which is inadmissible in court. It is, therefore, not necessary to constantly watch the police to be sure that they aren't planting unauthorized wiretaps.

This sort of passive enforcement is very inexpensive in economic terms - it requires no additional police to be added to the nation's police forces, no expensive equipment to detect wiretaps and other unauthorized monitoring, and no unreasonable actions on the part of individuals to obtain protection for their private communications. All it requires, in fact, is time spent by the courts in dispensing punishments and fines for violations of communications privacy. Of course, such passive enforcement is not enough to satisfy many individuals - there is always the fact that, whether or not the violator actually*uses* the information gained by a violation of communications privacy, the violation has still occurred, and passive enforcement doesn't really provide a remedy for such cases (if the violator doesn't use the information, and doesn't do anything to draw suspicion to himself, then nobody will ever know the violation occurred). However, as will be discussed later, people who are concerned enough about the privacy of their conversations can take more active measures to prevent them from being monitored - scrambled telephones and encrypted electronic mail are examples of these. For the great majority of individuals, however, a system of passive enforcement is an effective way of protecting the right to communications privacy.

3.5. The Effect of Communications Privacy on Law Enforcement

The third issue, that of the effect of protection of communications privacy on the government's ability to enforce other laws (and otherwise carry out its duty to its citizens), is the most difficult one to deal with. An effective solution requires an answer to the question of when the right of the government to enforce the laws and protect its citizens overrides the right of the individual to privacy in communications. This is an incredibly sensitive issue, which has recently been pushed quite visibly into the public spotlight by the various proposals for a national encryption standards made by the current administration. One way to solve this problem is to say that the government has the right to monitor private communications if there is valid reason to suspect that such communications are being used

to plan or execute criminal activities. One example of such use of private communications is a bank robber calling a getaway car driver to tell him exactly what time to be waiting outside the First Federal Bank of Kalamazoo and which route to follow for the getaway.

While this solution may seem very sensible at first glance, there are major problems to be overcome in its implementation. It is very difficult to determine what sorts of suspected "criminal activity" justify invading an individual's privacy by monitoring her private communications - for instance, both shoplifting and murder are crimes, but while most people would agree that a wiretap is justified in the case where a murder is being planned, it is almost certain that nobody would advocate placing a wiretap on the telephone of a teenager who talks to a friend about shoplifting. Admittedly, these are extreme examples, but the question of where the line should be drawn is truly a difficult one. Likewise, it is difficult to determine exactly what constitutes "valid reason" to suspect that a person is using private communications to plan or execute criminal activities - law enforcement officials often get their information from less than savory sources, and could easily end up violating individuals' rights to private communications without actual cause. Finally, when monitoring communications over shared resources such as telephone lines, the privacy rights of individuals other than the one under suspicion must be considered. Sworn testimony from a mother who believes that her son is using his own telephone line to arrange sales of illegal drugs might be enough to warrant a wiretap on the son's telephone line, but if it's the *family's* telephone line, a wiretap unnecessarily compromises the communications privacy not only of the person under suspicion but also of the remaining members of the family, who are not even suspected of any wrongdoing.

Unfortunately, there are no easy solutions to these problems. In practice, the types of criminal activity which are considered to justify the monitoring of private communications are set by law, as, though less strictly delineated, are the conditions which are necessary to provide sufficient cause for the use of a wiretap. The issue of compromising the communications privacy of innocent parties is generally not taken into consideration at all - after all, any person who talks to the person under suspicion on a tapped telephone line, or while under another form of surveillance, has his privacy rights violated regardless of his innocence, to say nothing of other individuals using the same shared resource (such as a

telephone line or a "bugged" room) as the individual under suspicion. The reason for this, of course, is that it is impossible to consider the privacy rights of innocent third parties and effectively carrying out the surveillance necessary to get whatever information is needed without the "cost" of the surveillance, both in terms of technology and manpower, being far too high to be justifiable. As a result, it is generally accepted that the government, while having to take reasonable precautions to avoid violating the privacy rights of innocent people, has a responsibility to do the sort of monitoring necessary for effective law enforcement even if it does sometimes infringe on the privacy rights of innocents.

3.6. Summary: The Need for Communications Privacy Protection

From the preceding discussion, it seems clear not only that a right to private communications exists, but also that it should be protected in some fashion. The most obvious way to do this is to institute a system of passive enforcement of legislation protecting rights of individuals to privacy in communications; however, in order for the government to effectively protect its citizens and maintain order, this protection must be able to be circumvented for the purposes of law enforcement. This is, in fact, the type of system which is in effect in the United States today and which protects telephone conversations, written letters, and various other forms of communication from illicit interception.

While such a system provides protection for communications privacy which is adequate for most individuals, other methods (such as data encryption, which will be dealt with in Chapter 5) should be made available in order to allow people who want, or need, more protection for their private communications to obtain it without extreme inconvenience. Currently, however, this sort of additional protection is largely unavailable to individuals. In addition, as will be shown in Chapters 5 and 6, while the currently existing laws and technical solutions can effectively protect the privacy of conventional communications, they are inadequate to the purpose of providing protection for the various kinds of computerized communications which are rapidly gaining a foothold not only in the United States, but throughout the world.

4

Computerized vs. “Normal” Communications

In order to say anything substantial about the protection of privacy in computerized communications, it is necessary to determine exactly what constitutes a “computerized communication” and how computerized communications differ from what I will call “normal communications”, such as telephone conversations, paper letters and radio and television broadcasts. In this chapter, I will describe the various types of computerized communications and contrast them with “normal” communications, as a prelude to an examination of the effectiveness of current communications privacy laws and technical solutions for the protection of computerized communications privacy.

There are six main categories of computerized communications: network transmission of textual (typed by the user) and/or binary (such as a picture or audio clip) information to one or more receivers; point-to-point real-time transmission of textual information between two individuals; real-time exchange of textual information among multiple individuals using a shared server; real-time transmission of audio and/or video communication among multiple individuals; network broadcast of textual and/or binary information from one sender to a possibly large number of receivers; and point-to-point broadcast of textual and/or binary information from one sender to a possibly large number of receivers with possible “return” communication from each receiver to the sender. These six types of computerized communication all share some characteristics with various types of “normal” communication, but they also have other qualities which, in some cases, make

privacy issues relating to computerized communications very difficult to deal with.

4.1. Electronic Mail

The first type of computerized communication, network transmission of textual and/or binary information from one sender to one or more receivers, is the predominant method of computerized communication. It is, put simply, what is known as "electronic mail", and will hereafter be referred to as such. The basic principle of its operation is as follows: a message (which may include text and/or binary data) is composed by the sender, specific destination addresses for the message are specified, and a separate copy of the message is then sent through a network (either a local area network, such as within a corporation's headquarters, or the Internet, which connects various local area networks) to each of those destination addresses. Each copy of the message passes through at least one host machine (though usually several) en route to its eventual destination, with each host creating and storing a local copy of the message when it is received and, ideally, removing the local copy when the message, with information appended to it to reflect the fact that it has passed through that particular host, is successfully sent to its next stop along the route.

The form of normal communication most closely analogous to electronic mail would seem to be, as one might guess from the name, mail as provided by such entities as the United States Postal Service. Both involve the composition of a specific message, which can contain not only text but also other content such as audio or video, and both involve the selection of a specific receiver for that message. However, there are several important differences between the two forms of communication. With normal mail, the actual message that is sent is physically the same exact message that will be received (barring mishaps such as the U.S.P.S. losing the letter or accidentally running over it with a mail truck). With electronic mail, on the other hand, the message is duplicated at least once, and usually multiple times, before it reaches its destination. Since, at each duplication, content is added to the message in the form of headers which trace the message's path through the network, the message which is received at the destination is not the same message as that originally sent either physically or in content.

Privacy is somewhat guaranteed in normal mail because of the fact that envelopes

have seals - an envelope which has been opened and resealed is easily detectable, unless the person resealing the envelope goes to a lot of trouble to hide the fact, and even then, the person has to be able to get physical possession of the envelope in the first place. With electronic mail, however, there is no analogue to the "seal" on an envelope to let the receiver know that nothing in the message has been removed or changed and that nobody has read the message en route - in fact, the message *must* be both read (at least by another machine, which makes a local copy) and changed as it travels through the network. To make matters worse, anybody running a host machine on the Internet (or anybody with access to the mail spool files, for that matter) can, for voyeuristic or other reasons, arbitrarily choose to read all the mail coming through that host and even to retain the local copies of mail going through the host after they have been passed on. Given the incredible number of host machines on the Internet, and the similarly large number of individuals who maintain and have access to them, the possibilities for violations of privacy with respect to electronic mail are staggering.

One analogy which seems particularly apt for comparing electronic mail and normal mail is to think of an electronic mail message as being equivalent, for the purposes of privacy, to a postcard. Both postcards and electronic mail messages can be read at any point along the path they follow from sender to receiver, and there is no easy way to tell whether either has been read or altered en route to its destination. The primary goal when discussing technical solutions to insure privacy in computerized communications, later in this paper, will be to provide protection for electronic mail similar to the protection provided by the envelope in normal mail.

4.2. "Talk" and Related Protocols

The second type of computerized communication, point-to-point real-time transmission of textual communication between two individuals, is also quite common, but not nearly as widely used as electronic mail. It involves the use of a program called "talk" (or some variant thereof using a similar protocol), which is run on the computers of the two individuals participating in the communication. One person requests the communication by sending a signal to the other person's computer, and the other person initiates the communication by responding to the signal. When communication is initiated, the

computers are connected to each other "directly" (over the Internet, such a connection goes through several routers, possibly including other Internet hosts, but requires no explicit action on the part of these routers). As the first person types, the characters are transmitted to the second person's screen, and vice-versa. No copies are explicitly made of the data being transmitted, other than those on the screens of the communicating individuals.

A telephone conversation is the form of normal communication most closely analogous to the use of programs like "talk". Both forms of communication involve the real-time transmission of words back and forth between two individuals (actually, more than two individuals can be involved in the same telephone conversation - there are also variants of "talk" which allow so-called "conference calls" - but the number of participants is largely irrelevant). The point might be raised that the typed word is different from the spoken word for the purposes of communication, but, in response to that, all one must do is look at the various TDD devices which are available to allow the deaf to have telephone conversations. It would seem, then, that these two forms of communication are very closely analogous. However, there is one critical difference: in a normal telephone conversation (or, for that matter, a telephone conversation using a TDD device), the spoken or typed words are converted to electrical impulses which, in and of themselves, are not intelligible as the words which they represent. In talk, however, the words are sent across the network *as words* which, if intercepted, can be understood without the use of any special equipment. As a result, it is far less difficult to monitor a talk session from a point in between the two machines engaged in the session than it is to monitor a telephone call from a point in between the two parties involved in the conversation - the technology to do so is basically built into every host on the Internet, ready to be taken advantage of with a few well-written lines of code.

A more obvious difference between talk sessions and telephone conversations lies in the susceptibility of talk sessions to what is usually called the "man in the middle" attack. Imagine that two people are involved in a talk session, and a third, who is a relatively skilled programmer, decides to compromise their communications security. This third person can "position" herself in such a way that she receives the words typed by both parties, and stops communication from each side from reaching the other. She can then

impersonate both people, communicating with both of them while they still think they are communicating with each other. Since typed words appear the same regardless of who is doing the typing, and since there is an arbitrary delay over the network (rendering it impossible to distinguish between individuals on the basis of characteristics such as typing speed), the man in the middle attack is very difficult to detect in a talk session. In a telephone conversation, on the other hand, the man in the middle attack will fail almost all the time, assuming that each person knows the other's voice well enough to be able to detect a third party entering the conversation.

Clearly, then, though talk sessions and telephone conversations share important characteristics, they are not strictly analogous, and any measures taken to protect the privacy of telephone conversations would most likely fail to protect the privacy of talk sessions. There *are* effective methods of protecting the privacy of talk sessions (mainly involving encryption, which will be discussed in detail in the next chapter) - however, they are at present very rarely used.

4.3. IRC and Analogous Services

The third type of computerized communication, real-time exchange of textual information among multiple individuals using a shared server, is somewhat like "talk", but on a larger scale. It is, in fact, in extremely wide use at the present time in the form of a system called Internet Relay Chat (IRC), as well as in so-called "Chat Rooms" on commercial online services such as America Online, CompuServe and Prodigy. The basic idea behind these services is that the sender and receivers "log in" to the same machine, on which they set up a "room" (for lack of a better term) and have a conversation. Multiple rooms can be running at once on the same server, and a person can be in multiple rooms at the same time. In most of these setups, privacy issues do not arise, because they are public-access systems - all users of the system have the freedom to enter and leave rooms at will. However, there are mechanisms for "private" rooms, which are restricted in some manner (either by requiring that people have "permission" to enter a room, or by requiring the entry of some sort of password). As in "talk", the words typed by participants in IRC rooms are routed through various devices on the network, but no local copies are made of the data en route to its

various destinations, whether the IRC room involved is a public or private one.

The form of normal communication which corresponds most closely to an IRC "private room" (public rooms are not relevant to the discussion at hand) is a conversation held in a private conference room with an arbitrary number of chairs. Both forms of communication require all the people involved to "meet" in a "common area" (the physical conference room or the "private" room on the shared server), and both allow access to the communication to be restricted (by means of a physical lock on the door of the conference room, or a password or other security measure on the "private" IRC room). Unless there is a tape recorder in the physical conference room, no copies of the communication are made other than those which belong to the participants (i.e.: the words they hear spoken), and, similarly, no copies of an IRC communication are made other than those which are transmitted to the screens of the participants. This analogy, then, would seem to be a relatively good one, since the private conference room and the private IRC room seem to be providing exactly the same function for the participants.

Unfortunately, as between talk sessions and telephone conversations, there are differences between private conference rooms and private IRC rooms which make the IRC rooms much more vulnerable to violations of communications privacy. The first of these is that, as with talk, the words transmitted to the screens of the individuals involved with the discussion are transmitted in a format which is easily interceptable and readable by sufficiently savvy users of any machine on the Internet. Also, since the IRC room is run from a central server, any individual with sufficient access to that server basically has access to the IRC room (actually, to *all* IRC rooms based on that server), and can monitor them at his leisure. Unlike a "bugged" conference room, where any devices used to monitor the private communication can be physically detected and removed, the interception of data from an IRC room would be nearly impossible to detect, and, even if detected, even more difficult to stop. Additionally, the man in the middle attack described above with respect to talk sessions works just as well with a private IRC room, as they are based on very similar technology.

Most seriously, however, the security of the IRC room in terms of who is allowed in and who is not is much more difficult to maintain than that of the private conference

room - in a private conference room, there are physical locks, doors, and possibly even security guards to prevent unauthorized individuals from entering while a private communication is taking place. However, an IRC room protected by a password can never be as secure as that, because passwords can be broken by merely trying various combinations of letters and numbers until the right one is discovered, and "invitations" to the room can be faked in various and sundry ways. As a result of this, it is impossible to obtain the same level of protection for communications privacy in an IRC room as in a physical room without using some sort of encryption or other security protocol (and thereby rendering the IRC room much more inconvenient to use). While the analogy between the IRC room and a private conference room *is* a good one, it is incomplete insofar as the security of the communications taking place within is vastly superior in the private conference room.

4.4. "Internet Phone" and Videoconferencing

The fourth type of computerized communication, real-time transmission of audio and/or video communication between two or more individuals, is not only the newest, having gained enormous momentum over the past year, but is also the easiest with which to draw an analogy to a specific type of normal communication. This type of communication, which I will refer to as IPhone, is manifested in such popular applications as Vocaltec's "Internet Phone", White Pine Software's "CU-SeeMe" and Apple Computer's "QuickTime Conferencing".[49] Basically, software which implements communication of this type allows the Internet to be used as a telephone system for audio and/or video transmission, making it easy to teleconference with colleagues in far-off places at incredibly affordable prices (it is free, except for the price of the software and whatever the particular Internet provider used charges for Internet access). As with talk sessions and IRC rooms, no copies are made of the transmitted data except for those appearing on the screens of the receivers.

The obvious analogy, then, is to the normal telephone system, which has supported both audio- and videoconferencing for many years. This analogy is, for the most part, an accurate one - for instance, as in a telephone conversation, which is not transmitted as words but rather as electrical impulses which must be decoded to form words, data

transmitted as part of an IPhone session is converted to a digital form before being transmitted over the Internet. However, while this similarity means that, in theory, the interception of a normal telephone call and the interception of an IPhone session should both be prohibitively difficult, in practice it is much easier to intercept an IPhone session than it is to intercept a telephone call. Rather than having to physically patch into the telephone wires with special equipment, which is detectable by various means, all that is necessary to intercept IPhone sessions with almost no risk of being detected is to get an account on a high-traffic Internet host and write a program to watch the network for IPhone packets (a program which watches for Internet packets is called a "packet sniffer") and copy any it finds. Since the programs to decode IPhone transmission are, in general, publicly available, the packets can then be viewed at the leisure of the interceptor, who merely has to fool his copy of the program into thinking that the packets came from some other site (by resending them to himself, perhaps).

Despite the ease with which IPhone sessions can be monitored, there are ways to protect the privacy of such communications. For example, a programming group at MIT has released a program called PGPFone, which, in addition to providing standard IPhone-type sessions, encrypts the data in such a way that it cannot be decoded if intercepted by a third party. This particularly interesting use of encryption technology will be revisited as part of a discussion on encryption in general, which follows in the next chapter.

4.5. Usenet News and Analogous Services

The fifth type of computerized communication, network broadcast of textual and/or binary information from one sender to a possibly large number of receivers, has in extremely widespread use for many years. Usenet newsgroups are examples of entities which allow communications of this type, as, on a smaller scale, are "forums" on CompuServe, America Online or other online services, and even "message boards" on independently-operated bulletin board systems. The principle behind this type of communication is the following: a message containing textual and/or binary data is composed by a sender and sent to a central server, which either redistributes the message to other servers (as in the case of Usenet newsgroups) or keeps the information at one

central location for access by multiple clients (as in the case of America Online or CompuServe). Whether or not multiple copies are made of the message, it is freely accessible to anyone who has the privileges to use the resource in question, and, theoretically, *not* accessible to anyone who does not have such privileges.

One analogy which is commonly used to describe the operation of newsgroups (as I will refer to all of the various entities which allow this type of communication) is a comparison to television or radio broadcasting. The idea is that posting one's ideas in a relatively public forum such as a newsgroup is basically the same as broadcasting one's ideas over radio or television airwaves to whoever might be listening or watching. This analogy seems to be a good one. For instance, it is possible to restrict access to newsgroups to people in particular "regions" (such as our own set of "local" newsgroups here at Caltech, which are not available to people outside of Caltech's computer network), just as television and radio signals can be limited to specific geographical areas (the limitation of access in newsgroups can, however, be much more selective than that for radio and television broadcasts, allowing specific individuals to be denied access to a newsgroup where it is impossible to do so for radio or television). In addition, it is possible to "record" newsgroup discussions (in the form of data files) for archival or redistribution purposes, just as it is to record television and radio broadcasts on video- or audiocassettes.

Because this analogy seems to fit so well, it might be assumed that there are no privacy issues associated with the use of newsgroups. However, I believe that there are privacy issues involved, though not quite the same ones that arise with respect to any of the previous four types of computerized communication. One issue is that, in order to broadcast on radio or television, one need not reveal his or her identity to the listeners or viewers, whereas, in order for an individual to post a message on a newsgroup, he must provide his electronic mail address. A talk-show host on the radio need not worry about finding his mailbox at home stuffed with mail regarding his actions on the air (though, if his fans or critics are sufficiently determined, they may find his address on their own), but a person posting a message on a newsgroup does need to worry about such things. This could well be considered an invasion of the person's right to privacy, though certainly a less "serious" one than the interception of his private communications. Another potential issue is that, even

though a given newsgroup may be restricted to a specific audience, it is much easier for "outsiders" to gain access to the discussions being held therein - the packets containing the messages can be intercepted directly over the network, as with the previous forms of computerized communication, for instance. While a person broadcasting their opinions on radio or television *knows* that anybody, anywhere, has a possibility of seeing their broadcast, a person posting a message on a newsgroup is far more likely to *believe* that his "broadcast" is to a restricted audience, and, as a result, to say things which might be considered "private".

While the privacy issues associated with newsgroups are not nearly as serious as those associated with the other types of computerized communications previously mentioned, they do exist, and are deserving of at least some consideration. As with the other forms of computerized communication, there are technical solutions to the problems associated with privacy on newsgroups, which will be discussed later at some length.

4.6. The World Wide Web, Gopher and FTP

The sixth and final type of computerized communication, point-to-point broadcast of textual and/or binary information from one sender to a possibly large number of receivers with possible "return" communication from each receiver to the sender, is made possible by World Wide Web and FTP servers, as well as Gopher servers (the predecessors of the World Wide Web, which have now fallen mainly into disuse). This type of communication has grown incredibly popular, and is currently used for purposes ranging from shopping to the publication of academic papers. The basic principle behind it is as follows: Some sort of client software is used by an individual to access a specific piece of information through the use of a Universal Resource Locator (URL), which not only tells the client software which server is serving the information, but also allows the client to ask that server for that specific piece of information. No copies are made of the communicated information, except for those which appear on request at the client side and those which permanently reside on the server side of the communication, and, as with newsgroups, the use of resources on the World Wide Web, FTP and Gopher can be restricted by means of password protection or the limitation of access to people from specific Internet domains. However, like the other types of computerized communications, the information must

usually travel through multiple routers en route to the client, and so there is a risk of interception by the same methods used to intercept other computerized communications.

There is no good analogy to be drawn between this type of communication and any non-computerized communication - it is not like television or radio broadcasting, because it is interactive, yet it is also unlike a telephone conversation because it is not interactive in "real-time". In fact, since this type of communication can be used for so many different purposes, it can be compared to anything from taking a trip to the local mall to using a library to find reference materials. The privacy issues which arise from this new type of communication have to do mostly with its use for commerce, as people are required to send their credit card numbers and other identifying information over the network, and such information, as well as information about what they are purchasing and in what quantities they are purchasing it, is easily intercepted. Also, despite the possibility of making certain areas "private" by means of password protection or other restrictions, the information transmitted, even to "authorized" clients, must still travel over the same insecure network. Finally, there is the issue of privacy which arises because, when an individual accesses a World Wide Web or other server, that server is told not only where that individual is accessing it from, but also what software they are using and on which hardware platform they are running it - this could be considered an invasion of the client's privacy, in that information about their location and their machine is transmitted without their express consent (most people who "surf the net" are actually unaware that such information is sent to the servers they visit).

The privacy issues associated with the World Wide Web, FTP and Gopher are much more serious than those associated with Usenet newsgroups - in the near future, it will likely be possible to construct a pretty good profile of a person just by monitoring his World Wide Web activity, where before the advent of the Web some sort of active physical surveillance would have been necessary to do so. This is exactly analogous to the potential for violations of privacy which has existed since the advent of libraries, where records are kept of the books read by an individual. This sort of information, like that available by monitoring Web activity, can be used to build a fairly accurate profile of a person's habits, political views, and other characteristics. In the case of libraries, the issue has been resolved

in favor of privacy protection by the actions of librarians: except in very extreme cases, it is impossible to get a librarian to reveal any information regarding the borrowing habits of a specific individual. The currently soaring popularity of the World Wide Web, combined with technology which makes obtaining the type of personal information which has been fiercely protected by librarians for centuries a relatively trivial undertaking, forces this same sort of privacy issue to figure prominently in any discussion of privacy with respect to computerized communications.

4.7. Summary: The Vulnerability of Computerized Communications

All six types of computerized communication discussed in this chapter are far more vulnerable to various attacks which compromise communications privacy than are any type of normal communication. All data traveling over a network, regardless of what type of computerized communication is involved, is vulnerable to interception by sufficiently savvy programmers using commonly available equipment, whereas normal communications, such as telephone conversations or paper mail, require much more complicated means of interception. In order to eavesdrop on conversations, the modern-day voyeur or investigator need not even leave his desk - merely opening a terminal window and running a "packet sniffer" is enough. Additionally, the use of computerized communications for the transmission of important personal information such as credit card numbers, addresses, Social Security numbers and the like opens up even more avenues for the invasion of individual privacy, even if private communications are not actually monitored - breaking into a single database belonging to a popular store on the World Wide Web would give an enterprising individual access to hundreds, or even thousands, of credit card numbers and countless other bits and pieces of private, personal information.

This incredible vulnerability makes it extremely important to explicitly protect the privacy of computerized communications. There are two main avenues for doing so: the application of technical solutions, such as encryption, to protect the privacy of communications by making them more difficult to intercept; and the use of legislation, much like the currently-existing legislation which protects normal communications, to set penalties for the unauthorized interception of private communications. An examination of

the feasibility, usefulness and current status of each of these two methods of privacy protection as applied to computerized communications is the main focus of the next two chapters.

5

Technological Methods of Protecting Privacy in Computerized Communications

As we have seen, computerized communications differ from "normal" communications in several fundamental ways, which render them especially vulnerable to unauthorized interception. This vulnerability has led to the development of various technological methods for protecting the privacy of computerized communications, the most prevalent of which are encryption (in its various forms) and the use of anonymous remailers. In this chapter, I will discuss these methods, examining not only the principles behind them and the procedures for their use, but also their effectiveness for privacy protection and the feasibility of their widespread use for protecting individual privacy rights.

5.1. Encryption

5.1.1. The Concept of Encryption

The concept of encryption is an extremely old one, and various forms of encryption have been used for the purpose of ensuring communications privacy for hundreds, and perhaps thousands, of years. However, it is only within the last few years that computer technology and cryptographic theory have advanced to the point where the use of strong encryption to protect computerized communications between individuals has become at least technically feasible, if not realistically implementable. Many different cryptographic systems currently exist which can be used to protect the various types of

computerized communications, and the main variants of these will be discussed in subsequent sections of this chapter.

Encryption is, at its most basic level, a process by which a piece of information, called the "message", is encoded in such a way that any receiver of the message cannot decode it without possessing a specific piece of information called the "key" (or the "decryption key"). Encryption can be used to protect the privacy of communications, because the sender of a communication can encrypt it and then give the key only to the intended receivers of the communication. In addition, encryption can also be used to ensure that a communication comes from the source the receiver *thinks* it comes from (this is called "authentication"), as well as for other purposes. Since these other uses of encryption have no bearing on the privacy of the communications involved, they will not be discussed here - there are already many good, publicly-available references on the various uses of encryption.

There are two general classes of encryption systems. One, called "symmetric key" encryption, involves the use of a single key for both encryption and decryption. The other, called "public key encryption", involves the use of two separate keys, one for encryption and the other for decryption. These two classes of systems are useful for different types of computerized communications (though there is some overlap between them). In order to see how these types of encryption can provide effective privacy protection for the various types of computerized communications, it is necessary to examine them individually.

5.1.2. Symmetric Key Encryption Systems

Symmetric key encryption systems use a single key, called a "secret key", for both encryption and decryption of messages. The basic principle behind this class of encryption is that a function, $f(m, k)$, exists such that $f(m,k) = n$ and $f(n, k) = m$ (where m is the original message, n is the encrypted message, and k is the secret key). In other words, applying the function to the message with the secret key yields an encrypted message, and applying the function to the encrypted message with the same secret key yields the original message. $f(m,k)$ is, therefore, a "symmetric" function (which is the source for the name of this class of

encryption).

There are certain advantages to symmetric key encryption systems. For instance, it is usually easier from a computational perspective to encode a message using a symmetric key encryption system, and it is also usually easier to devise a symmetric key, which makes encryption faster under symmetric key systems than under other systems (and, since the encoding functions are symmetric, decryption takes the same amount of computation as encryption). Also, under a symmetric key system, only one key need be "remembered" for each message that is encoded. However, this leads to the one major disadvantage of symmetric key encryption systems: in order to communicate encrypted messages using a secret key system, one must also somehow communicate the secret key, and if there were a good way to securely communicate the key, there would be no need for encryption at all. At first glance, it seems that this disadvantage would cripple symmetric key encryption as an effective tool for protecting the privacy of computerized communications, since, even if a message is transmitted securely, unauthorized interception of the key renders the encryption useless.

This problem, in fact, remained unsolved until 1976, when Whitfield Diffie and Martin Hellman, in an *IEEE Transactions on Information Theory* paper entitled "New Directions in Cryptography", published what is now known as the "Diffie-Hellman Key Agreement Protocol" (also referred to as "exponential key agreement"). This protocol allowed two parties to "agree" on a single secret key to be used for a symmetric key encryption protocol, without either party having to communicate any private information insecurely. The security of the Diffie-Hellman protocol, the details of which are available from many other sources and will not be dealt with here, is based in what is known as the "discrete logarithm problem". The largest weakness in the Diffie-Hellman protocol is that it is vulnerable to the "man-in-the-middle attack": a person can intercept both sides of the protocol, "agree" upon separate keys (which are almost guaranteed to be different, because of the way the Diffie-Hellman protocol works) with each participant, and then passively relay messages between the two participants. However, this weakness can be avoided in various ways: The easiest, if the encrypted communication involves voice transmission, is for the two participants to simply read aloud to each other the key they believe they have agreed

on - if it is not the same, then there is a man-in-the-middle attack taking place. The other primary method of avoiding this weakness involves public key encryption, which will be discussed later.

Since the publishing of the Diffie-Hellman protocol in 1976, it, and variants thereof, has been widely used for many purposes, including privacy protection for computerized communications. In fact, there currently exist multiple algorithms for secret key encryption which are considered "secure" (an encryption algorithm is considered secure if a message encrypted with that algorithm cannot be decrypted without the proper key using any means easier than an exhaustive search of all the possible keys), including the "Data Encryption Standard" (DES), defined and endorsed by the U.S. government in 1977, and the "International Data Encryption Algorithm" (IDEA), designed by X. Lai and J. L. Massey in 1990.

Combined with the Diffie-Hellman protocol (with the man-in-the-middle attack vulnerability compensated for), symmetric key encryption is ideal for computerized communications which take place in real-time between two individuals (or between one individual and a server) such as talk sessions, IPhone sessions, IRC sessions, purchases made via the World Wide Web, and files transferred through the Web, Gopher or FTP. In all of these cases, the Diffie-Hellman protocol can be incorporated easily into client and server software in such a way that the encryption is completely transparent to the user, and, in many cases, it already has been. In a particularly interesting use of symmetric key encryption, Dr. Philip R. Zimmerman (no relation) of the Massachusetts Institute of Technology has written a freely-distributable program called "PGPFone", which allows voice communications over the Internet to be securely encrypted.

5.1.3. Public Key Encryption Systems

Public key encryption systems use two separate keys, one called a "public key" (from which these systems get their name) and one called a "private key". The basic principle behind this class of encryption, which was invented by Whitfield Diffie and Martin Hellman and first appears in the same paper as the Diffie-Hellman Key Agreement Protocol, is that two functions, $f(m, k)$ and $g(n, l)$ exist such that $f(m, k) = n$ and $g(n, l) = m$

(where m is the original message, n is the encrypted message, k is the public key, and l is the private key). In other words, f (the "encryption function") generates the encrypted message from the original message and the public key, and g (the "decryption function") generates the decrypted message from the encrypted message and the private key.

Every person who uses a public key encryption system needs to have both a public key, which is given to everybody from whom that person would like to receive encrypted messages, and a private key, which is never given to anybody. In this way, a message can be sent to a specific person by encrypting it with that person's public key, so that nobody who does not possess the corresponding private key will be able to read the original message. In order for this type of encryption system to be secure, there cannot be an easy way of determining the private key from the public key, from an encoded message, or even from an encoded message and its corresponding original message - in other words, the encryption function must be *one-way*, so that its inverse can not easily be calculated.

Public key encryption possesses many advantages over symmetric key encryption, the most notable of which is that there is no need to communicate secret information (the secret key) in a possibly insecure way. Another great advantage held by public key encryption is that it can be used to create what are called "digital signatures" for authentication purposes, but, again, this does not affect the privacy issue, and will not be dealt with here. Unfortunately, there are disadvantages to public key systems as well. One of these is that, in order to send a message to someone, you must know her public key - this is not a problem for a user who only communicates with one or two other people, but for a user who communicates with a large number of people, keeping track of public keys for all those individuals can be incredibly cumbersome. Another disadvantage of public key cryptography is speed, since, at least at present, there exists a faster secret key encryption algorithm comparable in security to any given public key encryption algorithm.

Despite its disadvantages in terms of speed and key management, public key encryption is ideal for computerized communications which do not take place in real-time, such as electronic mail and postings to Usenet newsgroups. Also, public key encryption can be used to protect the secret keys used in symmetric key encryption, providing the "best of both worlds" - a server can send a secret key to a client, encrypted with that client's public

key, and that secret key can then be used to encrypt subsequent communications between the server and the client. This maintains the speed advantage provided by secret key encryption systems while eliminating the security hole involved in transmission of the secret key, and, in various forms, is the system currently in use for financial transactions over the World Wide Web. Netscape Communications Corporation, for example, has incorporated a public key encryption system devised by RSA Digital Security into their "Navigator" World Wide Web browsing software, as well as into their World Wide Web server software, and many other companies have followed their lead. The public key encryption system is used instead of a Diffie-Hellman protocol to agree on a secret key for symmetric key encryption, allowing fast point-to-point transactions with some minimal setup time required for the public key encryption. Another extremely common use of public key encryption involves a protocol called "Pretty Good Privacy" (PGP), developed and publicly distributed by Dr. Philip R. Zimmerman of MIT, which allows the public key encryption and decryption of electronic mail messages (or even just files which one wishes to keep secret) on conventional UNIX, Windows or Macintosh computer systems.

5.1.4. Obstacles to Widespread Use of Strong Encryption

Clearly, the use of encryption for privacy protection can only be effective if the encryption is secure (or "strong"), meaning that it is so difficult to decode the message without possessing the key that the attempt isn't worth the effort for potential eavesdroppers. Currently, it is technically possible to implement various strong encryption algorithms on most, if not all, of the computers being used for computerized communications. In fact, the PGP program, which implements at least relatively strong encryption on standard computer systems, is freely available on the Internet. Therefore, it would seem, the privacy of computerized communications could be protected by using one or more of the currently available encryption algorithms on these machines.

Unfortunately , there are some serious barriers to the widespread adoption of encryption in computerized communications. One of these, at least in the United States, is the National Security Agency., which exists for the primary purpose of decoding encrypted communications deemed to be of importance to national security interests. In addition to

researching and developing new methods of encryption and decryption for various purposes, the NSA also regulates the export of strong encryption technologies from the United States, because these encryption technologies are currently classified as "munitions" under United States law. This regulation is the most serious obstacle to the adoption of a strong encryption standard for computerized communication, because the Internet is a worldwide network, and it is necessary for all users to have access to the same encryption algorithms in order to successfully exchange encrypted messages.

In fact, the NSA and the current Administration have proposed their own standard encryption algorithm called Skipjack (though sometimes referred to as Clipper, in reference to the computer chip which implements the algorithm), implementations of which would be publicly available (and presumably exportable). However, the details of the algorithm remain classified by the NSA, which causes most cryptology experts to distrust the algorithm - in the words of Philip Zimmerman, "a well-designed encryption algorithm does not have to be classified to remain secure,"[30] and it is natural to distrust the security of an algorithm whose details are unavailable for scrutiny. The Clipper chip, itself, is an effort on the part of the Administration to provide strong cryptography to the general public, but it uses what is known as a "key escrow" system - the government gets to keep a copy of the secret key belonging to each individual Clipper chip in one (or more) central location, to be released to law enforcement officials for duly authorized law enforcement purposes. The justification for this is, as one might expect, that the government needs to be able to intercept certain communications in the interest of national security.

Public backlash against the Clipper proposal, from corporations as well as individuals, has been overwhelming. There are multiple reasons for the backlash, the main two of which are that people don't feel that the government should have the right to intercept their private communications, and that people are worried about the security risk represented by key escrow facilities (in essence, one unauthorized access to the facility could render all the encryption devices completely useless for privacy purposes). In response, the Clipper proposal has undergone two major revisions - the Administration recently (at the time of this writing) released "Clipper III", the third-generation Clipper proposal, which now involves two separate escrowed keys per device, each of which would

be stored at a separate key escrow facility and both of which would be necessary for decryption. Of course, this doesn't do much to address the privacy issues inherent in a mandatory key escrow system, and it does little to address the security problems - it seems, therefore, to represent very little improvement over the original proposal.

The unfortunate (for the NSA, at least) fact is that, no matter what the government does to promote an encryption standard with a "trapdoor" through which they can monitor communications for law enforcement purposes, there will always be people who will use strong encryption products which do not incorporate trapdoors. Even if all strong encryption products other than those based on NSA algorithms were made illegal to own or use, the problem would remain - after all, if one is planning a terrorist attack on a major U.S. city, one is not likely to worry too terribly much about being caught using an illegal implementation of a strong encryption algorithm. Only time will tell what the ultimate result of the Clipper proposals will be - however, with bills currently being debated on the House and Senate floors which would completely legalize the export of strong cryptographic products and which strongly condemn mandatory key escrow, it seems unlikely that the Clipper system will enter widespread use anytime in the near future (it is, however, already being used for secure communications within the government).

5.1.5. Limits to Privacy Protection Provided by Encryption

Even without the problem of export restrictions, there are other difficulties which limit the effectiveness of encryption as a method for protecting the privacy of computerized communications. An important one of these is that newer and faster computer hardware is being developed every day, and with it comes newer and faster software, including the software used for decoding encrypted messages. The rapid improvement in technology will, in the relatively near future, render much of the encryption used today insecure, as even exhaustive searches for decryption keys will be able to be performed in less and less time. As a result, not only will new encryption methods have to be devised frequently, leading to difficulty in standardization, but new software will also have to be written frequently, which is guaranteed to lead to a large number of people using "obsolete" encryption at any given time. Finally, a communication encrypted today with even an exceptionally strong

encryption scheme will almost certainly not be secure many years from now, and, in general, no long-term security can be gained by the use of encryption - a truly determined person who wishes to learn the contents of an encrypted private communication will merely keep a copy of the communication until the technology is available to easily decrypt it. Of course, for most people, protection against that kind of extreme action is unnecessary - unless the data being protected is some kind of industrial trade secret, it is not only unlikely that anybody would care enough about it to wait for new technology developments in order to decrypt it, but also unlikely that the individuals involved in the communication would*care* about its decryption after enough time had passed. However, the point is an important one, as it illustrates that not even strong encryption, taken by itself, can guarantee the privacy of computerized communications.

Another limitation to the privacy protection provided by encryption is that, even if the contents of a message are encrypted, the fact that the message was sent (and its source and destination) can not be easily hidden. This can lead to privacy violations even if the contents of the messages are never discovered, because a profile of a person can be built by tracking, for example, the purchases they make using the World Wide Web. Electronic fund transfer systems exist through which people can anonymously make and receive payments, and more are being developed at the time of this writing. While these can certainly do a lot to hide the identity of the individuals involved in purchases, they cannot do anything to hide the network numbers of the computer systems involved in the transactions (because the transactions need to actually take place, somehow - even with an "electronic cash" agency in the middle, communicating with both parties, it would likely still be possible for a sufficiently savvy individual to connect buyer and seller for an individual transaction) and, if one of those computer systems is an individual's personal workstation and the other belongs to a company selling stuffed teddy bears, it is not too difficult to determine that the individual in question is buying stuffed teddy bears. Needless to say, it would take exceptional determination to build a profile of a person in this way if all the information was encrypted and sent through electronic fund transfer services (in fact, it would probably be easier to build a profile of a person based on his spending habits in the non-virtual world by following them around for a week or two), but it could be done

nevertheless.

Yet another, more practical, limitation to the privacy protection provided by encryption is the fact that currently little or no software exists to make encryption of certain kinds of communications easy (or even feasible). For instance, IRC sessions cannot easily be encrypted by the average user, nor can FTP file transfers or videoconferences. The encryption solutions which *are* currently available (with the exception of those used on the World Wide Web, which are, for the most part, completely transparent to users) are often slow and cumbersome, requiring individuals to keep track of many public keys and taking enough time to use that they become inconveniences. In order to be truly useful as a way of safeguarding individual privacy in computerized communications, encryption should ideally be transparent to users at all times unless they explicitly wish to know the details involved (which, clearly, the majority of current users of the Internet do not).

5.2. Anonymous Remailers

Another fairly widespread method of privacy protection, used mainly in posting to Usenet newsgroups but also in sending electronic mail, is the use of a service called an "anonymous remailer". The function of an anonymous remailer is simple - it assigns to you a unique ID (usually something nondescript, like "anon752") on its system, and, whenever you send a message to the remailer, it resends it to a specified destination, removing any trace of the original electronic mail address from which the message originated. Any replies sent to the unique anonymous ID are forwarded to you at your real electronic mail address. The most common use of anonymous remailers is to post nasty messages to individuals on Usenet groups without fear of recrimination, but some people use them to prevent their electronic mail addresses from being known even to those Internet users with whom they engage in intelligent conversation.

Unfortunately, the use of anonymous remailers doesn't give any real privacy protection, for many reasons. The first of these is that the privacy protection is limited by the security of the database which links anonymous IDs to real electronic mail addresses, and this is usually not extremely secure. The second is that, even if the database is secure, all an enterprising privacy violator needs to do is watch the packets going into and out from

the anonymous remailer's machine, matching the incoming messages to the outgoing messages to determine the correspondence between anonymous IDs and real electronic mail addresses. Finally, of course, unless used in combination with some form of encryption, anonymous remailers provide no privacy whatsoever for the contents of a message - they merely prevent the electronic mail address of the sender from becoming public knowledge. Since it is easy enough to ignore unwanted electronic mail (most mail readers have a "bounce" key, which returns unwanted mail to its sender), the use of anonymous remailers seems ineffective and inconvenient for any other purpose than to avoid responsibility for one's own words. While they do serve that single purpose fairly effectively - a one-time use of an anonymous remailer to send an "anonymous tip" to a law enforcement agency, for example, would (unless the remailer's database was compromised) protect the privacy of the informant reasonably well - they do not do anything to address the problem of privacy for the contents of computerized communications, nor do they do anything to address the issue of individual privacy in any type of computerized communication other than electronic mail and Usenet news.

5.3. Summary: The Effectiveness of Technical Solutions

As we have seen, encryption is the primary technological solution for the problem of ensuring privacy in computerized communications. Anonymous remailers, while they address one very small issue, do not do much to protect individual privacy for the average user of computerized communication systems. However, even publicly-available strong encryption would not solve the privacy problem - people's messages, as noted previously, could still be traced to them, even if the specific contents of those messages could not be decrypted, and encryption is still not a feasible option for protecting the privacy of many of the forms of computerized communication which have been discussed. In addition, encryption, as well as any other possible technical solution, has the fundamental weakness that technology is always, in time, overtaken by better technology. It would seem, then, that even though technical solutions like encryption can enhance the privacy of computerized communications, more than a technical solution is necessary to ensure that the privacy rights of individuals using these new methods of communication are, and continue to be,

protected.

6

Legislation for Protecting Privacy in Computerized Communications

In the United States, laws protecting the privacy of "electronic communications" already exist. These are primarily contained in two chapters of Title 18 of the U.S. Code, which deals with crimes and criminal procedure. In addition, encryption rights bills currently being debated in the House and Senate at the time of this writing have the potential to profoundly affect the privacy rights of individuals with respect to computerized communications. In this chapter, the laws currently in force as well as the bills currently being debated will be examined to determine exactly how much privacy protection they provide (or will provide) for computerized communications.

6.1. United States Code, Title 18, Chapters 119 and 121

Chapter 119 of Title 18 of the United States Code, commonly known as the "Electronic Communications Privacy Act of 1986" (and hereafter referred to as "the ECPA"), is meant to protect the right to privacy in "electronic communications" by setting forth penalties for unauthorized interception of communications as well as detailing the conditions under which interception can be authorized for law enforcement or other purposes. However, because this legislation was passed before many of the types of computerized communication described in Chapter 4 even existed, and at a time when those which did exist were far less commonly used than they are today, it does not protect the privacy of all six forms of computerized communication equally. In fact, depending on

the interpretation of the law, there are some forms of computerized communication for which the ECPA provides no protection whatsoever.

18 USC 2510, the "definitions" section of the ECPA, defines several terms in ways which make it difficult to apply the ECPA, as written, to certain types of computerized communication. Of the definitions provided in §2510, the ones important to the present analysis are as follows[51] (note that some details, such as those regarding "tone-only paging devices" and those regarding special radio frequencies, have been omitted because of their lack of relevance):

> "aural transfer" *means a transfer containing the human voice at any point between and including the point of origin and the point of reception.*
>
> "wire communication" *means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication...*
>
> "oral communication" *means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication.*
>
> "electronic communication" *means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include...any wire or oral communication...*
>
> "electronic communications system" *means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.*
>
> "electronic communication service" *means any service which provides to users thereof the ability to send or receive wire or electronic communications.*
>
> "readily accessible to the general public" *means,* ***with respect to a radio communication***[52] *, that such communication is not: a) scrambled or encrypted; b) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication; c) carried on a subcarrier or other signal subsidiary to a radio transmission; d) transmitted over a communication system provided by a common carrier...*

These terms are used throughout the remainder of the ECPA, and, as we shall see, though their definitions allow the ECPA to provide adequate privacy protection for conventional electronic communications such as telephone calls, they prevent it from providing adequate protection for computerized communications.

The first difficulty with these definitions is the requirement that, to be considered an "electronic communication" or a "wire communication", a communication must "affect interstate or foreign commerce" or be transmitted using facilities which are operated for the purpose of providing interstate or foreign communications. Clearly, any communication on the Internet would fit under these definitions, since the Internet is a worldwide network and any site providing Internet access is clearly providing interstate or foreign communications. However, communications over local-area networks (such as those which might be found within a company's headquarters), or communications made directly between two computers within the same state using a dedicated line, might not fit under these definitions. However, it seems that all computerized communications, regardless of whether or not they cross state lines, should be equally entitled to protection, and therefore these definitions are inadequate for protecting all computerized communications.

Ignoring the "interstate or foreign commerce" issue, however, there is yet another difficulty with the application of these definitions to computerized communications. Applying the definitions to the various types of computerized communications previously discussed, it is clear that most fall under the category of "electronic communications", because they involve the transfer of signals over wires, but do not involve the transmission of the human voice at any point. IPhone sessions, however, *do* involve the transmission of the human voice, and would therefore seem to fall under the category of "wire communications" because, by virtue of containing the human voice, they are "aural transfers". To complicate the matter further, it is possible to use electronic mail, which would presumably be considered an "electronic communication", to send a digitized sample of a person's voice - this would force the electronic mail in question to be considered a "wire communication", since an "aural transfer" is now involved. This duality seems counter to the goal of protecting the privacy of computerized communications - after all, it makes no sense for typed and

spoken electronic mail messages to be regarded differently under the law.

Even if all computerized communications were categorized as electronic communications under the ECPA, though, it still would be inadequate for the purpose of protecting computerized communications privacy. The protections provided for electronic communications under the ECPA are as follows: §2511 states that, except under specific circumstances, any person who intercepts any wire, oral or electronic communication, or who has any other person do so on his behalf, shall be either punished (by means of a fine, imprisonment for up to five years, or both) or subject to suit. Similarly, any person who intentionally discloses or uses the contents of any wire, oral or electronic communication with the knowledge that such information was obtained in violation of the ECPA shall also be either punished or subject to suit. §2512 states that, except under specific circumstances, the manufacture, distribution, possession or advertising of devices whose primary function is to intercept wire, oral or electronic communications is prohibited, and is punishable by imprisonment (for up to five years) and fines (of up to $10,000). §2513 gives the government the right to seize any devices which violate §2511 or §2512, and §2515 prohibits the use of any intercepted wire or oral communications as evidence in a U.S. court of law. The remaining sections of the ECPA detail the exact procedures for obtaining authorization to intercept wire, oral or electronic communications, the circumstances under which such authorization can be legally granted, and the uses to which communications intercepted with such authorization can be put. The details of these sections are relatively unimportant - in summary, authorization for interception of an individual's communications can be granted if there are reasonable grounds for belief that the individual has committed, is committing, or will commit one of several specific crimes detailed in §2516, including all capital offenses as well as kidnapping, robbery, extortion, bribery, and many more.

On the surface, the ECPA, if enforced, would seem to do an adequate job of protecting electronic communications privacy. In fact, for all of the types of electronic communications in common use at the time the ECPA was signed into law, it does do so. However, some of the "specific circumstances" under which interception of communications is legal under the ECPA, combined with the definitions of terms used in the ECPA, provide large loopholes which render the interception of most types of

computerized communication completely legal under the ECPA.

The first, and largest, of these loopholes is opened by §2511, subsection (2), paragraph (g), which states:

> *It shall not be unlawful under this chapter or chapter 121 of this title for any person to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is* ***readily accessible to the general public****.*[53]

The loophole in this clause lies in the phrase "readily accessible to the general public". As can be easily seen by looking at the definition, this term, for the purposes of the ECPA, was only defined in the context of radio communications. Of course, none of the five types of computerized communications which fall under the umbrella term of electronic communications in the ECPA could be considered radio communications, so it is necessary to determine what the phrase "readily accessible to the general public" means when applied to them.

Extrapolating from the definition applied to radio communications, a computerized communication could be considered to be readily accessible to the general public if it was not scrambled or encrypted, and was not transmitted over an electronic communication system provided by a "common carrier". For the most part, however, computerized communications are *not* encrypted, for the reasons cited previously. In addition, the Internet as a whole cannot be considered a common carrier for many reasons, chief among them being that it is not a single entity but, rather, a collection of computers connected to each other in a myriad of ways. It might be possible to classify individual Internet service providers as common carriers, but there will always be individual machines on the Internet which cannot fall under such a classification. Therefore, at least until encryption becomes commonplace or the criteria for common carrier status change drastically, *all* computerized communications must be considered to be readily accessible to the general public.

In fact, it makes sense that all six types of computerized communication are considered to be readily accessible to the general public, assuming that the general public in this case consists of people with Internet access. After all, anybody with a "packet sniffer" program (many of which can be found on the Internet itself, in publicly accessible

places) and a little bit of time on their hands can intercept anything traveling over their segment of the Internet. Unfortunately, this renders the ECPA nearly useless for protecting the privacy of computerized communications other than IPhone sessions, which are classified as wire communications, and possibly other computerized communications which exhibit the "electronic/wire" duality previously discussed.

In addition, there is another major loophole in the ECPA with respect to computerized communications, which is caused by a clause of §2511, subsection (3). This clause states:

> *A person or entity providing electronic communication service to the public may divulge the contents of any such communication...to a person employed or authorized,* ***or whose facilities are used****, to forward such communication to its destination...*

Since, in almost all cases, computerized communications involve the routing of data packets through multiple machines, this clause makes the contents of all computerized communications routed through a specific system legally available to the administrator of that system, regardless of the ultimate destination of such communications. The problem, of course, is that the administrator of a system is basically given the right to monitor the communications of anybody on his own system, as well as anybody on any system whose communications are routed through any piece of equipment on his local network, without ever informing the participants in the communication that they are being monitored. Since the great majority of Internet users have no reason to suspect that their communications may be monitored, and much less reason to suspect that such monitoring is completely legal, this loophole is a very serious one, which seems to eliminate any effectiveness the ECPA may have, after considering the first loophole, with respect to computerized communications.

Aside from these two loopholes in the ECPA, there is also a rather striking omission in §2515, the section which prohibits the use of intercepted communications as evidence. §2515 says that no part of an intercepted wire or oral communication can be used as evidence in any court proceeding if the disclosure of the contents of the communication would be in violation of the ECPA. However, it says nothing whatsoever about the use of intercepted *electronic* communications as evidence in court proceedings, which implies that

intercepted electronic communications can, in fact, be admitted as evidence. This is a serious problem, as it provides a powerful incentive for the routine interception of computerized communications: since system administrators are legally entitled under the ECPA to know the contents of all computerized communications (except IPhone sessions) passing through their systems, it is easy to, for example, pass all these communications through some kind of keyword filter and highlight those which deal with potentially illegal activity, not only allowing the system administrator to notify law enforcement officials but also allowing said law enforcement officials to use the communications in question against the individual(s) involved, without ever needing reasonable grounds for suspecting criminal activity. This neatly circumvents all the precautions taken in the remaining sections of the ECPA to prevent unauthorized interception of communications and, based on our prior discussion of the individual's right to privacy and the right to private communications, is a clear violation of the privacy rights of the individual(s) involved.

In addition to the ECPA proper, Chapter 121 of Title 18 of the United States Code[54] also has some bearing on the privacy of computerized communications. This chapter deals with the circumstances under which stored electronic communications can be divulged to third parties, as well as protecting video tape rental records from wrongful disclosure. While Chapter 121 does not provide any real protection for privacy in computerized communications, it does provide a starting point for the protection of privacy in one area: transactions made via the World Wide Web.

Chapter 121 mandates a punishment of imprisonment, fines or both for intentional unauthorized access to a facility through which an electronic communication service is provided, which is meant to deter individuals from breaking into electronic communication service facilities for the purpose of obtaining, altering or preventing authorized access to electronic communications stored within. In addition, it authorizes the awarding of not only actual damages, but also punitive damages, attorneys' fees and, "such other preliminary and equitable relief as the court determines to be appropriate," for the wrongful disclosure of video tape rental records containing personally identifiable information about a consumer. This part of Chapter 121 is only applicable to video tape rentals, but it clearly provides a precedent which can be extended to commerce conducted

via the World Wide Web - if it was to actually be extended in such a way as to include that commerce, the protection of individual privacy for at least that one type of computerized communication would be enhanced, despite not being completely protected (since, after all, packet interception would still be possible, and there are still the major loopholes in the ECPA).

Clearly, the ECPA and Chapter 121 cannot effectively protect any of the types of computerized communications which have been discussed (except for Internet Phone conversations which, based on the definitions given in the ECPA, are basically treated as equivalent to normal telephone conversations for the purposes of the law). In order to effectively protect the privacy of computerized communications, either the ECPA must be amended or a new set of laws dealing specifically with computerized communications must be devised.

6.2. Encryption Rights Bills

On March 5, 1996, the "Security and Freedom through Encryption Act" (H.R. 3011) was introduced in the House of Representatives at the same time as the "Encrypted Communications Privacy Act of 1996 " (S. 1587) was introduced in the Senate[65] . Both of these bills sought to, "affirm the rights of Americans to use and sell encryption," by amending Title 18 of the United States Code with a new chapter, Chapter 122, entitled "Encrypted Wire and Electronic Communications".

Both the House and Senate bills allow for voluntary key escrow systems and prohibit mandatory release of a lawfully possessed key except when necessary for law enforcement purposes. The Senate bill, which is far more lengthy and detailed than the House bill, also sets forth detailed requirements and responsibilities for key holders, including the requirement that a key only be released with the consent of the person who owns the key except in a case where law enforcement officials are authorized under the ECPA or Chapter 121 to intercept communications or view records encrypted with that key. Additionally, requirements for law enforcement officers are set forth such that an officer to whom a key has been released may only use that key for the purpose set forth in the court order authorizing the key's release.

Both bills also provide for the freedom of any person within the United States, as well as any United States citizen in a foreign country, to either use or sell encryption technology regardless of the key length or specific implementation chosen, as long as comparable products are already commercially available from non-U.S. suppliers and, in the case of encryption software, as long as there is no substantial evidence that the software will either be used for military or terrorist purposes or be reexported without U.S. authorization. These described additions to Title 18 almost completely eliminate the export restrictions on encryption technology, which are currently among the greatest barriers to the protection of privacy in computerized communications.

Unfortunately, neither of these bills has passed and, even if both had, since they do not contain identical language they would still not have become law. However, on May 2, 1996, the Senate introduced another encryption rights bill, the "Promotion of Commerce On-Line in the Digital Era Act of 1996,"[56] (S. 1726, hereafter referred to as "Pro-CODE") the main goal of which is, "to promote electronic commerce by facilitating the use of strong encryption." In the "findings" section of this bill, the authors state:

> *Encryption of information enables businesses and individuals to protect themselves against the unauthorized viewing, alteration, and use of information by employing widely understood and readily available science and technology to ensure the confidentiality, authenticity, and integrity of information.*

In other words, encryption will help protect individual privacy in computerized communications, since the protection of communications privacy mainly involves preventing unauthorized access to information. Additionally, the bill specifically condemns any sort of mandatory key escrow system (such as the failed Clipper and Clipper II systems, and Clipper III, the most recent Clipper policy, proposed on May 22, 1996) by saying not only that, "there is no demonstrated commercial demand for features which give governments easy access to information," but also that, "the Federal Government should be prohibited from promulgating regulations and adopting policies that discourage the use and sale of encryption."

The Pro-CODE bill goes on to specifically restrict the Department of Commerce from imposing government-designed encryption systems on any computer systems other than those belonging to the federal government and from restricting export

of encryption technologies. In fact, if Pro-CODE passes, the only remaining export restriction will be that the export of software or hardware containing encryption technology will be prohibited if there is good reason to assume that said software or hardware will be either used for military or terrorist purposes or reexported without authorization from the United States (this is just like the restrictions left intact by the previous two bills, except that it includes both hardware and software, where the previous two bills restricted only software).

While Pro-CODE is clearly designed to facilitate electronic commerce, the encryption systems which will be made available under the bill, should it pass, are not applicable only to electronic commerce such as that conducted over the World Wide Web. Such encryption systems can also be used to protect electronic mail, messages posted via Usenet news, and files transmitted via Gopher or FTP (or the World Wide Web, for that matter). Assuming some enterprising programmers take up the gauntlet, encryption can even be used to protect talk sessions, IRC sessions, and (as is already being done using applications such as MIT's "PGPFone") IPhone sessions. Clearly, the passage of this legislation is in the best interest of everyone who values the privacy of computerized communications.

6.3. Summary: Current Legislation is Not Enough

Unfortunately, even if Pro-CODE passes, there will (at least for the foreseeable future) always be individuals for whom the use of encryption is too inconvenient, or too technically difficult, to be feasible as a routine method of protecting computerized communications such as electronic mail. The Electronic Communications Privacy Act, as previously shown, provides basically no protection whatsoever for the privacy of unencrypted computerized communications, which leaves such individuals completely vulnerable to violations of their communications privacy. It would appear, then, that new legislation dealing explicitly with the various forms of computerized communications should be enacted to protect privacy in such communications.

7
Conclusion & Recommendations

Computerized communications provide incredible convenience and flexibility to those who use them - they allow people to shop, look up articles in encyclopedias and newspapers, and talk to (and even see) colleagues on the other side of the globe, all from in front of a normal desktop computer. The number of people taking advantage of these new methods of communicating increases every day, and will continue to do so for the foreseeable future. With the great increase in the number of users of computerized communications, the privacy issues generated by them have become critically important.

In Chapters 2 and 3, the concepts of privacy and private communications were illustrated, and it became clear not only that the existence of private communications was important as a means of facilitating many different types of human interaction, but also that individuals had a right to engage in private communications. The existence of this right had, in fact, already been acknowledged by the U.S. government (among other entities), with the passage of laws, such as the Electronic Communications Privacy Act of 1986, which protect communications from unauthorized interception.

As shown in Chapter 4, each of the various types of computerized communication (except for use of the World Wide Web, FTP and Gopher) is directly analogous to a specific type of "normal" communication, the privacy of which is already protected under United States law (and the law in several other countries as well). Even use of the World Wide Web has a direct analogue (though not in the field of communications)

with respect to privacy issues, namely, the use of a public library, where records of the books borrowed by individuals are kept private under all but the most extreme circumstances. Because they are so similar to "normal" types of communication (or other types of interaction) for which privacy rights have already been affirmed, it is only natural that privacy rights also exist for the various types of computerized communication, and that they should be protected in the same way as privacy rights for the various normal types of communication.

Unfortunately, it is far more difficult to protect the right to privacy in computerized communications than in normal communications, because of the extreme vulnerability of computerized communications to illicit interception. Evidence of this difficulty can be seen in the fact that the ECPA, almost certainly meant to protect at least electronic mail (which was, though rare, in use at the time, especially in universities and large corporations), is completely inadequate for the purpose of protecting the privacy of *any* type of computerized communication. Those users of computerized communications who feel that they must take measures of their own to protect their privacy rights have resorted to publicly-available encryption, such as PGP, but because of current government policy regarding the export of strong encryption products, such solutions are ineffective for the protection of privacy on a global network such as the Internet. In addition, the encryption products currently available to the public are cumbersome to use and are only effective at protecting a very limited subset of computerized communications. Clearly, there must be a way to improve the situation, so that the privacy of *all* computerized communications is protected regardless of the computing ability or patience of the people communicating. In fact, it seems that there are two actions which should be taken to protect privacy rights in computerized communications.

First, new legislation, analogous to the ECPA, which explicitly protects the privacy of all the types of computerized communications discussed in Chapter 4, should be passed by the federal government. Such legislation can unquestionably be written in such a way that the loopholes in the ECPA would be closed, and, using a system of passive enforcement, would almost definitely be effective to some degree. This would place computerized communications on an equal legal footing with normal communications,

which seems appropriate given the fact that they are likely to become the dominant methods of communication over the coming years. The legal protection provided by such new legislation would also make people who are currently reluctant to use computerized communications more likely to do so, and will therefore increase the number of people who take advantage of the incredible convenience and economy provided by computerized communications.

New legislation, however, will not be enough to provide protection for computerized communications equal to that for normal communications, because the increased vulnerability of computerized communications to interception will still be present. Therefore, it is also necessary to make strong encryption technologies accessible to the general public, so that those who want to take advantage of the additional measure of protection provided by encryption can do so conveniently and effectively. Similarly, the export restrictions on strong encryption products should be, if not eliminated entirely, at least loosened such that people within the United States and people outside the United States can use the same encryption technologies to communicate with each other. Once an encryption rights law, such as one of the three mentioned in the previous chapter, is passed, software developers will almost certainly take up the gauntlet and develop new and easy implementations of strong encryption algorithms for use by the general public. Following the example of PGPFone and Netscape, computerized communication tools in which encryption is used in a fashion completely transparent to the user, there will eventually be applications for all the types of computerized communication which provide practically effortless privacy protection. Using such systems, people would finally be able to take full advantage of computerized communication in all its forms without fear of having their privacy invaded, protected by both federal legislation and their own use of encryption.

As I have shown, the right to privacy in computerized communications does exist, just as certainly as the right to privacy in normal communications. It has, up until very recently, been inexplicably ignored not only by the federal government but also by the providers of computerized communication services. Because of the rapidly increasing number of people using various types of computerized communications, however, the status quo is no longer acceptable. In order to allow individuals to take full advantage of the

potential represented by these new methods of communicating, the privacy issues associated with their use must be explicitly addressed by both the government and service providers. The implementation of a combined strategy of legislation and publicly-available encryption would not only acknowledge the existence of these issues, but also provide real protection for the privacy of the millions of people who regularly use computerized communications.

A

Text of United States Code, Title 18, Chapter 119 ("Electronic Communications Privacy Act of 1986")

The following is the complete text of the United States Code, Title 18, Chapter 119 (more commonly known as the "Electronic Communications Privacy Act of 1986"), from the Legal Information Institute at Cornell University Law School:

UNITED STATES CODE
TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
CHAPTER 119 - WIRE AND ELECTRONIC COMMUNICATIONS
INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

§2510. Definitions

As used in this chapter:

(1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than:

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

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

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means:

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) "communication common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) of title 47 of the United States Code;

(11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include:

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

(b) any wire or oral communication;

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

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

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

(a) uses an electronic communication service; and

(b) is duly authorized by the provider of such service to engage in such use;

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

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not:

(a) scrambled or encrypted;

(b) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(c) carried on a subcarrier or other signal subsidiary to a radio transmission;

(d) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(e) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) "electronic storage" means:

(a) any temporary, intermediate storage of a wire or electronic communication

incidental to the electronic transmission thereof; and

(b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and

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

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

(1) Except as otherwise specifically provided in this chapter any person who:

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

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

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)

(a)

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

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

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

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

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

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

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

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

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

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

(ii) to intercept any radio communication which is transmitted:

(A) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(B) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

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

(D) by any marine or aeronautical communications system;

(iii) to engage in any conduct which:

(A) is prohibited by section 633 of the Communications Act of 1934; or

(B) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

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

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

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

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

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(3)

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

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

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)

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

(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled or encrypted, then:

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

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

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

(i) to a broadcasting station for purposes of retransmission to the general public; or

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

(5)

(a)

(i) If the communication is:

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

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

(ii) In an action under this subsection:

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

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

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

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

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

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

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

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

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications, knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce, shall be fined not more than $10,000 or imprisoned not more than five years, or both.

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

(a) a provider of wire or electronic communication service or an officer, agent, or

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

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

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

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

§2514. Repealed

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

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

§2516. Authorization for interception of wire, oral, or electronic communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any

Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of:

(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relating to sabotage), chapter 115 (relating to treason), chapter 102 (relating to riots), chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 1014 (relating to loans and credit applications generally; renewals and discounts), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1751 (Presidential and Presidential staff assassination, kidnaping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), sections 2251 and 2252 (sexual exploitation of children), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal

official), and section 1341 (relating to mail fraud), section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnaping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), or section 1992 (relating to wrecking trains);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions);

(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

(i) any felony violation of chapter 71 (relating to obscenity) of this title;

(j) any violation of section 11(c)(2) of the Natural Gas Pipeline Safety Act of 1968 (relating to destruction of a natural gas pipeline) or subsection (i) or (n) of section 902 of the Federal Aviation Act of 1958 (relating to aircraft piracy);

(k) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act);

(l) the location of any fugitive from justice from an offense described in this section; or[57]

(m) any felony violation of sections 922 and 924 of title 18, United States Code (relating to firearms);

(n) any violation of section 5861 of the Internal Revenue Code of 1986 (relating to firearms); and[58]

(o) any conspiracy to commit any offense described in any subparagraph of this paragraph.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in

conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

§2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be

used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

§2518. Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that:

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify:

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained. An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that:

(a) an emergency situation exists that involves:

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime, that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception, may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the

application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8)

(a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of:

(i) the fact of the entry of the order or the application;

(ii) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(iii) the fact that during the period wire, oral, or electronic communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to

such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)

(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that:

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such

communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if:

(a) in the case of an application with respect to the interception of an oral communication:

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(iii) the judge finds that such specification is not practical; and

(b) in the case of an application with respect to a wire or electronic communication:

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and

(iii) the judge finds that such purpose has been adequately shown.

(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.

§2519. Reports concerning intercepted wire, oral, or electronic communications

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United

States Courts:

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for (including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title);

(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension of an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts:

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, and (iv) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

§2520. Recovery of civil damages authorized

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

(2) Relief. In an action under this section, appropriate relief includes:

(a) such preliminary and other equitable or declaratory relief as may be appropriate;

(b) damages under subsection (c) and punitive damages in appropriate cases; and

(c) a reasonable attorney's fee and other litigation costs reasonably incurred.

(3) Computation of Damages.

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

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

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

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

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

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

(4) Defense. A good faith reliance on:

(a) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(b) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(c) a good faith determination that section 2511(3) of this title permitted the conduct complained of

is a complete defense against any civil or criminal action brought under this chapter or any other law.

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

§2521. Injunction against illegal interception

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

B

Text of United States Code, Title 18, Chapter 121

The following is the complete text of the United States Code, Title 18, Chapter 121, from the Legal Information Institute at Cornell University Law School:

UNITED STATES CODE
TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
CHAPTER 121 - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

§2701. Unlawful access to stored communications

(a) Offense. Except as provided in subsection (c) of this section, whoever:

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

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

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain:

(A) a fine of not more than $250,000 or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than two years, or

both, for any subsequent offense under this subparagraph; and

(2) a fine of not more than $5,000 or imprisonment for not more than six months, or both, in any other case.

(c) Exceptions. Subsection (a) of this section does not apply with respect to conduct authorized:

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

§2702. Disclosure of contents

(a) Prohibitions. Except as provided in subsection (b):

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service:

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(b) Exceptions. - A person or entity may divulge the contents of a communication:

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or

(6) to a law enforcement agency, if such contents:

(A) were inadvertently obtained by the service provider; and

(B) appear to pertain to the commission of a crime.

§2703. Requirements for governmental access

(a) Contents of Electronic Communications in Electronic Storage. A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of Electronic Communications in a Remote Computing Service.

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection:

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity:

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service:

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing

services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records Concerning Electronic Communication Service or Remote Computing Service.

(1)

(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to any person other than a governmental entity.

(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental entity:

(i) uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury or trial subpoena;

(ii) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant;

(iii) obtains a court order for such disclosure under subsection (d) of this section; or

(iv) has the consent of the subscriber or customer to such disclosure.

(2) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for Court Order. A court order for disclosure under subsection (b) or (c) of this section may be issued by any court that is a court of competent jurisdiction set forth in section 3126(2)(A) of this title and shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No Cause of Action Against a Provider Disclosing Information Under This Chapter. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, or certification under this chapter.

§2704. Backup preservation

(a) Backup Preservation.

(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

(3) The service provider shall not destroy such backup copy until the later of:

(A) the delivery of the information; or

(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider:

(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(B) has not initiated proceedings to challenge the request of the governmental entity.

(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

(b) Customer Challenges.

(1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application

shall contain an affidavit or sworn statement:

(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure.

(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

§2705. Delayed notice

(a) Delay of Notification.

(1) A governmental entity acting under section 2703(b) of this title may:

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under

section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is:

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that:

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer or subscriber:

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay. (6) As used in this

subsection, the term "supervisory official" means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) Preclusion of Notice to Subject of Governmental Access. A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in:

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

§2706. Cost reimbursement

(a) Payment. Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) Amount. The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) Exception. The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually

voluminous in nature or otherwise caused an undue burden on the provider.

§2707. Civil action

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

(b) Relief. In a civil action under this section, appropriate relief includes:

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages. The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000.

(d) Defense. A good faith reliance on:

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of; is a complete defense to any civil or criminal action brought under this chapter or any other law.

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

§2708. Exclusivity of remedies

The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

§2709. Counterintelligence access to telephone toll and transactional records

(a) Duty to Provide. A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information,

or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required Certification. The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director, may:

(1) request the name, address, length of service, and toll billing records of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that:

(A) the name, address, length of service, and toll billing records sought are relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801); and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that:

(A) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific and articulable facts giving reason to believe that communication facilities registered in the name of the person or entity have been used, through the services of such provider, in communication with:

(i) an individual who is engaging or has engaged in international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act[59] or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States; or

(ii) a foreign power or an agent of a foreign power under circumstances giving reason to believe that the communication concerned international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act[60] or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States.

(c) Prohibition of Certain Disclosure. No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) Dissemination by Bureau. The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau

of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement That Certain Congressional Bodies Be Informed. On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

§2710. Wrongful disclosure of video tape rental or sale records

(a) Definitions. For purposes of this section:

(1) the term "consumer" means any renter, purchaser, or subscriber of goods or services from a video tape service provider;

(2) the term "ordinary course of business" means only debt collection activities, order fulfillment, request processing, and the transfer of ownership;

(3) the term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider; and

(4) the term "video tape service provider" means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

(b) Video Tape Rental and Sale Records.

(1) A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).

(2) A video tape service provider may disclose personally identifiable information concerning any consumer:

(A) to the consumer;

(B) to any person with the informed, written consent of the consumer given at the time the disclosure is sought;

(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;

(D) to any person if the disclosure is solely of the names and addresses of consumers and if:

(i) the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and

(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;

(E) to any person if the disclosure is incident to the ordinary course of business of the video tape service provider; or

(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if:

(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure. If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the video tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

(c) Civil Action.

(1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.

(2) The court may award:

(A) actual damages but not less than liquidated damages in an amount of $2,500;

(B) punitive damages;

(C) reasonable attorneys' fees and other litigation costs reasonably incurred; and

(D) such other preliminary and equitable relief as the court determines to be appropriate.

(3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.

(4) No liability shall result from lawful disclosure permitted by this section.

(d) Personally Identifiable Information. Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State.

(e) Destruction of Old Records. A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order.

(f) Preemption. The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.

§2711. Definitions for chapter

As used in this chapter:

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

C

Text of H.R. 3011 ("Security and Freedom Through Encryption Act")

The following is the complete text of H.R. 3011, also known as the "Security and Freedom Through Encryption Act" (or the "SAFE Act"), which was introduced by Representative Goodlatte during the second session of the 104th Congress, in March 1996.

A BILL

To amend title 18, United States Code, to affirm the rights of Americans to use and sell encryption, and to relax export controls on encryption.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Security and Freedom Through Encryption (SAFE) Act".

SECTION 2. SALE AND USE OF ENCRYPTION.

(a) IN GENERAL. Part I of title 18, United States Code, is amended by inserting after chapter 121 the following new chapter:

CHAPTER 122: ENCRYPTED WIRE AND ELECTRONIC COMMUNICATIONS

§2801. Definitions

§2801. Definitions

As used in this chapter:

(1) the terms 'person', 'State', 'wire communications, electronic communication', 'investigate or law enforcement officer', 'judge of competent jurisdiction', and 'electronic storage' have the meanings given those terms in section 2510 of this title;

(2) the terms 'encrypt' and 'encryption' refer to the scrambling of wire or electronic information using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such communications;

(3) the term 'key' means the variable information used in a mathematical formula, code, or algorithm, or any component thereof, used to decrypt wire or electronic communications that have been encrypted; and

(4) the term 'United States person' means:

(A) any United States citizen;

(B) any other person organized under the laws of any State, the District of Columbia, or any commonwealth, territory, or possession of the United States; and

(C) any person organized under the laws of any foreign country who is owned or controlled by individuals of persons described in subparagraphs (A) and (B).

§2802. Freedom to use encryption

Subject to Section 2805, it shall be lawful for any person within any State, and for any United States citizen in a foreign country, to use any encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.

§2803. Freedom to sell encryption

Subject to section 2805, it shall be lawful for any person within any State to sell in interstate commerce any encryption, regardless of the encryption algorithm selected encryption key length chosen, or implementation technique or medium used.

§2804. Prohibition on mandatory key escrow

(a) PROHIBITION. No person in lawful possession of a key to encrypted information may be required by Federal or State law to relinquish to another person control of that key.

(b) EXCEPTION FOR ACCESS FOR LAW ENFORCEMENT PURPOSES. Subsection (a) shall not affect the authority of any investigative or law enforcement officer, under any law in effect on the effective date of this chapter, to gain access to a key to encrypted information.

§2805. Unlawful use of encryption in furtherance of a criminal act

Any person who willfully uses encryption in furtherance of the commission of a criminal offense for which the person may be prosecuted in a court of competent jurisdiction:

(1) in the case of a first offense under this section, shall be imprisoned for not more than 5 years, or fined in the amount set forth in this title, or both; and

(2) in the case of a second or subsequent offense under this section, shall be imprisoned for not more than 10 years, or fined in the amount set forth in this title, or both.

(b) CONFORMING AMENDMENT. The table of chapters for Part I of title 18, United States Code, is amended by inserting after the item relating to chapter 33 the following new item:

122. Encrypted wire and electronic communications .... 2801.

SECTION 3. EXPORTS OF ENCRYPTION.

(a) AMENDMENT TO EXPORT ADMINISTRATION ACT OF 1979. Section 17 of the Export Administration Act of 1979 (50 U.S.C. App. 2416) is amended by adding at the end thereof the following new subsection:

(g) COMPUTERS AND RELATED EQUIPMENT.

(1) GENERAL RULE. Subject to paragraphs (2), (3), and (4), the Secretary shall have exclusive authority to control exports of all computer hard ware, software, and technology for information security (including encryption), except that which is specifically designed, or modified for military use, including command, control, and intelligence applications.

(2) ITEMS NOT REQUIRING LICENSES. No validated license may be required, except pursuant to the Trading With the Enemy Act or the International Emergency Economic Powers Act (but only to the extent that the authority of such Act is not exercised to extend controls imposed under this Act), for the export or reexport of:

(A) any software, including software with encryption capabilities:

(i) that is generally available, as is, and is designed for installation by the purchaser; or

(ii) that is in the public domain for which copyright or other protection is not available under title 17, United States Code, or that is available to the public because it is generally accessible to the interested public in any form; or

(B) any computing device solely because it incorporates or employs in any form software (including software with encryption capabilities) exempted from any requirement for a validated license under subparagraph (A).

(3) SOFTWARE WITH ENCRYPTION CAPABILITIES. The Secretary shall authorize the export or reexport of software with encryption capabilities for nonmilitary end-uses in any country to which exports of software of similar capability are permitted for use by financial institutions not controlled in fact by United States persons, unless there is substantial evidence that such software will be:

(A) diverted to a military end-use or an end-use supporting international terrorism;

(B) modified for military or terrorist end-use; or

(C) reexported without any authorization by the United States that may be required under this Act.

(4) HARDWARE WITH ENCRYPTION CAPABILITIES. The Secretary shall authorize the export or reexport of computer hardware with encryption capabilities if the Secretary determines that a product offering comparable security is commercially available outside the United States from a foreign supplier, without effective restrictions.

(5) DEFINITIONS. As used in this subsection:

(A) the term 'encryption' means the scrambling of wire or electronic information using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such information;

(B) the term 'generally available' means, in the case of software (including software with encryption capabilities), software that is offered for sale, license, or transfer to any person without restriction, whether or not for consideration, including, but not limited to, over-the-counter retail sales, mail order transactions, phone order transactions, electronic distribution, or sale on approval;

(C) the term 'as is' means, in the case of software (including software with encryption capabilities), a software program that is not designed, developed, or tailored by the software publisher for specific purchasers,

except that such purchasers may supply certain installation parameters needed by the software program to function properly with the purchaser's system and may customize the software program by choosing among options contained in the software program;

(D) the term 'is designed for installation by the purchaser' means, in the case of software (including software with encryption capabilities) that:

(i) the software publisher intends for the purchaser (including any licensee or transferee), who may not be the actual program user, to install the software program on a computing device and has supplied the necessary instructions to do so, except that the publisher may also provide telephone help line services for software installation, electronic transmission, or basic operations; and

(ii) the software program is designed for installation by the purchaser without further substantial support by the supplier;

(E) the term 'computing device' means a device which incorporates one or more microprocessor based central processing units that can accept, store, process or provide output of data; and

(F) the term 'computer hardware', when used in conjunction with information security, includes, but is not limited to, computer systems, equipment, application-specific assemblies, modules, and integrated circuits.

(b) CONTINUATION OF EXPORT ADMINISTRATION ACT. For purposes of carrying out the amendment made by subsection (a), the Export Administration Act of 1979 shall be deemed to be in effect.

D

Text of S. 1587 ("Encrypted Communications Privacy Act of 1996")

The following is the complete text of S. 1587, also known as the "Encrypted Communications Privacy Act of 1996", which was introduced by Senator Leahy during the second session of the 104th Congress, in March 1996.

A BILL

To affirm the rights of Americans to use and sell encryption products, to establish privacy standards for voluntary escrowed encryption systems, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Encrypted Communications Privacy Act of 1996".

SECTION 2. PURPOSE.

It is the purpose of this Act:

(1) to ensure that Americans are able to have the maximum possible choice in encryption methods to protect the security, confidentiality, and privacy of their lawful wire or electronic communications; and

(2) to establish privacy standards for key holders who are voluntarily entrusted with the means to decrypt such communications, and procedures by which investigative or law

enforcement officers may obtain assistance in decrypting such communications.

SECTION 3. FINDINGS.

The Congress finds that:

(1) the digitization of information and the explosion in the growth of computing and electronic networking offers tremendous potential benefits to the way Americans live, work, and are entertained, but also raises new threats to the privacy of American citizens and the competitiveness of American businesses;

(2) a secure, private, and trusted national and global information infrastructure is essential to promote economic growth, protect citizens' privacy, and meet the needs of American citizens and businesses.

(3) the rights of Americans to the privacy and security of their communications and in conducting their personal and business affairs should be preserved and protected;

(4) the authority and ability of investigative and law enforcement officers to access and decipher, in a timely manner and as provided by law, wire and electronic communications necessary to provide for public safety and national security should also be preserved;

(5) individuals will not entrust their sensitive personal, medical, financial, and other information to computers and computer networks unless the security and privacy of that information is assured;

(6) business will not entrust their proprietary and sensitive corporate information, including information about products, processes, customers, finances, and employees, to computers and computer networks unless the security and privacy of that information is assured;

(7) encryption technology can enhance the privacy, security, confidentiality, integrity, and authenticity of wire and electronic communications and stored electronic information;

(8) encryption techniques, technology, programs, and products are widely available worldwide;

(9) Americans should be free lawfully to use whatever particular encryption techniques, technologies, programs, or products developed in the marketplace they desire in order to interact electronically worldwide in a secure, private, and confidential manner;

(10) American companies should be free to compete and to sell encryption technology, programs, and products;

(11) there is a need to develop a national encryption policy that advances the development of the national and global information infrastructure, and preserves Americans' right to privacy and the Nation's public safety and national security;

(12) there is a need to clarify the legal rights and responsibilities of key holders who are voluntarily entrusted with the means to decrypt wire or electronic communications;

(13) the Congress and the American people have recognized the need to balance the right to privacy and the protection of the public safety and national security;

(14) the Congress has permitted lawful electronic surveillance by investigative or law enforcement officers only upon compliance with stringent statutory standards and procedures; and

(15) there is a need to clarify the standards and procedures by which investigative or law enforcement officers obtain assistance from key holders who are voluntarily entrusted with the means to decrypt wire or electronic communications, including such communications in electronic storage.

SECTION 4. FREEDOM TO USE ENCRYPTION.

(a) LAWFUL USE OF ENCRYPTION. It shall be lawful for any person within any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States, and by United States persons in a foreign country to use any encryption, regardless of encryption algorithm selected, encryption key length chosen, or implementation technique or medium used except as provided in this Act and the amendments made by this Act or in any other law.

(b) GENERAL CONSTRUCTION. Nothing in this Act or the amendments made by this Act shall be construed to:

(1) require the use by any person of any form of encryption;

(2) limit or affect the ability of any person to use encryption without a key escrow function; or

(3) limit or affect the ability of any person who chooses to use encryption with a key escrow function not to use a key holder.

SECTION 5. ENCRYPTED WIRE AND ELECTRONIC COMMUNICATIONS.

(a) IN GENERAL. Part I of title 18, United States Code, is amended by inserting after chapter 121 the following new chapter:

CHAPTER 122: ENCRYPTED WIRE AND ELECTRONIC COMMUNICATIONS

§2801. Definitions

As used in this chapter:

(1) the terms 'person', 'State', 'wire communication', 'electronic communication', 'investigative or law enforcement officer', 'judge of competent jurisdiction', and 'electronic storage' have the same meanings given such terms in section 2510 of this title;

(2) the term 'encryption' means the scrambling of wire or electronic communications using mathematical formulas or algorithms in order to preserve the confidentiality, integrity or authenticity and prevent unauthorized recipients from accessing or altering such communications;

(3) the term 'key holder' means a person located within the United States (which may, but is not required to, be a Federal agency) who is voluntarily entrusted by another independent person with the means to decrypt that person's wire or electronic communications for the purpose of subsequent decryption of such communications;

(4) the term 'decryption key' means the variable information used in a mathematical formula, code, or algorithm, or any component thereof, used to decrypt wire or electronic communications that have been encrypted; and

(5) the term 'decryption assistance' means providing access, to the extent possible, to the plain text of encrypted wire or electronic communications.

§2802. Prohibited acts by key holders

(a) UNAUTHORIZED RELEASE OF KEY. Except as provided in subsection (b), any key holder who releases a decryption key or provides decryption assistance shall be subject to the criminal penalties provided in subsection (e) and to civil liability as provided in subsection (f).

(b) AUTHORIZED RELEASE OF KEY. A key holder shall only release a decryption key in its possession or control or provide decryption assistance:

(1) with the lawful consent of the person whose key is being held or managed by the key holder;

(2) as may be necessarily incident to the holding or management of the key by the key holder; or

(3) to investigative or law enforcement officers authorized by law to intercept wire or electronic communications under chapter 119, to obtain access to stored wire and electronic communications and transactional records under chapter 121, or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801), upon compliance with subsection (c) of this section.

(c) REQUIREMENTS FOR RELEASE OF DECRYPTION KEY TO INVESTIGATIVE OR LAW ENFORCEMENT OFFICER.

(1) CONTENTS OF WIRE AND ELECTRONIC COMMUNICATIONS. A key holder is authorized to release a decryption key or provide decryption assistance to an investigative or law enforcement officer authorized by law to conduct electronic surveillance under chapter 119, only if:

(A) the key holder is given:

(i) a court order signed by a judge of competent jurisdiction directing such release or assistance; or

(ii) a certification in writing by a person specified in section 2518(7) or the Attorney General stating that:

(I) no warrant or court order is required by law;

(II) all requirements under section 2518(7) have been met; and

(III) the specified release or assistance is required;

(B) the order or certification under paragraph (A):

(i) specifies the decryption key or decryption assistance which is being sought; and

(ii) identifies the termination date of the period for which release or assistance has been authorized; and

(C) in compliance with an order or certification under subparagraph (A), the key holder shall provide only such key release or decryption assistance as is necessary for access to communications covered by subparagraph (B).

(2) STORED WIRE AND ELECTRONIC COMMUNICATIONS.

(A) A key holder is authorized to release a decryption key or provide decryption assistance to an investigative or law enforcement officer authorized by law to obtain access to stored wire and electronic communications and transactional records under chapter 121, only if the key holder is directed to give such assistance pursuant to the same lawful process (court warrant, order, subpoena, or certification) used to obtain access to the stored wire and electronic communications and transactional records.

(B) The notification required under section 2703(b) shall, in the event that encrypted wire or electronic communications were obtained from electronic storage, include notice of the fact that a key to such communications was or was not released or decryption assistance was or was not provided by a key holder.

(C) In compliance with the lawful process under subparagraph (A), the key holder shall provide only such key release or decryption assistance as is necessary for access to the communications covered by such lawful

process.

(3) USE OF KEY.

(A) An investigative or law enforcement officer to whom a key has been released under this subsection may use the key only in the manner and for the purpose and duration that is expressly provided for in the court order or other provision of law authorizing such release and use, not to exceed the duration of the electronic surveillance for which the key was released.

(B) On or before completion of the authorized release period, the investigative or law enforcement officer to whom a key has been released shall destroy and not retain the released key.

(C) The inventory required to be served pursuant to section 2518(8)(d) on persons named in the order or the application under section 2518(7)(b), and such other parties to intercepted communications as the judge may determine, in the interest of justice, shall, in the event that encrypted wire or electronic communications were intercepted, include notice of the fact that during the period of the order or extensions thereof a key to, or decryption assistance for, any encrypted wire or electronic communications of the person or party intercepted was or was not provided by a key holder.

(4) NONDISCLOSURE OF RELEASE. No key holder, officer, employee, or agent thereof shall disclose the key release or provision of decryption assistance pursuant to subsection (b), except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate.

(d) RECORDS OR OTHER INFORMATION HELD BY KEY HOLDERS. A key holder, shall not disclose a record or other information (not including the key) pertaining to any person whose key is being held or managed by the key holder, except:

(1) with the lawful consent of the person whose key is being held or managed by the key holder; or

(2) to an investigative or law enforcement officer pursuant to a subpoena authorized under Federal or State law, court order, or lawful process.

An investigative or law enforcement officer receiving a record or information under paragraph (2) is not required to provide notice to the person to whom the record or information pertains. Any disclosure in violation of this subsection shall render the person committing the violation liable for the civil damages provided for in subsection (f).

(e) CRIMINAL PENALTIES. The punishment for an offense under subsection (a) of this section is:

(1) if the offense is committed for a tortious, malicious, or illegal purpose, or

for purposes of direct or indirect commercial advantage or private commercial gain:

(A) a fine under this title or imprisonment for not more than 1 year, or both, in the case of a first offense under this subparagraph; or

(B) a fine under this title or imprisonment for not more than 2 years, or both, for any second or subsequent offense; and

(2) in any other case where the offense is committed recklessly or intentionally, a fine of not more than $5,000 or imprisonment for not more than 6 months, or both.

(f) CIVIL DAMAGES.

(1) IN GENERAL. Any person aggrieved by any act of a person in violation of subsections (a) or (d) may in a civil action recover from such person appropriate relief.

(2) RELIEF. In an action under this subsection, appropriate relief includes:

(A) such preliminary and other equitable or declaratory relief as may be appropriate;

(B) damages under paragraph (3) and punitive damages in appropriate cases; and

(C) a reasonable attorney's fee and other litigation costs reasonably incurred.

(3) COMPUTATION OF DAMAGES. The court may assess as damages whichever is the greater of:

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

(B) statutory damages in the amount of $5,000.

(4) LIMITATION. A civil action under this subsection shall not be commenced later than 2 years after the date upon which the plaintiff first knew or should have known of the violation.

(g) DEFENSE. It shall be a complete defense against any civil or criminal action brought under this chapter that the defendant acted in good faith reliance upon a court warrant or order, grand jury or trial subpoena, or statutory authorization.

§2803. Reporting requirements

(a) IN GENERAL. In reporting to the Administrative Office of the United States Courts as required under section 2519(2) of this title, the Attorney General, an Assistant Attorney General specially designated by the Attorney General, the

principal prosecuting attorney of a State, or the principal prosecuting attorney of any political sub division of a State, shall report on the number of orders and extensions served on key holders to obtain access to decryption keys or decryption assistance.

(b) REQUIREMENTS. The Director of the Administrative Office of the United States Courts shall include as part of the report transmitted to the Congress under section 2519(3) of this title, the number of orders and extensions served on key holders to obtain access to decryption keys or decryption assistance and the offenses for which the orders were obtained.

§2804. Unlawful use of encryption to obstruct justice

Whoever willfully endeavors by means of encryption to obstruct, impede, or prevent the communication of information in furtherance to a felony which may be prosecuted in a court of the United States, to an investigative or law enforcement officer shall:

(1) in the case of a first conviction, be sentenced to imprisonment for not more than 5 years, fined under this title, or both; or

(2) in the case of a second or subsequent conviction, be sentenced to imprisonment for not more than 10 years, fined under this title, or both.

§2805. Freedom to sell encryption products

(a) IN GENERAL. It shall be lawful for any person within any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States, to sell in interstate commerce any encryption, regardless of encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.

(b) CONTROL OF EXPORTS BY SECRETARY OF COMMERCE.

(1) GENERAL RULE. Notwithstanding any other law, subject to paragraphs (2), (3), and (4), the Secretary of Commerce shall have exclusive authority to control exports of all computer hardware, software, and technology for information security (including encryption), except computer hardware, software, and technology that is specifically designed or modified for military use, including command, control, and intelligence applications.

(2) ITEMS NOT REQUIRING LICENSES. No validated license may be required, except pursuant to the Trading With The Enemy Act or the International Emergency Economic Powers Act (but only to the extent that the authority of such Act is not exercised to extend controls imposed under this Act), for the export or reexport of:

(A) any software, including software with encryption capabilities, that is:

(i) generally available, as is, and designed for installation by the

purchaser; or

(ii) in the public domain or publicly available because it is generally accessible to the interested public in any form; or

(B) any computing device solely because it incorporates or employs in any form software (including software with encryption capabilities) exempted from any requirement for a validated license under subparagraph (A).

(3) SOFTWARE WITH ENCRYPTION CAPABILITIES. The Secretary of Commerce shall authorize the export or reexport of software with encryption capabilities for nonmilitary end-uses in any country to which exports of software of similar capability are permitted for use by financial institutions not controlled in fact by United States persons, unless there is substantial evidence that such software will be:

(A) diverted to a military end-use or an end-use supporting international terrorism;

(B) modified for military or terrorist end-use; or

(C) reexported without requisite United States authorization.

(4) HARDWARE WITH ENCRYPTION CAPABILITIES. The Secretary shall authorize the export or reexport of computer hardware with encryption capabilities if the Secretary determines that a product offering comparable security is commercially available from a foreign supplier without effective restrictions outside the United States.

(5) DEFINITIONS. As used in this subsection:

(A) the term 'generally available' means, in the case of software (including software with encryption capabilities), software that is widely offered for sale, license, or transfer including, but not limited to, over-the-counter retail sales, mail order transactions, phone order transactions, electronic distribution, or sale on approval;

(B) the term 'as is' means, in the case of software (including software with encryption capabilities), a software program that is not designed, developed, or tailored by the software company for specific purchasers, except that such purchasers may supply certain installation parameters needed by the software program to function properly with the purchaser's system and may customize the software program by choosing among options contained in the software program;

(C) the term 'is designed for installation by the purchaser' means, in the case of software (including software with encryption capabilities):

(i) the software company intends for the purchaser (including any licensee or transferee), who may not be the actual program user, to install the software program on a computing device and has supplied the necessary instructions to do so, except that the company may also

provide telephone help-line services for software installation, electronic transmission, or basic operations; and

(ii) that the software program is designed for installation by the purchaser without further substantial support by the supplier;

(D) the term 'computing device' means a device which incorporates one or more microprocessor-based central processing units that can accept, store, process, or provide output of data; and

(E) the term 'computer hardware', when used in conjunction with information security, includes, but is not limited to, computer systems, equipment, application-specific assemblies, modules, and integrated circuits.

(b) TECHNICAL AMENDMENT. The table of chapters for part I of title 18, United States Code, is amended by inserting after the item relating to chapter 33, the following new item:

122. Encrypted wire and electronic communications .... 2801.

SECTION 6. INTELLIGENCE ACTIVITIES.

(a) CONSTRUCTION. Nothing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity.

(b) CERTAIN CONDUCT. Nothing in this Act or the amendments made by this Act shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General, or activities intended to:

(1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;

(2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978; or

(3) access an electronic communication system used exclusively by a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978.

E

Text of S. 1726 ("Promotion of Commerce On-Line in the Digital Era Act of 1996")

The following is the complete text of S. 1587, also known as the "Promotion of Commerce Online in the Digital Era Act of 1996" (or the “Pro-CODE Act of 1996”), which was introduced by Senator Burns during the second session of the 104th Congress, in May 1996.

A BILL

To promote electronic commerce by facilitating the use of strong encryption, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1996"

SECTION 2. FINDINGS; PURPOSE.

(a) FINDINGS. The Congress finds the following:

(1) The ability to digitize information makes carrying out tremendous amounts of commerce and personal communication electronically possible.

(2) Miniaturization, distributed computing, and reduced transmission costs make communication via electronic networks a reality.

(3) The explosive growth in the Internet and other computer networks reflects the potential growth of electronic commerce and personal communication.

(4) The Internet and the global information infrastructure have the potential to revolutionize the way individuals and businesses conduct business.

(5) The full potential of the Internet for the conduct of business cannot be realized as long as it is an insecure medium in which confidential business information and sensitive personal information remain at risk of unauthorized viewing, alteration, and use.

(6) Encryption of information enables businesses and individuals to protect themselves against the unauthorized viewing, alteration, and use of information by employing widely understood and readily available science and technology to ensure the confidentiality, authenticity, and integrity of information.

(7) In order to promote economic growth and meet the needs of businesses and individuals in the United States, a variety of encryption products and programs should be available to promote good, flexible, and commercially acceptable encryption capabilities.

(8) United States computer, computer software and hardware, communications, and electronics business are leading the world technology revolution, as those businesses have developed and are prepared to offer immediately to computer users worldwide a variety of communications and computers hardware and computer software that provide good, robust, and easy-to-use encryption.

(9) United States businesses seek to market the products described in paragraph (8) in competition with scores of foreign businesses in many countries that offer similar, and frequently stronger, encryption products and programs.

(10) United States businesses have been discouraged from further developing and marketing products with encryption capabilities because of regulatory efforts by the Secretary of Commerce, acting through the National Institute Of Standards and Technology and other entities of the Department of Commerce, to promulgate standards and guidelines in support of government-designed solutions to encryption problems that:

(A) were not developed in the private sector; and

(B) have not received widespread commercial support.

(11) Because of outdated Federal controls, United States businesses have been prohibited from exporting goods encryption products and programs.

(12) The Secretary of Commerce, acting through the National Institute of Standards and Technology has attempted to leverage the desire of United States businesses to sell commercial products to the United States Government, and sell a single product worldwide, to force the businesses to include features in

products sold by the businesses in the United States and in foreign countries that will allow the Federal Government easy access to the plain text of all electronic information and communications.

(13) Specifically, the Secretary of Commerce, acting through the National Institute of Standards and Technology, has proposed that United states businesses be allowed to sell products and programs offering good encryption to the United States Government, and in foreign countries only if the products and programs include a feature guaranteeing the Federal Government access to a key that decrypts information (hereafter in this section referred to as "key escrow encryption").

(14) The key escrow encryption approach to regulating encryption is reflected in the approval in 1994 by the National Institute of Standards and Technology of a Federal information processing standard for a standard known as the "clipper chip", that was flawed and controversial.

(15) The Federal Government:

(A) has designed key escrow encryption to solve a perceived problem; and

(B) has ignored the fact that:

(i) there is no demonstrated commercial demand for features which give governments easy access to information; and

(ii) numerous non-key escrow encryption alternatives are available commercially from foreign suppliers and free of charge from the Internet.

(16) In order to promote electronic commerce in the twenty-first century to realize the full potential of the Internet and other computer networks:

(A) United States businesses should be encouraged to develop and market products and programs offering encryption capabilities; and

(B) the Federal Government should be prohibited from promulgating regulations and adopting policies that discourage the use and sale of encryption.

(b) PURPOSE. The purpose of this Act is to promote electronic commerce through the use of strong encryption by:

(1) recognizing that businesses in the United States that offer computer hardware and computer software made in the United States that incorporate encryption technology are ready and immediately able, with respect to electronic information that will be essential to conducting business in the twenty-first century to provide products that are designed to:

(A) protect the confidentiality of that information: and

(B) ensure the authenticity and integrity of that information;

(2) restricting the Department of Commerce with respect to the promulgation or enforcement of regulations, or the application of policies, that impose government-designed encryption standards; and

(3) promoting the ability of United States businesses to sell to computer users worldwide computer software and computer hardware that provide the strong encryption demanded by such users by:

(A) restricting Federal or State regulation of the sale of such products and programs in interstate commerce;

(B) prohibiting mandatory key escrow encryption systems; and

(C) establishing conditions for the sale of encryption products and programs in foreign commerce.

SECTION 3. DEFINITIONS.

For purposes of this Act, the following definitions shall apply:

(1) AS IS. The term "as is" means, in the case of computer software (including computer software with encryption capabilities), a computer software program that is not designed, developed, or tailored by a producer of computer software for specific users or purchasers, except that such terms may include computer software that:

(A) is produced for users or purchasers that supply certain installation parameters needed by the computer software program to function properly with the computer systems of the user or purchaser; or

(B) is customized by the user or purchaser by selecting from among options contained in the computer software program.

(2) COMPUTING DEVICE. The term "computing device" means a device that incorporates one or more microprocessor-based central processing units that are capable of accepting, storing, processing, or providing output of data.

(3) COMPUTER HARDWARE. The term "computer hardware" includes computer systems, equipment, application-specific assemblies, modules, and integrated circuits.

(4) DECRYPTION. The term "decryption" means the unscrambling of wire or electronic communications or information using mathematical formulas, codes, or algorithms.

(5) DECRYPTION KEY. The term "decryption key" means the variable information used in a mathematical formula, code, or algorithm, or any component thereof, used to decrypt wire or electronic communications or information that has been encrypted.

(6) DESIGNED FOR INSTALLATION BY THE USER OR PURCHASER. The term "designed for installation by the user or purchaser" means, in the case of

computer software (including computer software with encryption capabilities):

(A) with respect to which the producer of that computer software:

(i) intends for the user or purchaser (including any licensee or transferee), to install the computer software program on a computing device; and

(ii) has supplied the necessary instructions to do so, except that the producer or distributor of the computer software program (or any agent of such producer or distributor) may also provide telephone help-line or on-site services for computer software installation, electronic transmission, or basic operations; and

(B) that is designed for installation by the user or purchaser without further substantial support by the supplier.

(7) ENCRYPTION. The term "encryption" means the scrambling of wire or electronic communications or information using mathematical formulas, codes or algorithms in order to preserve the confidentiality, integrity, or authenticity of such communications or information and prevent unauthorized recipients from accessing or altering such communications or information.

(8) GENERAL LICENSE. The term "general license" means a general authorization that is applicable to a type of export that does not require an exporter of that type of export to, as a condition to exporting:

(A) submit a written application to the Secretary; or

(B) receive prior written authorization by the Secretary.

(9) GENERALLY AVAILABLE. The term "generally available" means in the case of computer software (including software with encryption capabilities), computer software that:

(A) is distributed via the Internet or that is widely offered for sale, license, or transfer (without regard to whether it is offered for consideration), including over-the-counter retail sales, mail order transactions, telephone orders transactions electronic distribution, or sale on approval.

(B) preloaded on computer hardware that is widely available.

(10) INTERNET. The term "Internet" means the international computer network of both Federal and non- Federal interconnected packet-switched data networks.

(11) SECRETARY. The term "Secretary" means the Secretary of Commerce.

(12) STATE. The term "State" means each of the several States of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

SECTION 4. RESTRICTION OF DEPARTMENT OF COMMERCE

ENCRYPTION ACTIVITIES IMPOSING GOVERNMENT ENCRYPTION SYSTEMS.

(a) LIMITATION ON REGULATORY AUTHORITY CONCERNING ENCRYPTION STANDARDS. The Secretary may not (acting through the National Institute of Standards and Technology or otherwise) promulgate, or enforce regulations, or otherwise adopt standards or carry out policies that result in encryption standard for use by businesses or entries other than Federal computer systems.

(b) LIMITATION ON AUTHORITY CONCERNING EXPORT OF COMPUTER HARDWARE AND COMPUTER SOFTWARE WITH ENCRYPTION CAPABILITIES. The Secretary may not promulgate or enforce regulations, or adopt or carry out policies in a manner inconsistent with this Act, that have the effect of imposing government-designed encryption standards on the private sector by restricting the export of computer hardware and computer software with encryption capabilities.

SECTION 5. PROMOTION OF COMMERCIAL ENCRYPTION PRODUCTS.

(a) PROHIBITION ON RESTRICTIONS ON SALE OR DISTRIBUTION IN INTERSTATE COMMERCE.

(1) IN GENERAL. Notwithstanding any other provision of law, neither the Federal Government nor any State may restrict or regulate the sale in interstate commerce, by any person of any product or program with encryption capabilities. Nothing in this paragraph may be construed to preempt any provision of Federal or State law applicable to contraband or regulate substances.

(2) APPLICABILITY. Paragraph (1) shall apply without regard to the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used for a product or program with encryption capabilities.

(b) PROHIBITION ON MANDATORY KEY ESCROW. Neither the Federal Government nor any State may require, as a condition of sale in interstate commerce, that a decryption key be given to any other person (including a Federal agency or an entity in the private sector that may be certified or approved by the Federal Government or State).

(c) CONTROL OF EXPORTING BY SECRETARY.

(1) GENERAL RULE.-Notwithstanding any other provision of law and subject to paragraph (2), (3) and (4), the Secretary shall have exclusive authority to control exports of all computer hardware, computer software, and technology with encryption capabilities, except computer hardware, computer software, and technology that is specifically designed or modified for military use, including command, control, communications, and intelligence applications.

(2) ITEMS THAT DO NOT REQUIRE VALIDATED LICENSES. Only a general license may be required, except as otherwise provided under the Trading With The Enemy Act (50 U.S.C. App.1 et seq.) or the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (but only to the extent that the authority of the International Emergency Economic Power Act is not exercised to extend controls imposed under the Export Administration Act of 1979), for

the export or reexport of:

(A) any computer software, including computer software with encryption capabilities, that is:

(i) generally available, as is, and designed for installation by the user or purchaser; or

(ii) in the public domain (including on the Internet) or publicly available because it is generally accessible to the interested public in any form; or

(B) any computing device or computer hardware solely because it incorporates or employs in any form computer software (including computer software with encryption capabilities) that is described in subparagraph (A).

(3) COMPUTER SOFTWARE AND COMPUTER HARDWARE WITH ENCRYPTION CAPABILITIES.

(A) IN GENERAL. Except as provided in subparagraph (B), the Secretary shall authorize the export or reexport of computer software and computer hardware with encryption capabilities under a general license for nonmilitary end-users in any foreign country to which those exports of computers software and computer hardware of similar capability are permitted for use by financial institutions that the Secretary determines not to be controlled in fact by United States persons.

(B) EXCEPTION. The Secretary shall prohibit the export or reexport of computer software and computer hardware described in subparagraph (A) to a foreign country if the Secretary determines that there is substantial evidence that such software and computer hardware will be:

(i) diverted to a military end-use or an end-use supporting international terrorism;

(ii) modified for military or terrorist end-use; or

(iii) reexported without the authorization required under Federal law.

(d) STATUTORY CONSTRUCTION. Nothing in this Act may be construed to affect any law in effect on the day before the date of enactment of this Act designed to prevent the distribution of descramblers and any other equipment for illegal interception of cable and satellite television signals.

Notes

1. Philosophical Dimensions of Privacy: An Anthology, p. 272

2. ibid, p. 78

3. ibid, p. 78

4. ibid, p. 82

5. ibid, p. 82

6. ibid, p. 86 (my italics)

7. ibid, pp. 87-90

8. ibid, p. 89

9. ibid, p. 89 (my italics)

10. ibid, p. 90

11. ibid, p. 107

12. ibid, p. 107

13. ibid, p. 107

14. ibid, p. 108

15. ibid, p. 108

16. ibid, p. 109

17. ibid, p. 111

18. ibid, p. 111-112

19. ibid, p. 112

20. ibid, p. 114

21. ibid, p. 114

22. ibid, p. 116

23. ibid, p. 116

24. ibid, p. 117

25. ibid, p. 117

26. ibid, p. 124

27. ibid, p. 162

28. ibid, p. 78

29. ibid, p. 163

30. ibid, p. 163

31. ibid, p. 165

32. ibid, p. 165

33. ibid, p. 170

34. ibid, p. 175

35. ibid, p. 174-175

36. ibid, p. 175

37. ibid, p. 187

38. ibid, p. 334

39. ibid, p. 334

40. ibid, p. 335

41. ibid, p. 335

42. ibid, p. 337

43. ibid, p. 336

44. ibid, p. 338

45. ibid, p. 339

46. ibid, p. 338

47. ibid, p. 272

48. ibid, p. 205

49. All product names are trademarks of their respective companies.

50. PGPFone Owner's Manual, p. 13

51. excerpted from United States Code, Title 18, Chapter 119, Section 2510. The full text of United States Code Title 18, Chapter 119 can be found in Appendix A.

52. my italics

53. my italics

54. The full text of United States Code Title 18, Chapter 121 can be found in Appendix B.

55. The full texts of H.R. 3011 and S. 1587 can be found in Appendices C and D (respectively).

56. The full text of S. 1726 can be found in Appendix E.

57. So in original. The word "or" probably should not appear.

58. So in original. Probably should be "or".

59. So in original. Probably should be "Act of 1978".

60. So in original. Probably should be "Act of 1978".

References

Ernst, Morris L. and Schwartz, Alan U. *Privacy: The Right to be Let Alone.* New York: The Macmillan Company, 1962.

Johnson, Deborah G. and Nissenbaum, Helen (editors). *Computers, Ethics and Social Values*. Englewood Cliffs, New Jersey: Prentice-Hall, 1995.

McClellan, Grant S. (editor). *The Right to Privacy*. New York: The H. W. Wilson Company, 1976.

Schoeman, Ferdinand D. (editor). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press, 1984.

Valliappan, Sambasivam (editor). *Frequently Asked Questions about Today's Cryptography*. World Wide Web: <http://www.rsa.com/rsalabs>, 1995.

Text of United States Code, Title 18, Chapters 119 and 121 obtained from the Legal Information Institute of Cornell University, <http://www.law.cornell.edu/>.

Text of H.R. 3011, S. 1587 and S. 1726 obtained from the Center for Democracy and Technology, <http://www.cdt.org/>.

THIS PAGE
INTENTIONALLY LEFT BLANK