# PRIVACY AND COMPUTER-BASED INFORMATION SYSTEMS

Meredith W. Mendes

***Program on Information Resources Policy***

Harvard University

Center for Information Policy Research

Cambridge, Massachusetts

A publication of the Program on Information Resources Policy.

PRIVACY AND COMPUTER-BASED INFORMATION SYSTEMS
Meredith W. Mendes
January 1985, P-85-1



Meredith Mendes is an associate with the law firm Mintz, Levin, Cohen, Ferris, Glovsky and Popeo, P.C. She received a J.D. from Harvard Law School.



Printing 5 4 3 2 1

February 1985

# PROGRAM ON INFORMATION RESOURCES POLICY

**Harvard University** | **Center for Information Policy Research**

## Contributors

Action for Children's Television
American District Telegraph Co.
American Management Systems, Inc.
American Telephone & Telegraph Co.
Arthur D. Little, Inc.
Auerbach Publishers Inc.
Automated Marketing Systems
BellSouth Corporation
Bell Atlantic
Booz-Allen Hamilton
Canada Post
Codex Corp.
Communications Workers of America
Computer & Communications Industry Assoc.
COMSAT
Continental Cablevision, Inc.
Continental Telecom, Inc.
Coopers & Lybrand
Copley Newspapers
Cowles Media Co.
Dialog Information Services, Inc.
Digital Equipment Corp.
Direction Generale
des Telecommunications (France)
Doubleday, Inc.
Dow Jones & Co., Inc.
Dun & Bradstreet
Economics and Technology, Inc.
EIC/Intelligence Inc.
LM Ericsson (Sweden)
Federal Reserve Bank of Boston
France Telecom (France)
Gannett Co., Inc.
General Motors Corp.
General Telephone & Electronics
GTE Sprint Communications Corp.
Harte-Hanks Communications, Inc.
Hazel Associates
Hitachi Research Institute (Japan)
Honeywell, Inc.
Hughes Communication Services, Inc.
E.F. Hutton and Co., Inc.
IBM Corp.
Information Gatekeepers, Inc.
International Data Corp.
International Resource Development, Inc.
Invoco AB Gunnar Bergvall (Sweden)
Knowledge Industry Publications, Inc.
Kokusai Denshin Denwa Co., Ltd. (Japan)
Lee Enterprises, Inc.
John and Mary R. Markle Foundation
MCI Telecommunications, Inc.
McKinsey & Co., Inc.
Mead Data Central
MITRE Corp.
Motorola, Inc.
National Association of Letter Carriers
National Telephone Cooperative Assoc.
The New York Times Co.
NEC Corp. (Japan)
Nippon Telegraph & Telephone Public
Corp. (Japan)
Northern Telecom Ltd. (Canada)
Northrop Corp.
NYNEX
The Overseas Telecommunications
Commission (Australia)
Pacific Telesis Group
Pitney Bowes, Inc.
Public Agenda Foundation
RCA Corporation
Reader's Digest Association, Inc.
Research Institute of Telecommunications
and Economics (Japan)
Royal Bank of Canada (Canada)
Salomon Brothers
Satellite Business Systems
Scaife Family Charitable Trusts
Seiden & de Cuevas, Inc.
Southern New England Telephone
Southwestern Bell Corp.
Telecom Futures, Inc.
Telecommunications Research
Action Center (TRAC)
Telecom Plus International, Inc.
Times Mirror Co.
Times Publishing Co.
TRW Inc.
United States Government:
Central Intelligence Agency
Department of Commerce:
National Oceanographic and
Atmospheric Administration
National Telecommunications and
Information Administration
Department of State
Office of Communications
Federal Communications Commission
Federal Emergency Management Agency
Internal Revenue Service
National Aeronautics and Space Admin.
National Security Agency
United States Information Agency
United States Postal Rate Commission
United States Postal Service
US West
United Telecommunications, Inc.
The Washington Post Co.
Wolters Samsom Group (Holland)

## ACKNOWLEDGMENTS

Special thanks are due to the following persons who reviewed and commented critically on drafts of this report. These reviewers and the Program's affiliates are not, however, responsible for or necessarily in agreement with the views expressed herein, nor should they be blamed for any errors of fact or interpretation.

Lynn Abraham
David Beier
William Canning
Linda Culhane
Robert Gellman
Douglas Ginsburg
George Jelen
Cameron F. Kerry
Joshua Noah Koenig
Frank W. Lloyd
Herbert E. Marks
A. P. Mendes
Richard Neustadt
Thomas J. Pulver
Joseph Romanow
Jonathan Winer
Alan F. Westin

TABLE OF CONTENTS

## EXECUTIVE SUMMARY


- This paper examines the current legal environment for privacy issues believed by some to be raised by the changing technology of data collection and distribution. It further examines the extent to which these privacy concerns may be warranted.

- Privacy protection in the U.S. legal system has focused on legislative efforts to develop laws for specific functional areas and for specific types of information. That is, banking records are treated separately from medical or educational records. Interception of telephone messages is covered by different statutes than those regulating radio communications. A study by the federal Privacy Protection Study Commission rejected an "omnibus" approach to privacy regulation.

- A number of privacy laws recently enacted emphasize the type of information being collected rather than the service collecting the data. Thus it may be less important today than in the past to determine among the various players -- collectors, providers, transmitters -- who will be liable for information abuses.

- Much of the authority and responsibility for privacy protection rests with the states. Such autonomy allows for flexibility but also creates inconsistency among laws and uncertainties among those affected by such laws. States with relatively lax laws could become "data havens." States with information privacy protection statutes have modeled them after the federal Privacy Act.

- One characteristic of American privacy protection policy has been respect for private enterprise and an attempt to minimize the intrusiveness and burdens of government regulation. Business has often found it advantageous to deal with protection of customer data, for example, in a way that avoids adverse market reactions and minimizes the imposition of government regulation.

- Because of the rapid growth and changes in information technology, a number of laws originally designed to protect information privacy are no longer applicable. Laws such as the Communications Act of 1934 and the Omnibus Crime Control and Safe Streets Act of 1968 do not comfortably reflect an age of electronically stored and transmitted information and hybrid forms of telecommunications. Still, it seems that few criminal prosecutions for privacy abuses have failed for lack of statutory sanctions.

- It may be necessary to determine whether publicly accessible information service operators, such as CompuServe, which operate on a public utility-like basis, will be liable for content. The degree of protection that should be afforded to messages and who should be responsible for providing such protection remain to be determined.

- Much attention in the privacy area has been on the laws designed to punish offenders and presumably deter potential offenders. There has been less attention paid to preventing information abuses through physical security measures. These range from simply blocking physical access to mainframe computers, programs, and data from unauthorized users to the use of passwords, ID numbers, and voiceprints. Security measures may also include communications controls to protect data transmission from interception.

- To date, relatively few computer-related privacy violations and crimes have come to the public's attention. This might indicate that there have not been many; that current levels of security, detection, and enforcement are nominally adequate. However, because reporting and prosecuting violators may entail further loss of information privacy, some instances may not be reported.

# INTRODUCTION

Developments in information technology are widely perceived to play an expanded role in data collection.[1] Increased efficiency and decreased costs of computers and telecommunications have contributed to a growing demand for information and services from institutions and from personal users in their homes. The mechanics of information systems, their interconnection through networks and their expansion into users' homes, and the large amount of personal information being collected and retained in such systems have raised questions about the effects of information technology on individual privacy.[2]

Reactions to the growing computerization of information services, their interconnection, and the expanding use of both one-way and interactive information technology for institutional, business, and personal use range from outrage over the potential for impropriety and privacy invasion,[3] to admonishments that although the potential for such invasions exist, privacy regulations may be "premature."[4]

A study conducted by Louis Harris and Associates, Inc. in 1984 to examine people's perceptions of the impact of technology on personal privacy stated that "[v]ast majorities of the general public and most leadership groups believe it is now possible to assemble master files from many sources. And they believe such files are an invasion of privacy."[5] Moreover, although society recognizes the computer as a "symbol of the new era and the core of much of our high technology," a majority of those polled see the present uses of computers as an "actual threat to personal privacy."[6]

This paper explores the extent to which such privacy concerns may be warranted in light of the types of privacy invasions that may become possible as a result of changes in and the expansion of both information technology, and current and proposed laws regulating the information collected, transmitted, and stored by that technology.

The following designations distinguish the types of privacy violations discussed in this paper: aggregation,[7] unauthorized access, intrusion, misuse, and piracy. Additionally, the personal data contained in any information system may be obtained by or of interest to any of the following groups of users: government executive and regulatory agencies; law enforcement officials, judges, prosecutors, and private party lawyers; private institutions, agencies, and employers; systems operators and commercial marketing organizations; and private party "hackers". Confidential information may also be disclosed by subjects of privacy violations who feel pressured or coerced into revealing such information.

Some of the forms of privacy violations described in this paper and defined in Appendix B may have occurred in the past, and may still occur in manually stored records, while many of the presumed dangers and the potential privacy violations pointed out here may never be realized. However, this paper is intended to raise privacy issues that might occur, and to reflect privacy concerns of users, policymakers, authors of articles or books on the subject, and others. Moreover, the changes in information technology have increased the probability that at least some violations discussed herein will occur.

The objectives of this paper are:

1. To define privacy and personal information in a way that is useful in electronically stored one-way and interactive information technology;

2. To discuss the changes in technology that may increase the potential for privacy violations;

3. To examine existing common law and statutory provisions, measures that have been taken, and measures that are pending in response to potential privacy intrusions;

4. To discuss whether these measures are likely to be responsive to privacy concerns; and

5. To present alternatives to existing and pending legal sanctions.

This analysis is divided into six parts. Section I delimits privacy and what constitutes legally protectable personal information by reviewing common law and constitutional privacy, and the types of personal information legislators and their constituents have singled out as warranting separate legal protection. Section II examines changes in the way information is transmitted via computer information systems and electronic funds transfer (EFT), and how these developments may affect personal privacy. Section III presents a legal framework of privacy statutes and other legislative responses to perceived threats created by information technology. It also addresses certain local privacy regulations and industry attempts at self-regulation. The statutes discussed group into the following categories: current federal legislation and regulation of stored records, federal legislation and regulation of communications services, and current state legislation and

regulation of stored records and communications services. Section IV discusses proposed federal legislation that would address some of the privacy concerns raised in this paper. Section V examines policy decisions reflected by the legal measures taken to address information privacy, and presents options to existing and pending legal sanctions to protect information privacy. Section VI summarizes the issues addressed herein.

Database is used in this paper to mean a system in which a central operator provides text and sometimes graphics on a public dial up access basis to a large number of subscribers or users.

# I

# DEFINING PRIVACY

The concept of privacy seems simple enough, but a study of the legal and philosophical literature on privacy today reveals a surprising lack of consensus on its meaning. Nevertheless, it is important to define privacy, even if this definition exceeds current limits of legal protection, because privacy allows us to achieve other values that our society considers important.[8] Privacy is important in the context of information technology because the degree to which individuals are willing to forego their privacy gives them some control over decisions that affect them, such as whether they qualify for employment, insurance, credit, loans, or government benefits. Defining privacy as a legal value may help raise awareness of its importance, deter reckless invasions, and create predictability in the law. Coming to a consensus on the meaning of privacy may aid in determining which losses are most undesirable, therefore most in need of legal protection.

## A. Constitutional Right to Privacy

The Supreme Court expressly recognized a right to privacy under the United States Constitution in Griswold v. Connecticut.[9] In Katz v. United States[10] the Court developed a subjective "expectation of privacy" test that it has subsequently used to determine whether individual privacy expectations will be protected.[11] Three categories of privacy interests have been found to be within the constitutionally protected right to privacy: the right to make certain kinds of important (i.e., intimate) decisions independent of state interference,[12]

the expectations of freedom from government intrusion into places where one's reliance on privacy is justified,[13] and, most recently, the individual's interest in avoiding disclosure of certain "personal matters" contained in stored records.[14]

Although certain records have been found to be within the procedurally protected expectation of privacy, the boundaries of this right are unclear. For example, the Supreme Court held that bank customers lacked standing to contest government access to their bank records because the bank records were the property of the bank.[15] The Court maintained that "the depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government,"[16] and that the depositor therefore had no justifiable expectation of privacy in his bank records.[17] The Court has not recognized substantive privacy rights for individual records stored in data banks.

The Supreme Court has held that the use of an electronic system that records signals from a private home is not unconstitutional. In 1979, the Court found in Smith v. Maryland[18] that the use of pen registers without a warrant to record telephone numbers dialed from a private household is not an expectation of privacy "that society is prepared to recognize as reasonable."[19]

The scope of the right to privacy protected by the Constitution is unclear, and, it might be asserted, largely a matter of judicial discretion. Moreover, the constitutional right to privacy does not extend to protect invasion perpetrated by private third parties, unless that invasion can be characterized as state action.[20]

Individuals' privacy may also be protected by asserting the Fifth Amendment privilege against self-incrimination when a state or the federal government has attempted or is attempting to conduct an inquiry into a person's records. The Fifth Amendment, applicable to the states through the Fourteenth, confers a privilege to be silent in an inquiry as long as an individual's answers to official questions might be employed either as evidence or as leads to evidence in a future criminal prosecution of that individual.[21] Exercise of such a privilege cannot be punished by the government as a failure to cooperate with a proper inquiry, or used as the basis for adverse treatment, including denial of a public benefit.[22]

This doctrine could be used to support the argument that unauthorized government inquiries into computer records for personal information are the equivalent of forcing individuals to testify against themselves, and as such, violate the Fifth and Fourteenth Amendments. The argument is somewhat undercut by the fact that once an individual has been promised immunity from future prosecutorial use of compelled answers or their "fruit," refusal to answer questions pertaining to a legitimate government interest may be punished criminally and civilly.[23] Thus, the government might promise immunity and still conduct an inquiry, which would then be difficult to link to the denial of a benefit or subsequent privacy violation. The government is, however, limited in the scope of its inquiry, which cannot be of unjustifiable breadth.

B. Common Law Privacy[24]

The common law privacy tort affords minimal protection against potential privacy invasions in the context of modern information

technology. Warren and Brandeis[25] wrote the seminal article on the creation of a legally recognizable right to privacy wherein they defined privacy as the right to be left alone.[26] Although the motivation for their article was a series of then-current technological developments including the telephone, microphone, audio recorder, and camera,[27] the right has not been subsequently expanded to deal with more modern phenomena.

The widely accepted analysis of the privacy rights covered by this tort recognizes four categories: 1) unreasonable intrusion on the seclusion of another, 2) appropriation of another's name or likeness, 3) unreasonable publicity given to another's private life, and 4) publicity that places another in the false light before the public.[28]

The law of intrusion may be violated by "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another, or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable man."[29] In contrast to the other branches of the privacy tort, intrusion requires no publication or other use of the materials obtained for a defendant to be liable.[30] Actionable privacy intrusions have arisen from improper investigations of individual bank accounts,[31] tax returns,[32] and over-zealous police work.[33]

Courts have upheld actions for intrusion of privacy where eavesdropping through a wiretap or concealed microphone was used to intercept private communications.[34] However, in an action where a court ruled the information tapped was not confidential, no actionable privacy intrusion was found.[35] Intrusion is actionable only if the plaintiff can prove that the defendant's conduct was "truly intrusive" and that

the intrusion was designed to elicit information unavailable through normal inquiry or observation.[36] Standards for measuring what is "truly intrusive" or "highly offensive to a reasonable man" may vary considerably and may ultimately be a matter of judicial discretion.[37]

A second branch of the privacy tort was developed to prevent unauthorized uses of people's images in photographs for commercial gain.[38] This branch is probably inapplicable to modern information technology. It could be argued that disclosure of computerized personal information can create a profile of a person perhaps more intrusive than a photograph.[39] But the argument seems misplaced since the crux of this action is the unjust enrichment a defendant gains by his gratuitous use of a plaintiff's identity.[40]

The latter two branches of the privacy tort, unreasonable publicity and false light, require plaintiffs to prove the offending disclosure was published or disseminated to the public at large. Disclosure to one person does not constitute "the public." This allowance means any file containing confidential information about a person could be disclosed without authorization, and not constitute an actionable privacy violation.[41] Thus, without creating a common law action for invasion of privacy, one who obtained a credit grantor's identifying code number could conceivably get detailed information on thousands of individuals by simply telephoning information-gathering agencies.

In addition, false light requires that any publicity be highly offensive to a "reasonable person" before damages will be awarded.[42] This reasonableness raises the same definitional problems as does the definition of an "unreasonable" intrusion.

Each category of the privacy tort is subject to common law privileges. If the defendant can show the exposure of information was in the community's interest, the victim must show the defendant's act was motivated by willful and malicious intent.[43] Consent, which may be used as a form of pressure in return for a benefit or favor, may also curtail the utility of a common law action in the computer context.[44] While a common law action for invasion of privacy could conceivably be developed as a deterrent for information privacy invasions, the current definitions and requirements for an actionable privacy invasion severely limit the privacy tort's usefulness to modern information technology.

C. Privacy Statutes

Congress has passed a patchwork of statutes protecting individuals against privacy invasions by the federal government and, in some areas, against informational privacy intrusions in the private sector. Surprisingly, none of these statutes attempts to define privacy. In 1974, Congress enacted the Privacy Act,[45] a general enactment of self-restraint regulating unauthorized disclosures of individual records by the federal government.[46] Specific federal statutes have been passed preventing unauthorized disclosures of the United States mail[47] and credit information,[48] regulating wiretapping[49] and the seizure of work product materials relating to the news media by government officials,[50] and prohibiting unauthorized interception of broadcast telecommunications.[51] A privacy interest has been recognized against searches or seizures by federal officials where such actions would intrude upon a "known confidential relationship," including clergyman and parishioner, lawyer and client, or doctor and patient.[52] Privacy rights are also recognized in educational records.[53]

Several states have enacted either constitutional provisions or statutes that supplement federal law and limit state governments' uses of personal data.[54] A number have adopted state fair-information practice statutes, modeled on the federal Privacy Act of 1974, that define the procedure for collection, maintenance, correction, reports, and public access to stored personal information.[55] However, many states have not adopted comprehensive privacy statutes, and those enacted are uneven. Some states have passed statutes protecting information privacy in one or perhaps a few areas.[56] While such a policy promotes state autonomy, it also creates disunity, unevenness, and unpredictability in the law, and leaves individuals largely unprotected against private business enterprises and other private sector violations -- except to the extent that such businesses and private parties regulate themselves.

Thus, a grab bag of rights might be compiled under the heading "privacy." But there seems to be no unifying concept to identify why certain types of information are legally protectable. Indeed, there are commentators who believe privacy is just a bag of unrelated goodies.[57] Those who subscribe to this concept argue privacy rhetoric in the law is misleading[58] because privacy is never protected without some other interest also being protected.[59] Hence, the argument follows, the law would be clearer if the real values at stake were identified and the term "privacy" were disregarded altogether.[60]

Moreover, because the law has strong commitments to values that may conflict with individual privacy concerns, no area of individual concern can ever be absolutely protected. Among such values are the public interest in preventing evasions of the law and promoting effective

enforcement,[61] the freedom of expression protected by the First Amendment, the corresponding right of the public to be well informed, and the protection of public health. In addition to these gaps, some privacy invasions may go unreported because reporting them necessitates a further loss of privacy. Litigation costs and delays may also discourage actions for privacy invasions, unless courts award or statutes provide for victims to be awarded attorney fees. Moreover, a definition of privacy based on legally protectable rights recognized in the past may be inadequate to cover privacy violations in the context of modern information technology.

A descriptive definition of privacy constructed from remedies at law, then, will leave gaps and will afford little prescriptive guidance for future law- and policymakers. The constitutional concept of privacy is nebulous and unpredictable. The common law is outdated, has doubtful application to information technology, and is subject to privileges and immunities. Federal statutes are riddled with exceptions and holes because of competing considerations that circumscribe the right. State statutes vary in coverage, and most are modeled after the federal Privacy Act. States without specific privacy statutes rely on legislation passed in specific areas. No statute adequately defines privacy.

D. Types of Privacy Concerns

What seems to be needed is a prescriptive definition of privacy that will provide grounds for consensus yet be flexible enough to encompass and adapt to developments in information technology. At the same time, it must afford some limits so as not to encompass every type of information that may be disseminated about a person.

At least five types of privacy concerns may arise as a result of changes in the methods and amounts of information gathered and stored by information technology: unauthorized access, misuses, piracy, aggregation of data, and continuous or intermittent intrusion into terminal lines.[62] Changes in the methods of collecting and storing data, and how these changes may affect information privacy are discussed in Section III.

E. Alternative Definitions

Given the limitations of constructing a legal definition, several commentators have suggested more expansive definitions for understanding the content of the right to privacy. There is little agreement on the meaning of privacy, although there is consensus on the fact that no definition is appropriate in every context.[63] One definition in the computer context has been suggested by Dr. Alan F. Westin, who has written a number of books about privacy and information technology. Westin wrote in one of his early books,

> Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[64]

Westin's definition has been influential, but certain aspects of it have received criticism.[65] For example, the dictionary[66] defines the word "claim" as an assertion of one's due. But as indicated above, claims to privacy are not absolutely protected because of changes in facts, because of conflicts between individuals' and society's needs, because of changes of circumstances or developments giving rise to new claims, and because some claims may not be asserted.

Moreover, if "claim" means a legal claim, then it implies an interest recognized by courts and legislatures. This definition is too

narrow. If "claim" refers to a "moral" claim, then it assumes a preferred position in society's hierarchy of values and, equally important, by the courts. But, while most Americans esteem their privacy[67] -- perhaps as much as any other value -- it is freedoms of thought and speech that occupy the highest position in our courts.[68] Thus, the assertion of a broad unitary claim of privacy may imply that privacy holds, or should hold, an exalted position over other conflicting values, which is not always true.[69] A definition based on privacy as a "right" is vulnerable to the same criticisms.[70]

Privacy is defined in this paper as a condition, because it carries no legal or normative connotations. The legislative process and the courts are ill-equipped to handle many privacy invasions because they are either too clumsy, too slow in responding to abuse, or because competing considerations outweigh personal privacy protection in the eyes of law- and policymakers. In many situations privacy may be better protected when legal measures are supplemented with, or replaced by, non-legal preventive measures such as physical security precautions or market forces. Thus, the word "condition" is used herein because it implies no legal value judgment.

Another criticism that can be made of Westin's definition is that the word "information" is too broad. We constantly communicate information that is unintended, but that may not result in someone's loss of privacy. It is suggested that privacy should be equated with "personal and confidential information" and that loss of privacy should be recognized only when such personal and confidential information are disclosed without the subject's authorization. Personal and confidential information will be defined as information about oneself

that one would not want disclosed without one's prior consent. This definition allows individuals substantial discretion, and individual viewpoints of what is personal are certain to vary considerably. Since the law will never afford complete protection to all private information,[71] it may be more accurate to recognize the disparity among individual viewpoints rather than to attempt to define personal information according to some external and arbitrarily imposed standard.[72] For the purposes of this analysis, however, it is presumed that certain types of information are private, including information relating to one's own financial transactions; buying habits; entertainment and information sources (books, programs, newspapers, magazines, and movie selections); medical, drugs, and related data; educational and tax records; work papers and intellectual material relating to one's employment; and unpublished written and oral communications.[73] Westin's definition, then, subject to the above changes, will be used to delimit privacy in the context of information technology. This paper will define privacy as:

> A condition in which individuals, groups or institutions can determine for themselves, when, how and to what extent private information about them is communicated to others.

# II

# CURRENT AND PROPOSED DATABASE AND OTHER COMPUTER-BASED SYSTEMS

## A. Historical Background

This section discusses certain information services that are currently available or proposed including personal computers, database transmitted via cable television or telephone systems, and electronic funds transfer.

It is useful to note before discussing these technologies that technological innovations have historically been approached with trepidation, which has later been considered unwarranted or premature. For example, in Warren and Brandeis' article advocating a right to privacy[74] the authors warned that cameras and newspapers:

> [H]ave invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the housetops."[75]

Moreover, futurists and courts have predicted privacy losses and dire consequences of technology that never materialized.[76] Thus, while it may be wise to be aware of the potential ramifications and privacy losses that could result from today's new information technology, it may also be advisable to wait to see which threats, if any, are realized, before calling for legal remedies.[77]

This policy was adopted, for example, in the development of the tort of defamation, where the courts developed a distinction between the degree of protection afforded to public and private figures. It might be argued that this policy of "wait and see" is misplaced because it victimizes innocent individuals and results in a legal system that is

unresponsive to current privacy invasions. It might also be argued that some privacy invasions may be so gross, or their harm so great, that they should be prevented before they are realized. But the counter argument is that trying to prevent even the most egregious privacy invasions with immediate legal preventives would be costly, would be likely to result in overly broad legislation, and would probably be disfavored by those who view such a policy as a hindrance to innovation. And while innovation and change may not always be beneficial, the costs, delays, inexactitude, and political conflicts inherent in the legal system might be minimized by other privacy protections such as industry self-regulation in the form of privacy codes,[78] physical security locks, or encryption codes. Local information systems such as interactive cable may be regulated by franchise agreements or private party contracts.[79] These protections would probably be more responsive to privacy dangers requiring immediate attention than would be statutory measures or litigation.

B. Electronic Databases

Interactive data systems, some of which are called videotex, especially when they are designed for the mass audience, may transmit information via cable television hook-ups, over the air (for at least the "down stream" part of the transmission from the user's console to the head-end computer), over the switched telephone network, or through some combination of these forms.[80] One of the first systems to offer some degree of interactivity, though not a videotex system, was the Warner Amex cable television system marketed under the name of Qube.[81] True videotex systems that have been commercially or test marketed include Cox Cable Communications, INDAX, Times Mirror's Gateway, and

Knight-Ridder's Viewtron.[82] In addition to receiving text and simple graphic information, users can transmit responses and request services using typewriter-like consoles linking televisions, via coaxial cable wire or the telephone network, to a central computer. Among the services that videotex systems offer or are expected to offer are:

- newspaper-like services -- news, financial, sports, and Congressional information;
- financial services -- market reports, routine accounting services, and electronic funds transfer;
- shopping services -- mail order merchandising, a wide variety of ticket and reservation services, and comparative shopping information;
- message services -- word processing and text formatting, and, eventually, electronic mail;
- information storage;
- entertainment services -- schedules of events and games;
- educational services -- instructional material and drills;
- monitoring services -- home security devices to detect smoke, fire, sound, movement; energy load management; and medical oversight;[83]
- program selection (when part of a cable television service) — commercial channels; premium channels (primarily movies that have not been shown on commercial channels; community channels that allow users to participate in community politics, talk shows, and interviews).[84]

Warner Amex introduced its Qube system in Columbus, Ohio. Warner has subsequently received approval for two-way cable operations in Cincinnati, Pittsburgh (a system subsequently sold), Dallas, Houston, St. Louis, suburban Chicago, and Milwaukee.[85] Qube gathers billing and response data on its computer by "polling" each subscriber's terminal every six seconds.[86] The information collected includes whether the set is in use, the channel selected, and the last response button touched.

A separate computer performs billing and administrative services. Data is transferred from the polling computer to the information system via magnetic tape and then matched with user names and addresses in the information system. Itemized bills are kept for nine months;[87] summary data, not containing individual names, is kept indefinitely for programming and marketing purposes.[88] Infomercials offer products for purchase and, for programming, request viewer preferences on products, pilot commercials, and serials. Infomercials are also used in other marketing functions.[89]

Some Qube systems offer subscribers a home security system. This system is comprised of ultrasonic motion detectors, pressure sensors placed under rugs, infrared photoelectric cells, doors and window sensors, and an emergency button that polls the system once every ten seconds.[90] Once an alarm is triggered, information is conveyed manually by an operator to the appropriate authority.[91]

Videotex transmitted via common carrier is currently offered on the broadest scale in Great Britain.[92] American companies are also investing in videotex, however. An estimated $100 million had been invested nationwide by U.S. companies in the development and testing of videotex systems through 1984.[93]

Because computerized databases are capable of storing and retrieving archival records, some futurists have predicted that some information will no longer be stored in books. Instead, much may be stored as electronic data entered digitally into a computer.[94]

Futurists and other prognosticators have also speculated that electronic mail service will eventually by-pass the current mail system.[95] Users may be able to send messages to general or limited

(closed user group [CUG]) audiences. Confidential messages could be limited to CUGs by transmitting messages in codes known only to certain people.[96] Alternatively, computer information systems could be used to conduct business meetings without requiring all of the participants to be physically present or available for a conference call at the same time. According to this scenario, conferences could be conducted by sending prepared messages (in the form of speeches) to the meeting's participants. Recipients could respond if so inclined, and each terminal would log their responses giving a serial number to each.[97] This way a participant could "attend" meetings while conducting other business at the same time. Travel time and expenses would be saved as well.

C. Computer Systems[98]

Computer systems have proliferated in business organizations and in user households. Many business' inventory and internal control procedures, communication systems, and information systems are computer operated. Computers in users' homes could provide services similar to videotex. Americans' household computers[99] are now being used to play games, control activities within the home, perform accounting functions and data analysis,[100] write letters and reports, and store confidential information. Such information may include data concerning personal and business finances, medical treatment and physical conditions, personal diaries, and work-product of substantial intellectual property value.[101] Personal computer users have also created voluntary, noncommercial networks to share common interests and information through data communication. These networks, called "bulletin-boards," send

information outside users' homes and voluntarily open up the owner's data to outside access by network members.[102]

D. Electronic Funds Transfer

A computer network comprised of commercial financial institutions has been created by the growth of electronic funds transfer (EFT). EFT is money transferred in the form of electronic bits[103] via telephone wire, cable, satellite, or magnetic media.[104] Four types of operations are generally grouped under the heading of EFT: automated teller machines (ATM), national bank cards, automated clearing house systems (ACH), and point-of-sale (POS) transfers.

Automatic tellers are located in almost every major city in the United States and in most industrialized nations.[105] Among the services performed by ATMs are cash withdrawal, deposits, transfer of funds, and installment payments to financial institutions.[106] Customers can use their bank cards at any bank branch, and in states with less restrictive banking laws, ATMs have been installed in shopping centers, supermarkets, airports, and workplaces.[107] Arrangements have been made to share ATMs among different financial institutions.[108] Regional and national networks are increasingly permitting cash withdrawals from ATMs at institutions other than the user's own bank.

Another category of EFT technology is the national bank card network. The two largest credit card operations, VISA USA and Interbank Card Association (Master Card), have automated their credit operations and have also issued debit cards.[109] These access cards will authorize automatic payments nationwide without clearing first through the Federal Reserve System.[110]

A third change in the national banking system is the automatic clearing house (ACH). The ACH is a computerized center that receives payment information in electronic form.[111] The information received is sorted automatically, forwarded to the receiving bank, and posted in appropriate accounts.[112] No paper is involved other than the customer's receipt of documentation. The basic services ACH offers are direct payroll deposit, preauthorized payments of a fixed amount (mainly mortgage, insurance, loans), and bill-checking.[113] The latter allows the customer to authorize payment of a bill by signing the bill and returning it. The need for a check is thus eliminated.[114]

Finally, POS transfers allow customers to transfer funds immediately from their accounts into merchant's accounts.[115] POS terminals are located at retail stores and are operated by the debit cards (also known as cash or asset cards) discussed above. These terminals function like ATMs, verifying and guaranteeing checks, and allowing customers to make immediate deposits and withdrawals.[116]

The current trend is toward an electronically linked nationwide financial network. Commercial banks, savings and loans, merchants, the travel and entertainment industries, insurance companies, and the Federal Reserve are becoming interconnected.[117] Networks of banking institutions are also becoming internationalized. The first of these networks, Society for Worldwide Interbank Financial Transactions (SWIFT), is operated and owned by participating banks in Canada, Europe, and the United States.[118]

E. Developments Creating Potential Privacy Issues

The development of these and other computer-based services offer users several potential benefits, including greater choice and access to

information, time and energy savings, greater efficiency, less margin for error, and potentially increased security for stored information.

Certain aspects of electronically stored information and the technology transmitting the information, however, have raised fears of possible new forms of privacy invasions, and have increased the amount of harm that could result from other intrusions. Some observers warn against potential abuses of:

(i) Networks

The interconnection of remote terminals via networks and the sharing of information have increased the potential for privacy invasions.[119] Networks reduce the accountability of any one organization for stored confidential information. Communications facilities are shared among many unrelated users, all of whom have access to information contained in the files of every other organization in the network, unless a particular organization installs security measures on its files. Networks have thus exponentially increased the potential for unauthorized access, misuse, and disclosure of personal information among private and government agencies,[120] commercial information providers, and "hackers."

(ii) Ease of Access

As networking has grown, so has the "user friendliness" of accessing electronically stored data through networks.[121] Most systems use some variant of an identification code/password system to protect their information against privacy invasions. During the past few years, however, personal computers have been used to break these codes by systematically speeding up what would otherwise be a slow hit-or-miss

process.[122] Thus, password codes may no longer be satisfactory security.

(iii) Increased Memory of Microchips

Another aspect of information technology that has increased the potential for privacy violations is the use of microchips. Record keepers were once limited in the amounts of information they could retain and exchange by physical storage space. Even if information were stored, it was necessary to physically locate that information. But now the microchip compresses information so that voluminous data can be retained. Electronically stored files can be retrieved and reviewed more quickly than printed matter, and as the price of data retrieval and systems decreases, more agencies, organizations, and individuals will have access to computer information systems.

Any stored records could be the target of the privacy violations enumerated in Section I — unauthorized access, misuse, interception, and aggregation of data and piracy.[123] However, the developments of networks, the need for easy access to files (user friendliness), the microchip, and price decreases of technological components that have made information storage and retrieval a growth industry have also increased the potential gravity (and perhaps the likelihood) of such privacy violations.

F. Detection of Privacy Abuses

Some observers fear a possible increase in the accessibility of potentially damaging and incriminating information due to unauthorized access. Computer "break ins" may be easier to execute than traditional break ins because they can be perpetrated from a remote terminal, and do not require the physical presence of the violator. Currently, detecting

and prosecuting such violations is difficult because there is generally no tangible evidence of the violations. Complications may also arise because, as discussed in Section III of this paper, few states have statutes directed at information privacy violations and no federal statutes address potential privacy invasions in the private sector.

G. Forms of Privacy Abuses

The interconnection of many computers into networks and the sharing of information among organizations may increase the incidence of voluntary transfers of information without subjects' authorization.[124] And it is possible that increased storage capacity will encourage the tendency to retain outdated and no longer accurate data about individuals.

Networking might create damaging and incriminating "psychographic profiles""[125] by aggregating information that could well be innocuous when segregated. These profiles and projections based on them, says the Attorney General of New York, could be used by credit companies, government officials, landlords, insurance companies, investigators, marketing firms, and others for decision making.[126] In addition, the existence of large pools of stored personal information and the current low risk of detection are likely to have significant appeal to third parties.[127] Unauthorized disclosures of psychographic profiles and projections could seriously harm the personal and professional lives, and emotional and psychological well-being of the subjects of disclosures.

For example, at least two attempts have been made to use the information maintained by Warner Amex on its Qube subscribers for

purposes that might constitute invasions of subscriber privacy. In one of these incidents, Columbus mayor Tom Moody's opponent in an election tried to use some information from Qube's records to damage Moody's reputation and gain an unfair advantage in the campaign.[128] In another incident, a proprietor of a movie theater who was prosecuted for showing X-rated films sought (but did not obtain) a subpoena to acquire the names of Qube subscribers who had watched a particular X-rated film when it aired over the interactive cable television system.

Interactive technology will also create the potential for unauthorized intrusions into subscribers' homes. For instance, a cable operator providing a home security service could use the system to determine whether subscribers are home.[130] This information could be used, in turn, to jeopardize subscriber security if it was used for unauthorized purposes such as facilitating robbery. (Of course, burglars have also been able to use the telephone to ascertain that inhabitants are not at home before breaking in.) Utility companies could also monitor or regulate the energy level of homes.[131]

H. Electronic Protection of Information Privacy

Conversely, technology may help prevent privacy invasions and electronic information crimes. It is possible that as the amount of personal information collected increases, privacy may also increase. Information in machine-readable form reduces access to the human eye.[132] And there may be less opportunity for leakage, mishandling, and human error because fewer individuals may ultimately handle this information.[133] Computer security, like safes for physical goods, can be used to prevent unauthorized access to other computers, thus further reducing access to the human eye.[134]

Even if information crime may be made easier in certain respects by electronic systems, reducing the number of computers and instituting elaborate security measures may not be necessary to reduce the number of unauthorized appropriations of information. According to at least one expert, information thefts have occurred most frequently where no security precautions have been taken. Thus, implementing management policies and procedures that encourage the use of any security measure at all should provide significantly better protection.[135]

# III

# LEGAL FRAMEWORK

This section presents a framework for examining the legal protections intended to safeguard information privacy in the United States, and addresses some of the communications industry's attempts at self-regulation. The laws have been divided into the following categories: those that apply to records maintained by federal agencies and the executive branch, federal communications statutes, state penal statutes and theft laws, and state cable television laws.

This section is not intended to advocate or suggest that legislation is a necessary or even appropriate response to many privacy concerns. Indeed, certain legal enactments such as the Bank Secrecy Act[136] may actually increase the possibility of individuals' privacy violations because the information required under this Act might not otherwise have been retained.

## A. The Privacy Right: Current Federal Legislation and Regulation of Stored Records

In 1973 the Department of Health, Education, and Welfare Secretary's Advisory Committee on Automated Personal Data Systems developed five principles for fair information practices. It recommended that:

> (1) there must be no personal data record-keeping systems whose very existence is secret; (2) there must be a way for an individual to find out what information about him is in a record and how it is used; (3) there must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent; (4) there must be a way for an individual to correct or amend a record of identifiable information about him; and (5) any organization creating, maintaining, using,

> or disseminating records of identifiable personal data must assure the reliability of the data for its intended use and must take reasonable precautions to prevent misuse of the data.[137]

These principles were intended to guide the development of new statutes, regulations, and private sector initiatives so that privacy rights in all uses of personal data might be preserved. Congress has enacted several statutes guaranteeing the protection of privacy in specific areas: the Fair Credit Reporting Act of 1971,[138] protecting credit, insurance, and employment information; the Fair Credit Billing Act,[139] protecting privacy by mandating disclosure of finance charges and credit provisions in consumer transactions; the Freedom of Information Act of 1976 (FIOA),[140] which requires disclosure and publication of agency decision-making procedures and opinions, and affords individuals the right to examine agency records;[141] and the Family Education and Privacy Rights Act,[142] which denies federal funding to educational institutions that deny individuals the right to see their records, or that make unauthorized disclosures.

(i) The Privacy Act of 1974

A year after the Secretary's Advisory Committee report, Congress enacted the Privacy Act of 1974.[143] This Act prohibits, with limited exceptions,[144] federal agencies from disclosing records that identify an individual unless that individual has either requested the disclosure or has consented to it in writing.[145] The Privacy Act provides that individuals on whom records have been maintained by federal agencies may request amendment of these records. Agencies may either make the requested correction or inform individuals that they refuse to amend the record, giving the reason for the refusal and notifying them of the procedure to request a review of the refusal.[146] Individuals must be

informed of the uses to which information will be put on the forms used to collect the information.[147]

The Privacy Act also states that agencies may retain only those records that are "relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order."[148] The Act does not establish criteria to determine what information is relevant and necessary under this provision. Moreover, the "routine use" exemption from the nondisclosure provision of the Act,[149] which allows disclosures for a "purpose which is compatible with the purpose for which the information was collected,"[150] has been used to circumvent other requirements of the Act.[151]

The Office of Management and Budget (OMB) has been charged by Congress with issuing guidelines and with overseeing the administration of the Privacy Act.[152] While guidelines establishing security measures for computer systems have been issued,[153] the OMB has been severely criticized for its failure to implement and enforce the Act.[154] Because the Privacy Act applies only to records maintained by federal agencies, private telecommunications companies are not subject to this Act.[155]

(ii) Privacy Protection Study Commission

The Privacy Act established a Privacy Protection Study Commission (the Commission) comprised of Presidential and Congressional appointees.[156] The Commission was instructed to "make a study of the data banks, automated data processing programs, and information systems of governmental, regional, and private organizations to determine the standards and procedures currently in force, and to make recommendations for the protection of personal information."[157] The Commission issued its report in 1977 recommending that

> Congress provide individuals by statute with an expectation of confidentiality in a record identifiable to him maintained by a private sector record-keeper in its provision of . . . telecommunications services. [emphasis added][158]

The report further recommended that individuals be permitted to challenge the relevance and scope of a summons, and to assert the protections of the Fourth and Fifth Amendment in a defense against compelled production of such records.[159] Despite this recommendation, Congress has not enacted legislation to protect records identifiable to an individual maintained by a private sector record keeper in its provision of telecommunications services.[160]

(iii) Right to Financial Privacy Act

In response to a 1976 Supreme Court decision,[161] Congress took steps to protect the privacy of data contained in financial records. The Right to Financial Privacy Act of 1978 prevents government access to individual financial records except pursuant to authorization by the customer, an administrative subpoena or summons, a search warrant, or in other limited circumstances as required by statute.[162] An individual must receive notice of an investigation of his records and may challenge access through procedures established by the Act.[163]

(iv) EFT Act

Contemporaneous with the Right to Financial Privacy Act of 1978, Congress passed the Electronic Funds Transfer Act.[164] This statute requires financial institutions to maintain their own records; provide customers with accurate detailed records and periodic statements of all account activity;[165] promptly correct all account errors;[166] and notify customers of the terms, conditions, and disclosures respecting their accounts.[167]

Ironically, neither the EFT Act nor regulation E,[168] which was designed to answer customers' questions concerning EFT services,[169] deals with consumer privacy concerns that may be raised by electronic banking. Because banks and financial institutions are required by law[170] to retain copies of almost all financial transactions and because so much information -- credit, liabilities, mortgage payments, purchases, and salary -- could be retrieved from one terminal, the incentive to intercept information may be greater when such information is stored electronically than when less information was retrievable from one place because of limitations on physical storage space.

It has been claimed that EFT will increase the amount of confidential information available to individual and institutional third parties with access to the POS network without customer consent.[171] Others have posited that consumers will have less control over, and knowledge of, their financial transactions because pre-authorized payments will reduce flexibility and float, and there will be no leverage against merchants for unauthorized payments.[172]

But it might be argued that it will be easier to keep track of information and more cost-efficient to establish maximum security guards for POS terminals, since all financial information will be centrally stored in one computer terminal. Thus, financial information may be better protected and easier to control when it is stored in computers than it was when it was manually filed on hard copy. The introduction of third parties with computer terminals (for example, retail stores and supermarkets) to the POS network is unlikely to have added deleterious effect on personal privacy, however, because stores already have access to sensitive financial information, and because, if needed, customers

could have receipts for transactions. All account activity will be recorded on customers' statements.

(v) Privacy Act of 1980

The Privacy Act of 1980 limits government officers or employees from searching for or seizing any work product materials from persons who intend to use them for public communication.[173] The Act describes a "public communication" as a newspaper, book, broadcast, or other similar form of public communication in or affecting interstate or foreign commerce.[174] The legislation's purpose is to protect the dissemination of public information by preventing overly broad searches and unnecessary seizures of such information by the federal government. The Act does not affect information maintained by the private sector.

B. Current Federal Legislation and Regulation of Communications Services

Privacy for communications services is protected by two federal laws: Title III of the Omnibus Crime Control and Safe Streets Act of 1968[175] and Section 605 of the Communications Act.[176]

(i) Common Carrier

Title III imposes criminal sanctions for the interception of wire communications by unauthorized persons. "Wire communications" are defined as transmissions provided by common carrier.[177] Title III also regulates the use of wiretapping by federal law enforcement officials.[178] Because the statute applies only to common carriers, information services that are not hooked up to telephone lines will not be covered by the Act.[179] Moreover, because the statute defines "intercept" as the "aural acquisition of the contents of any wire or oral communication," the Act will not apply to nonvideo data and

transmission services provided by common carrier,[180] nor will it cover nonaural information transmitted over cable wire. Information that does not travel by wire is not covered by Title III.

The word "content" may pose still another barrier to the Omnibus Act's application to electronic telecommunications. Content, as construed by at least one court, is "information concerning the identities of the parties to [the] communication, or the existence, substance, purport or meaning of the communication."[181] Pen registers, which record numbers dialed from a telephone without intercepting verbal communications, have been found by the Supreme Court not to violate this Act because they do not overhear the substance of telephone conversations.[182] Similarly, it might be argued that billing information compiled for various information and communication services does not constitute "content."

(ii) Wire Communications

Section 605 of the Communications Act[183] prohibits unauthorized interception of radio and broadcast signals. The operative provision of the Communications Act states:

> . . . No person not being authorized by the sender shall intercept a radio communication and divulge or publish the existence, contents, substance, purport or effect or meaning of such intercepted communication to any person.[184]

This section has been interpreted in certain court decisions to apply to wire communications not covered by Title III,[185] as well as to traditional radio and broadcast signals. However, Congress amended Section 605 in 1968 to make it clear that Title III is intended for wire communications.[186]

Under this law, legal violations of communications may occur only if such communications are divulged or published. Thus, a party may

intercept information without divulging it or publishing it and incur no legal liability. Divulgence by a party to a conversation, or a telephone operator eavesdropping on a conversation on demand of a lawful authority with a court order have been interpreted by courts not to violate this Act.[187]

It would appear that some accommodation may always be necessary between personal privacy and effective law enforcement. On the other hand, currently enacted federal communications statutes are based on a model developed when communications were restricted to audio transmissions via wire or radio signal, and when most information was stored as hard copy. Neither the Omnibus Act nor the Communications Act addresses privacy issues raised by hybrid forms of communications. Much information is now transmitted in the form of nonaural electronic bits and stored electronically in computer memories. Information that might not constitute "content" under Title III may be damaging when aggregated with other information that might not be considered substantive under this Act. And as indicated, information may be misused without being divulged or published by an unauthorized party intercepting a communication.

(iii) FCC Regulation

The Federal Communications Commission (FCC) has addressed consumer privacy in hybrid technology. In 1974, the FCC spoke to privacy concerns that may be raised by two-way cable television.[188] Interestingly, it did so in a warning to local franchising authorities that they were becoming too protective of the public on the issue of privacy. Fearing that two-way capability would be unduly restricted, the FCC commented that "there has been much misinformed over-reaction to

this problem."[189] The FCC said it would "take any action necessary to assure system integrity[190] and urge "[a]ll governmental jurisdiction . . . [to be] on guard to guarantee that the right of privacy is maintained."[191] The FCC specifically called for a policy requiring that any activation of two-way service be at the subscriber's option.[192]

Nonetheless, after warning the states away, the FCC has never implemented the federal privacy protections it promised in its 1974 Ruling.[193] And as yet, no Congressional act has been passed preventing disclosure or sale of subscriber billing records, or requiring corrections of inaccuracies in such records maintained by private telecommunications companies. Moreover, no federal act has been passed addressing potential privacy issues -- unauthorized access; aggregration, misuse, and interception of data; and intrusions by electronic means into subscriber households[194] -- that may be raised by the collection and flow of so much information into one central storage bank.

C. State Legislation and Regulation of Stored Records and Communications Services[195]

There is a great diversity of information privacy protection among the states. In California, for instance, the right of privacy is considered an inalienable right guaranteed by the state constitution.[196] In New York, courts have upheld a right of privacy based on public policy embodied in a statute[197] and an implied promise of confidentiality.[198] Computer fraud statutes exist in at least ten states as a general safeguard for computer information systems.[199] A number of states have also adopted broad non-disclosure statutes in the form of fair-information practice statutes.[200]

(i) Fair Information Practice Statutes

Fair information practice statutes require information to be collected, to the greatest extent feasible, from subjects directly, in order to promote accuracy and afford maximum notice to individuals when they are the subjects of information searches.[201] Certain state privacy statutes also place an affirmative duty on a regulatory agency or an information board to notify subjects when information is used for any purpose other than that for which it was collected, or when it is transferred to another agency without the subject's authorization.[202]

But as do the federal information privacy acts these statutes are modeled after,[203] many state statutes place an affirmative duty on the individual himself to contest unauthorized uses or transfers of information regarding that individual, or to correct the information's accuracy or completeness. In most cases, however, subjects will not be apprised prior to unauthorized uses of such information. It is unlikely that people will be aware when stored information about them is being used or transferred to another agency unless agencies are affirmatively required to notify them.[204] Moreover, these statutes do not apply to records maintained by private organizations.

(ii) Larceny

Larceny statutes[205] presently in force in many jurisdictions are based on a number of assumptions that are untenable in the context of electronic technology.[206] One assumption is the concept of unjust enrichment -- that a person may gain only at another person's expense. This concept is manifest in both the Model Penal Code[207] and New York Penal Law.[208] New York, like many states, defines larceny in terms that

require the defendant to intend a permanent deprivation before a larceny will be recognized.

Electronically stored information, however, can be reproduced and misappropriated without "depriving" the data owner or the subject of its use. This requirement may preclude the application of larceny statutes to prosecute unauthorized appropriations of electronically stored information. It might be argued that stored information that is disseminated or misappropriated may lose its monetary value, thus depriving the owner of its value. But the value of stored information may vary significantly depending on the person seeking the information, the person about whom the information pertains, and the number and identities of persons with knowledge of the information. Information that is valuable to one person may be valueless to another, and its disclosure might not be recognizable in a court of law. Many states define deprivation in terms that require that property be "withheld" from the owner.[209]

In addition to requiring a deprivation, larceny statutes are based on an assumption that theft requires a physical transportation of property. The term "property" appears to be based on the traditional notion of private property that can be measured by its economic market value. The Model Penal Code and the New York statute define larceny in terms of "taking, obtaining, withholding or exercising unlawful control over property."[210] Again, this assumption, that property cannot be stolen unless it is physically carried away, is incongruous when the item being apportioned is information in the form of electronic bits. A wrongful appropriation of electronically stored information would not require any physical movement. An intruder could violate a data

subject's privacy simply by gaining access to information and reading it, without taking notes or physically transporting any information.

(iii) Unfair Competition

As early as 1918, the Supreme Court recognized the potential for misappropriation of intangible property without depriving the owner of its use in the law of unfair competition. In International News Service (INS) v. Associated Press (AP)[211] INS charged that AP was pirating the fruit of INS's efforts by scanning bulletins and early editions of newspapers serviced by INS and selling the "pirated" news in competition with INS.

The Court refuted AP's argument that the news was uncopyrightable and, once distributed, could be used by anyone for any purpose. The Court said the plaintiff's rights against the public were different from plaintiff's rights against a competitor in business. Further, the Court said the AP's act was itself an admission that it was taking material acquired by INS "as a result of plaintiff's organization, and the expenditure of labor, skill, and money," and that by appropriating and selling such material in competition with plaintiff, the defendant was attempting to "reap where it had not sown."[212]

INS has been interpreted most liberally to stand for the proposition that it is unlawful for a business competitor to "interfere with the normal operation of a competitor's legitimate business organization."[213] The doctrine of the case has been upheld in cases before and since.[214] However, INS has been severely criticized and limited by subsequent case law[215] and by the federal Copyright Act. The federal Copyright Act protects works of authorship that are "fixed in a tangible medium of expression and [that] come within the subject matter

of [federal copyright protection]." All other equivalent state and common law rights are preempted.[216]

Justice Brandeis' dissents in the INS case and subsequent cases have criticized the majority decision because of its "unwarranted" extension of the concept of property to "knowledge, truths ascertained, conceptions and ideas" that become (with a few exceptions that are patentable or copyrightable), "after voluntary communication to others, free as the air to common use."[217] Other courts have refused to accept the INS doctrine because of its anticompetitive implications.[218]

Because the Copyright Act invalidates all state-created "legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright,"[219] state-created unfair competition law is probably preempted by the Copyright Act. The only thing that is clearly not preempted by the Copyright Act is state protection of works not yet "fixed in a tangible medium of expression."[220] This would include performances and broadcasts recorded without the owner's permission.[221]

It is unclear whether electronically stored information falls within the protection of the federal Copyright Act or whether such information would be protected against misappropriation if it were not eligible for copyright protection.[222] Moreover, if stored information is not within the scope of the Copyright Act, an argument could be made that states should not have the right to protect information when nondisclosure conflicts with the federal policy of disclosure and free access.[223]

Where copyright law is not applicable, however, the INS misappropriation doctrine will be limited to situations involving

business competitors. Even a liberal application of the misappropriation doctrine would not cover many privacy violations discussed in this paper that might occur where information is electronically stored.[224]

(iv) Theft of Services

A number of states have modernized their larceny statutes and expanded the definition of property to include electronically stored or processed records.[225] Specific prohibitions against attetmpts to misappropriate telecommunications services, called "theft of services statutes," have also been legislated in many states.[226]

These statutes are intended to prevent the wrongful interception of pay and subscription cable television services. Theft of service statutes do not require physical transportation of an object or property as defined in larceny statutes, so will prevent privacy invasions to the extent that they deter invasions into subscribers' terminals and related equipment.[227] The word "services" probably would not encompass a prohibition against intrusions into electronically stored videotex records or computer software, however.[228] Some theft of services statutes may also contain limiting provisions as does a Massachusetts statute that requires information to be published before an appropriation of information constitutes an actionable theft.[229]

(v) Other Offenses

In states where computer fraud statutes do not exist, prosecutors have attempted to prosecute computer crimes by alleging various offenses involving the habitation.[230] Such offenses -- burglary, for instance -- require a breaking and entry into a home or business establishment. Prosecutors have also found that statutes prohibiting offenses against

property (in addition to larceny) such as embezzlement, false pretenses, extortion, malicious mischief, and receipt of stolen property may apply to computer crimes. Successful prosecution will depend on whether the data, program, or equipment is interpreted to fall within the state's definition of property, or whether a state's statute has been amended to encompass computer crimes.[231]

(vi) Cable Television Statutes

At least seven states have adopted cable television privacy legislation that responds to privacy concerns such as aggregration, misuse, unauthorized access and disclosure of individually identifiable data, and intrusion into subscribers' homes via interactive cable television systems.[232]

Illinois was the first state to pass a cable privacy act. The Communications Consumer Privacy Act became effective on January 1, 1982.[233] The Act prohibits 1) a cable television operator from monitoring a subscriber's set or his selection of viewing fare without the knowledge or permission of the subscriber, 2) the disclosure of subscriber lists without prior notice to the subscriber, 3) the disclosure of viewing habits of any subscriber without his or her consent, and 4) the use of home protection scanning devices without the written consent of the occupant.[234]

Wisconsin's cable privacy act, adopted in April 1982, requires that a subscriber's cable equipment be fitted with a device at no extra charge to prevent both the reception and transmission of all messages upon the subscriber's request.[235] A cable operator may not disclose any individually identifiable information or monitor its subscribers' terminals without written subscriber authorization.[236]

The California cable privacy bill was also enacted in 1982 as part of the State Penal Code. The California act prohibits cable operators from recording, transmitting, observing, monitoring, or listening to events or conversations that occur in a subscriber's work place,[237] and from disclosing any individually identifiable information on its subscribers.[238] The act further limits the retention of subscriber information,[239] prevents operators from making information available to government agencies without legal compulsion, and, on such event, requires prior notice when lawful to the subscriber.[240] Subscribers have the right to obtain information gathered by cable operators,[241] and must be provided with a notice from cable operators explaining their privacy rights under the act.[242]

Both the Minnesota[243] and Connecticut[244] legislatures have adopted statutes that require the agencies responsible for regulating cable communications in these states[245] to adopt and administer cable television regulations that include prohibitions against privacy invasions in two-way cable systems.[246] The Minnesota Cable Communications Board also requires that all state franchise agreements contain a provision prohibiting any signals from being transmitted from a subscriber terminal for the purpose of monitoring individual viewing patterns or practices without a subscriber's express, revokable written consent. No information obtained by monitoring the transmission of a signal from a subscriber terminal including the subscriber's name, address, and viewing habits, may be disclosed to any third party without specific written subscriber authorization.[247]

Regulatory authorities in New York[248] and Rhode Island[249] have also adopted provisions in their cable operating rules that restrict the

transmission of two-way signals.[250] Cable telecommunications privacy legislation is pending in several jurisdictions.[251]

(vii) Computer Fraud Statutes

Numerous states have proposed computer fraud statutes in response to theft and related offenses involving computers.[252] While these statutes do not specifically address the private information stored in computers, virtually all computer fraud statutes make it a crime to access, alter, damage, or destroy any data contained in a computer.[253]

A number of computer fraud statutes distinguish between crimes involving hardware and those involving software, programs, and data.[254] Many statutes also distinguish between access for the purpose of 1) devising or executing any scheme or artifice to defraud, or 2) obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises,[255] and intentional access, alteration, damage, or destruction of either computer hardware or the software, data, and programs.[256]

The penalties for violating computer fraud statutes range from $150[257] to $50,000.[258] It is unclear what fine within this range will be a sufficient deterrent to computer crimes. Moreover, some computer fraud statutes base the recovery of the owner on the "amount of the loss."[259] It may be particularly difficult to determine the amount of the loss to the owner, however, when the major loss is a privacy violation.

D. Municipal Regulation of Cable Subscriber Privacy

Electronically stored information collected and retained by cable television operators may also be regulated locally. Municipal officials may insert provisions in franchise agreements that prohibit unauthorized

access to and monitoring of cable subscribers' terminals and disclosures, misuses, and aggregation of data.[260] Advocates of this type of local control over cable operations maintain it is easier for local authorities to "keep tabs" on community operators than on cable company officials who may be hundreds of miles away "behind corporate walls."[261]

Although many municipal franchise agreements do not place controls on the collection, use, and dissemination of information, subscriber privacy provisions are appearing more frequently in such agreements. Warner Amex's Cincinnati, Ohio franchise agreement contains a section entitled "Rights of Individuals" in which Warner Amex promises to observe, protect, and ensure the privacy of all subscribers; to comply with all applicable laws, rules, and regulations respecting privacy; to keep all subscriber records in strict confidence; and to develop data specific to individual subscribers only as necessary to provide pay-per-view services.[262]

Additionally, the standard franchise agreement in Massachusetts includes a section entitled "Privacy and Rights to Information," which bars the licensee from recording or making available to any person information regarding subscriber viewing habits without subscriber consent. Any instances of recording or monitoring of the cable system must be reported by the licensee. Subscribers must receive written notice if equipment is installed to enable the recording or monitoring of viewing habits. Subscribers must take "some action to activate" transmissions from their homes, and the licensee must inform the issuing authority of the nature of any information obtained and the manner in which it is used. Finally, the subscriber is entitled to examine

records pertaining to him upon written request. The issuing authority is not prohibited from obtaining general demographic, market, and other related data.[263]

E. Cable Industry Self-Regulation

(i) Industry Responses

The cable industry is generally opposed to state cable bills and restrictive franchise agreements.[264] The New York Cable Television Association opposes the New York cable privacy bill, which was introduced in 1983 and reintroduced in 1984,[265] because of its stringent authorization requirements and provisions mandating the destruction of subscriber records. Association officials object to the large fines for violations, maintaining that the cable industry should not be singled out when there are not comparable privacy laws regulating banks, telephone, and computer firms.[266]

The industry further argues that state bills and regulations will saddle cable operators with restrictions similar to those imposed on common carriers.[267] Many analysts also believe that if there is to be legislation, it should be federal law to promote uniform rules and standards for the industry.[268] Other two-way cable promoters argue that privacy regulation is "premature," is "frightening people and giving interactive cable a bad name,"[269] and is "a cure in need of a problem."[270] Finally, industry officials point out it is in their "own best interests to protect their subscribers from privacy violations and to maintain a structure of operations which continually reassures the public regarding safety and the reasonableness of [cable's] products."[271]

(ii) Privacy Codes

Despite protests against externally imposed regulations, cable associations and operators maintain that protecting subscriber privacy is, in fact, in their industry's best interest. Some of the major cable operators have thus introduced subscriber privacy codes.[272] Warner Amex was the first cable operator to introduce such a code (see Appendix A) for its Qube subscribers in 1981.[273] According to Warner Amex, "it is clearly possible to provide subscribers with the important benefits of interactive cable, while at the same time guarding against real or perceived infringements of their subscriber rights."[274]

The Warner code, however, allows for the disclosure of stored subscriber information to the company's own employees.[275] It includes no provisions for damages to injured parties, or penalties to punish employee violations of the Code.[276] Terms such as "adequate safeguards" and "reasonably necessary" do not specifically define the company's responsibilities to protect subscriber information, or limit the company's retention of subscriber data to any specified length of time. The Code does not specify who will enforce its provisions, and whether any subscriber data may be shared with Warner Cable Communication's parent company.[277] Finally, there has been concern that not all operators will adopt these rules or that the rules they do adopt will not provide comprehensive subscriber privacy protection, especially where the rules threaten to diminish income from secondary uses of subscriber data.[278]

# IV

# PROPOSED FEDERAL REGULATIONS

## A. Cable Television Bills

### (i) Content of the Bills

The multitude of state cable laws, local regulations, and rate restrictions in franchise agreements have prompted the cable industry to seek uniform regulations in the form of a federal cable telecommunications bill.

The Cable Communications Policy Act was passed by Congress in 1984 as Title VI of the Communications Act of 1934.[279] The law was passed despite battles and lessening support in the cable industry [280] following court decisions in Miami and Nevada in 1984 limiting local regulators' control over cable,[281] and the Supreme Court's decision in the Capital Cities[282] case. In Capital Cities, the Court said that the FCC has absolute power to regulate and preempt state and local jurisdiction over cable television.[283] It appears that those who withdrew support from the bill feared that the FCC's preemption of cable television jurisdiction would loosen city regulators' hold on franchise fees, rates regulation, and program content.[284]

The Protection of Subscriber Privacy section of the cable bill [285] prohibits cable service providers from collecting personally identifiable information without the prior written or electronic consent of the subscriber, requires destruction of subscriber information collected, prevents disclosure of information except with subscriber consent or a court order, and requires notice to subscribers before disclosure of their records. Subscribers must be notified of their

rights prior to entering into any agreement for cable services, and must be given access to their records.

The cable law also prohibits the interception or receipt, or assistance in the interception or receipt of cable service without the specific authorization of a cable operator or as may specifically be required by law.[286]

The passage of a federal cable telecommunications act containing subscriber privacy provisions preempts the existing inconsistencies in state and local cable subscriber privacy laws and regulations; provides uniform practices and procedures for cable operators; and should help end the struggle among the FCC, cities, the cable industry, and the cable industry's competitors for jurisdiction over two-way cable services.

B. Proposed Federal Computer Bills

The Cable Franchise Policy and Communications Act does not apply to electronic databases operated over telephone lines, nor does it apply to potential privacy invasions of privately owned computer databases. Legislators have proposed federal legislation such as the Federal Computer Systems Protection Act (FCSPA) to prevent computer crime.[287]

Federal prosecutions of computer software crimes may be based on the federal Copyright Act, patent law, trademark and service mark protection, federal statutes prohibiting fraud perpetrated through interstate communication wires, or the federal mail fraud statutes. But the Copyright Act only applies to original works of authorship, and does not extend to "ideas, procedures, processes, systems, methods of operation, concepts, principles or discovery."[288] Inventions and discoveries of processes are protected by patents, but patentable works

must be useful and novel,[289] and there are expenses and delays in securing a patent. Trademarks and service marks are applicable to proprietary designations, and the federal fraud statutes will apply only where a person has devised or intends to devise a fraudulent scheme or artiface for obtaining money or property.[290] As indicated above, computer software and electronic files have not traditionally been considered property.

# V

# POLICY DECISIONS AND OPTIONS

The legal sanctions that may become available for prosecuting crimes involving computers, telecommunications services, and electronically stored records are only touched upon in this paper. Some statutes such as the Cable Franchise Policy and Communications Act of 1984[291] and state cable privacy acts are responsive to privacy invasions that may be posed by interactive cable. Other statutes such as the Omnibus Crime Control Act[292] and the Communication Act of 1934[293] are based on the notion that communications media can be plugged into categories that, in reality, may be inapplicable to hybrid and new forms of technology.[294] Additionally, some statutes contain provisions such as the publication requirement in the Communications Act of 1934,[295] the aural content requirement in the Omnibus Act,[296] and the services requirement in theft of services statute, that limit their applicability to electronically stored data. Some states have passed theft of services statutes, some have passed computer fraud statutes, and still others have amended the definition of property in their larceny statutes to apply to services and electronic data. The purpose of this section is to examine the policy decisions reflected in the legal sanctions affecting information privacy in the United States and to present options to protect, and perhaps improve, information privacy for present and future law- and policymakers.

## A. Policy Decisions[297]

### (i) Emphasis on Specific Areas

The legal framework of privacy protections in the United States indicates that lawmakers have made a policy decision to focus legis-

lative efforts on developing proposals for specific areas and specific types of information. Banking information is treated separately from information contained in medical or educational records, and interceptions of telephone messages are covered by a different statute than that which regulates radio communications. In its study on record keeping, the Privacy Protection Study Commission rejected an "omnibus approach" that would apply to any private or public agency, organization, or individual.[298]

Specific legislation is responsive to specific abuses. But in the long run, as evidenced by existing privacy statutes, specificity may lack flexibility. Information technology is evolving so rapidly that attempts to mold legal privacy protections to match fleeting developments are inefficient. Such attempts at exactitude create a blueprint for avoidance.[299] In addition, this practice of focusing on specific areas engenders a disparity in the amount of information privacy afforded to different industries in the United States.

The lack of a uniform national standard of informational privacy protection may also have detrimental effects on international data transmissions, since many countries have stricter privacy laws. Other countries may be wary of transmitting confidential information to the United States if it will be less protected here.[300] On the other hand, uniform standards may be too broad and all-inclusive in some areas, but not strict enough to protect confidential information in other areas. Privacy protection may be more effective when it is responsive to particular privacy intrusions. This type of regulation can only be done on an ad hoc basis.

(ii) Federalism

One way to develop a more uniform set of information privacy protections would be to compromise the notion of federalism reflected in the current patchwork of statutes applicable to information privacy. Federalism is a policy of governing that elevates the value of state sovereignty above federal power.[301]

State autonomy creates flexibility but it also creates inconsistency among privacy protection laws and uncertainties among those affected by such laws. People may have difficulty learning and keeping abreast of the law in their particular state. Moreover, state autonomy may instigate struggles over the power to regulate a particular industry.[302] This policy could also lead to the development of "data havens" -- areas which attract companies with unscrupulous information storage practices -- because privacy laws are more lax in these states than in others.[303] But inconsistency may be less problematic than failure to adopt any protections at all, since it appears that those states with information privacy protection statutes have modeled them after the federal Privacy Act.[304] Moreover, all of these risks should be examined in light of the countervailing prospect of a federal government without adequate checks.

(iii) Balance of Interests

Another policy decision illustrated by the aforementioned framework of information privacy protections is that differing rights should be weighed and balanced against competing interests.[305] This reflects the American notion of the democratic political process, in which various constituencies with differing interests compete to make themselves heard. Such a characterization of American politics may be accurate

some of the time. But interest groups with the most monetary resources and/or the most effective connections may dominate the political process, or those with fewer resources or who are ignorant of political issues may not make themselves heard. Thus, privacy protection legislation is not necessarily responsive to the needs of those constituencies whose interests are not represented in the political system. However, this is a criticism of the legislative process rather than of privacy law or any other specific area of law. It would seem to be inherent in the democratic system that no legislation, whether or not it becomes law, will ever be totally responsive to every political constituency.

(iv) Respect for Private Enterprise

American privacy protection policy has traditionally respected private enterprise and attempted to minimize the intrusiveness and burdens of government regulation. This respect is based on the assumption that business and industry will find it in their self-interest to deal with matters such as privacy invasions in a constructive way in order to avoid adverse market reaction or the imposition of government regulation.[306] Industry self-regulation may be preferable to external government regulation because industries are likely to be more familiar with their own operations and the most frequent and dangerous information abuses than external regulatory bodies would be. Industry self-regulation could lead to less stringent controls than external regulations, but it could arguably lead to regulations that will be enforced if the organizations handling personal data deem it their best interest to maintain their integrity and to avoid external regulation.

B. Policy Options

Because of the rapid growth and changes in information technology, a number of the laws originally passed to protect information privacy no longer appear applicable. But laws such as the Communications Act[307] and the Omnibus Act[308] could be amended to apply to electronically stored and transmitted information and to hybrid forms of telecommunications. The passage of the Cable Franchise Policy and Communications Act in 1984 and a federal computer anti-fraud statute containing user privacy provisions would together replace the multiplicity of state and local regulations in these areas, and would establish a more uniform national policy. Such uniformity would stimulate predictability and confidence in our legal system, both domestically and abroad.

Legislation that defines certain conduct as criminal and that provides for legal sanctions cannot be effective without the means to enforce it, however. The problems of detecting electronic information abuses, enforcing existing federal and state statutes, and establishing local and industry self-regulation in the private sector have been discussed. But according to at least one source, few criminal prosecutions have failed for lack of statutory sanctions.[309] Moreover, many information violations are not being reported.[310] It would appear that resources could be productively spent to increase prevention, detection, and reporting of electronic information violations.

(i) Physical Security Measures

One method of preventing electronic information crimes is to increase and enforce the use of security measures. Installing security measures may be as simple as blocking off physical access by

unauthorized users to the mainframe computer, programs, data, and output, and requiring the use of passwords. Voiceprints to identify users have been used by planners for Prestel, the leading videotex system in Britain.[311] Voiceprinting registers the authorized operator's voice on a microphone, and thereafter the system functions only if it registers that operator's voice.[312] This measure would probably reduce the number of intruders into videotex and computer systems. Restricting the circulation of operations manuals or programs that control user access could also help prevent access to computer systems by unauthorized users.

Security measures may also take the form of communications controls designed to protect data transmissions by preventing or detecting interception. Encryption, or security coding, has also been used to deter break ins and interceptions of computer communications. The codes may be created by computer equipment or scramblers currently on the market.[313]

Black markets for descramblers of encryption codes could develop, as they have for other types of computer systems.[314] But encryption codes are extremely expensive both to create and to crack, and it is unlikely that resources would be expended on routine data transmissions. Messages extremely confidential or vulnerable to break ins such as foreign intelligence or financial transactions could be protected with more complicated codes,[315] or might be transmitted using other means.

Hardware controls may also be used to help control unauthorized access. Hardware controls are mechanical controls built into a system to lessen the opportunity for improper use of the computer. Examples of such controls include machine-maintained logs of individual user

numbers, time records, and restrictions on acceptable programming languages.[316]

Increased prevention, detection, and reporting of electronic information crimes may ultimately depend on the willingness of three potential groups -- operators, manufacturers, and outside auditors[317] -- to accept these responsibilities voluntarily, or on a Congressional decision to impose such responsibilities.

(ii) Operators[318]

The implementation and maintenance of security measures could siginficantly reduce the incidence of videotex and other computer crimes.[319] According to at least one study, however, most operators either fail to initiate security procedures,[320] or they delegate such jobs to analysts and programmers who may not have training in auditing and security techniques, but who are likely to be knowledgeable about systems and best able to perpetrate fraud.[321] Users may be reluctant to report incidents of computer crime because of fear of liability to shareholders for negligence, because of a desire to avoid negative publicity, and a wish to maintain public confidence.[322]

It might be possible to require licensing of individual computer systems to ensure compliance with minimum security requirements. However, standard procedures applicable to all computers would be difficult to develop,[323] and minimum security might be inadequate for certain systems. Mandatory reporting procedures might be easier to develop, but both licensing and reporting would require government regulation.[324] Such mandatory regulation would, in all likelihood, be vehemently opposed by the industry.

Increasing public awareness of potential privacy invasions and electronic data crimes may be an alternative to mandatory security procedures for operators. Publicizing computer crimes could increase public demand for security measures.[325] Another approach to increasing prevention by users would be to create economic incentives such as government grants or tax breaks for organizational users who voluntarily implement security measures.

(iii) Manufacturers

Manufacturers currently provide only those security measures for which users pay. Computer system developers are not liable for failure to provide security features unless such developers contractually agree to provisions imposing such liability.[326]

The same problems that apply to government regulation of users would appear to apply to regulation of manufacturers. It might be argued that imposition of statutory liability on manufacturers would deter organizations from remaining or becoming computer manufacturers. The result might be less progress in the computer field, or alternatively, a diversion of resources from innovations in programming, technology, and services to advancements in security technology. The latter may be desirable. Additionally, investment in security technology may be more cost justified than equal investment in attempting to enforce computer crime laws.[327]

Imposing statutory liability on computer and database system developers or operators would be complicated by additional practical difficulties of tort law such as determining whether buyers or subsequent users have tampered with an original design, and whether and how far manufacturers' liability should extend beyond the first user.[328]

(iv) Accountants

Accountants could also help detect and report privacy invasions and other computer crimes in their quarterly and year-end audits of business organizations.[329] Accountants are currently required to review clients' "internal control" systems to certify their clients' financial statements.[330] Such review specifically includes an examination of computer accounting control procedures,[331] testing the client's compliance with previously implemented procedures,[332] and evaluating the adequacy of particular computer systems' security procedures.[333]

The accountant's examination does not affect the outcome of the audit, however, and is not designed to detect computer crimes.[334] Rather, assessing the quality of a client's internal controls is intended to help the accountant determine the extent of testing that should be performed to certify that client's financial statements. Thus, the American Institute of Certified Public Accountants (AICPA) does not require auditors to state a conclusion or to determine the adequacy of a client's computer system and its vulnerability to potential computer crimes. The accountant's liability if fraud surfaces is determined by the degree of care exercised in conducting the audit.[335] And except in extraordinary circumstances, the accountant can avoid liability by showing conformity with Generally Accepted Auditing Principles promulgated by the AICPA (GAAP).[336]

Because accountants must review their clients' computer data processing systems, a statutory requirement that auditors report uncovered computer crime would relieve them of the decision whether or not disclosure is necessary, and would increase the incidence of reported computer crimes.[337]

The imposition of increased liability on auditors would be likely to cause practical difficulties, however. The AICPA has traditionally been the body that sets standards for auditors, and the AICPA is not likely to be enthusiastic about increasing the liability of its members.[338] Except where there is voluntarily compliance by the accounting profession, the government has generally declined to mandate auditing standards.[339] The Securities and Exchange Commission (SEC) has in some instances required accountants to comply with different standards for reports filed with the SEC than the standards required by the AICPA or the Financial Accounting Standards Board for certification of financial statements.[340] But the SEC's regulations apply to only relatively large corporations that file with the SEC.

## VI

## SUMMARY

This paper has attempted to delimit within the sprawling concept of privacy a smaller zone of information privacy that may call for different protections than in the past because of changes in the way information is handled, transmitted, and stored. Electronics can increase efficiency and could increase access to stored personal data. Computers have also created the potential for the aggregation of hitherto harmless information that could constitute a privacy invasion when combined with other information. Many of policy- and lawmakers' assumptions about the distinctness of various media and the legal categorizations that regulate these media may be inapplicable to regulate interactive technology. Many of the assumptions that form the foundation for the criminal law also seem outdated when applied to misappropriations and misuses of information.

Still, other assumptions about individuals' rights to retain their privacy and autonomy with respect to personal or sensitive information remain the basis of both general and specific privacy protection laws. Federal and state privacy acts have been passed establishing fair information procedures to notify individuals when they are the subject of information searches by the government, and of the procedures to obtain redress for privacy intrusions. Federal and state laws also prohibit collection and dissemination of certain types of information in the private sector without individuals' knowledge in industries where the collection of information by legislators and their constituents have been deemed most intrusive.

These laws do not protect individuals against the kinds of privacy abuses that may occur as a result of electronic information storage, however. Additionally, most forms of the federal communications laws are based on an outmoded notion of the separability of distinct types of communications facilities, which limits the laws' applicability to hybrid technology, and they contain certain other provisions that limit their applicability to electronically stored information.

However, recently enacted legislation such as the Cable Communications Act does not contain these restrictions and is drafted to apply to electronic information. Several states have also recognized the limited applicability of prior common law notions and federal statutes to electronic information crimes. This has resulted in amended larceny statutes in some jurisdictions, theft of service statutes, protection of pay television statutes, cable television privacy laws, and computer fraud statutes.

The passage of federal laws directed at the kinds of abuses that may be created by electronically stored information would create greater uniformity and predictability in the law. Struggles among members of the communications industry and local, state, and federal officials for jurisdiction to regulate the communications industry might also dissipate.

Nonetheless, legislative sanctions against electronic information crimes are not enforceable without preventive measures and increased detection and reporting of violations. It remains to be decided who, if any, of the various players in the communications and computer business (information collectors, providers and transmitters, computer system developers and operators) will or should be responsible for enforcement

of security measures, and for reporting and detecting privacy and information abuses. Such distinctions may be less meaningful now than in the past because many of the functions and services previously performed by distinct entities such as newspapers, radios, television, electronic information retrieval, shopping, banking, and message transmission may be combined by a single information provider. It may also be necessary to determine how much and what form of security should be afforded or mandated for computer information systems.

Until now, privacy safeguards in the communications and computer industry have been largely voluntary, presumably based on the assumption that industry self-regulation will be prompted by fear of adverse market reaction or excessive government regulation. Such an assumption might be valid in light of the examples provided by the cable, broadcast, and motion picture industries. Much of the media now seems to be subject to codes of conduct that depend on voluntary self-enforcement. Privacy codes could be extremely effective if the present political power of professional and industry associations used their power to enforce privacy codes. The pressures of conformity from within an industry may be as cogent as legal restraints, and may provide more flexibility.

On the other hand, members of the communications and computer industry may not adopt voluntary regulations. It is possible that no segment or organization connected with these industries -- operators, manufacturers, or independent auditors -- will be willing to accept responsibility for enforcing security measures and for detecting and reporting information abuses without external compulsion or economic incentives. And historically Congress has been unwilling to impose such measures or to single out any one segment of the industry because of

practical enforcement difficulties, and because of a policy preference for industry self-regulation.

Relatively few computer privacy violations and crimes have come to the public's attention.[341] This might indicate that widespread privacy invasions have not resulted from the growing use of computers and electronic telecommunications. However, because of the further loss of information privacy inherent in reporting violations, it is difficult to know whether the absence of public reports supports such a conclusion. Because there is no way to substantiate this conclusion, the best policy may be to come to a consensus on what we mean by information privacy, to sensitize ourselves to the ways in which electronic information storage and developments in interactive technology may affect our privacy, and to wait and see whether such invasions of information privacy are real or imagined.

ENDNOTES

1. A. Westin, "Information Abuse and Personal Computers," Popular Computing, August 1982, at 113 to 114 [hereafter cited as Westin, Popular Computing]. Westin writes that 2 million personal computers are functioning in users' homes today, 5 million are expected to be purchased in 1985, and forecasts for 1990 range from lows of 8 to 10 million to highs of 15 to 25 million. Id., at 114. Additionally, some form of computer-based technology is employed by virtually every major American and international business, private, and government institution. Computers have in fact become so fundamental to our society that some colleges and graduate schools require students to enroll in at least one basic computer programming course. Major business schools may either require students to purchase personal computers prior to enrollment or charge for them in the cost of tuition.

2. A. Westin, "New Eyes on Privacy," Computerworld, November 28, 1983, at 1 [hereafter cited as Westin, Computerworld], Westin, Popular Computing, Supra, Westin, "Home Information Systems: The Privacy Debate," Datamation, July 1982, at 100 [hereafter cited as Westin, Datamation], D. Nash & J. Smith, Interactive Home Media and Privacy, January 1981 (Report for the Office of Policy, Planning, Federal Trade Commission). See also United States Information Society (1977) [hereafter cited as P.P.S.C., Info. Society]; United States Privacy Protection Study Commission, Technology And Privacy (1977) [hereafter cited as P.P.S.C., Technology], A. Miller, The Assault on Privacy, Computers, Databanks and Dossiers (University of Michigan Press: Ann Arbor, 1971).

3. For instance, New York Attorney General Robert Abrams has testified at state assembly committee hearings that interactive cable television operators will collect "large banks of confidential, personal information about cable subscribers" that could be used to create "detailed psychographic profiles." These profiles could be used by credit companies, landlords, insurance companies, government investigators, marketing firms, and others to harass subscribers and invade their privacy. A. Breznick, "NY Attorney General Favors Cable Bill", Multichannel News, March 26, 1984, at 33. For two futurists' predictions, see J. Wicklein, Electronic Nightmare (The Viking Press: New York, 1981) and J. Martin, Telematic Society: A Challenge For Tomorrow (Prentice-Hall, Inc.: Englewood Cliffs, 1981). Wicklein says that although the new communications systems will create many benefits, they "will also put us in danger of losing our individual liberty." Martin, who is in general a strong proponent of telecommunications, warns, "[e]lectronics could make our lives as visible to officials as that of a goldfish in a bowl." Martin, note 2, at 199. The Privacy Protection Study Commission concluded that largely as a result of technology, reports have "never been able to affect an individual as easily, as broadly and potentially unfairly as they can today." P.P.S.C., Info. Society, note 2, at 60.

4. D. Nash & D. Bollier, Protecting Privacy in the Age of Hometech, 8 Tech. Rev. 67, at n.86 (1981) [hereafter cited as Nash & Bollier].

Advocates of interactive cable television argue that privacy regulation is "premature," is "frightening people and giving interactive cable a bad name," and is "a cure in need of a problem." Remarks of New York Attorney General Robert Abrams to State Commission on Cable Television cited in Westin, Datamation, supra note 2, at 111. See also Breznick, supra note 3, at 33. Cable industry officials also point out it is in their "own best interests to protect their subscribers from privacy violations and to maintain a structure of operations which continually reassures the public regarding safety and the reasonableness of [cable's] products." J. Koenig, "Protecting Consumer Privacy" in Cable TV Renewals & Refranchising 113 (1983). See generally R. Neustadt, G. Skall, & M. Hammer, The Regulation of Electronic Publishing IV-3 (Report, 1981).

5. Louis Harris Associates, Inc., The Road After 1984: The Impact of Technology on Society, Presented by Southern New England Telephone (1984), at 7 [hereafter cited as Road After 1984].

6. Id., at 13.

7. For this and subsequent terms, see Appendix B, Definitions.

8. R. Gavison, Privacy and the Limits of the Law, 89 Yale L. J. 421, 423 (1980). Among these values are liberty, autonomy, and intimacy. See S. Bok, Secrets on the Ethics of Concealment and Revelation (Random House: New York, 1983). Bok has written that control over secrecy (which the author says is overlapping with privacy because the purpose of both privacy and secrecy is to become "less vulnerable, more in control." Id., at 11) is important to protect four values: identity, plans, action, and property. These values relate to "protection of what we are, what we intend, what we do and what we own." Id., at 20. Charles Fried argues privacy is necessary for the development of trust, love, and friendship. Human relations, he suggests, are determined by personal information shared by a partner but with no one else. C. Fried, Privacy, 77 Yale L.J. 475, at 484-485 (1970).

9. 381 U.S. 479 (1969) (right to privacy includes right of a married couple to use contraceptives). The Supreme Court found privacy to be within the "penumbra" of rights expressly granted by the Constitution. Although seven Justices concurred in the opinion, the members of the Court disagreed on the theory used to reach its opinion. Justice Douglas said the right to privacy is implicit in the Bill of Rights, protected by the First, Third, Fourth, Fifth, and Ninth Amendments. Justices Goldberg, Warren, and Brennan said the right to privacy is one of the additional fundamental rights protected by the Ninth Amendment. Id., at 486. Justices Harlan and White relied on the Due Process Clause of the Fourteenth Amendment. Id., at 499.

10. 389 U.S. 347 (1967) (FBI agents listened to respondent's conversations from a telephone booth with electronic eavesdropping device).

11. Katz v. United States, 389 U.S. 347, 352-53. Justice Harlan, in his concurrence, stated the two-pronged test to determine whether an individual has a right to privacy. The test requires a person to have exhibited an actual expectation of privacy, and that the expectation be one society is prepared to recognize as reasonable. Id., at 361. The Katz rule has been applied in civil as well as criminal cases. Miller, 425 U.S. 435, 442-44 (1976) (bank depositor has no legitimate expectation of privacy in bank records). For criticism of the Katz rule, see, e.g., A.G. Amsterdam, Perspectives on the Fourth Amendment, 56 Minn. L. Rev. 349 (1974).

12. See Roe v. Wade, 410 U.S. 223, 152 (1973) (right to privacy includes the right of a woman to determine whether or not to have an abortion); Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) (an individual has a right to privacy from government intrusion in deciding whether or not to have a child).

13. See Katz v. United States, 389 U.S. 347 (1967).

14. See Whalen v. Roe, 429 U.S. 589, 599-600 (1977). (Individuals had justifiable expectation of privacy in state records containing names and addresses of persons who have obtained a doctor's prescription for certain harmful drugs. State's retention of records did not violate individuals' right to privacy, however, because adequate safeguards were taken to protect the information.) But see Schulman v. New York City Health and Hospital Corporation, 38 N.Y.2d 234, 342 N.E.2d 501, 506 (1975) (court refused to uphold a constitutional challenge to the New York City Health Code requirement that names and addresses of patients obtaining abortions be recorded); Belmont v. State Personnel Board, 36 Cal. App. 3d 518, 522-25, 111 Cal. Rptr. 607 (1974) (two psychiatric social workers employed by the State Department of Social Welfare were suspended from employment for willful disobedience of Department order calling on them to furnish confidential information on patients).

15. See United States v. Miller, 425 U.S. 435, 440 (1976). But see The Right to Financial Privacy Act of 1978 §1101-1122, 12 U.S.C. 3401-3422 (amended 1980 and 1982). This Act gives customers standing to challenge unauthorized government access to their bank records.

16. United States v. Miller, 425 U.S. 435, 446 (1976).

17. But see Charnes v. Digiacomo, 200 Colo. 94, 612 P.2d 1117 (Colo., 1980). (Respondent was served with an administrative subpoena for alleged tax evasion. The court said the Colorado constitution protects the depositor from government intrusions into bank records in the absence of judicial supervision.)

18. 442 U.S. 735 (1979).

19. 442 U.S. 735, 745 (1979).

20. See Civil Rights Cases, 109 U.S. 3 (1883) (parts of this case have been overruled and expanded, but the majority's holding that

Congressional power does not reach private conduct under the Fourteenth Amendment still stands). G. Gunther, Constitutional Law, 984, 10th ed., (The Foundation Press, Inc.: Mineola, N.Y., 1980).

21. Mallory v. Hogan, 378 U.S. 1 (1964); Murphy v. Waterfront Commission of New York, 378 U.S. 52 (1964). See L. Tribe, American Constitution Law (The Foundation Press: Mineola, 1978), 1979 Supplement.

22. See, e.g., Lefkowitz v. Turley, 414 U.S. 70 (1973) (state statute requiring public contracts to provide that existing contracts may be cancelled and contractor disqualified for five years from future transactions with state if contractor refuses to testify concerning contracts or waive immunity is unconstitutional); Spevack v. Klein, 385 U.S. 511 (1967) (failure to produce financial records and refusal to testify by attorney in disbarment proceeding cannot be used as evidence of misconduct).

23. See Gardener v. Broderick 392 U.S. 273, 278 (1968) (dictum): A public employee may be compelled to answer questions "specifically directly, and narrowly relating to the performance of his official duties," if his answers or the fruits thereof cannot be used in a subsequent criminal prosectuion. Tribe, supra note 21, at 710. The government may have broader discretion to inquire into the duties of public servants than into the affairs of those employed inside in the private sector, however.

24. For a discussion of the development of common law privacy in England, see D. Seipp, English Judicial Recognition of a Right to Privacy, Program on Information Resources Policy, Harvard University, May 1982, at 13-24, 34-44.

25. See S. Warren & L. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

26. Cooley, Torts 29 (2d ed. 1888) cited in Warren & Brandeis, Id., at 195.

27. Nash & Smith, supra note 3. See W. Prosser, Privacy, 48 Cal. L. Rev. 383 (1980). But see E.J. Bloustein, Privacy As An Aspect of Human Dignity: An Answer to Dean Prosser, 39 N.Y.U.L. Rev. 962, 1001-07 (1964).

28. Restatement (Second) of Torts §652P.

29. W. Prosser, The Law of Torts, §117 (4th ed., West Publishing Company: St. Paul, 1971).

30. Id.

31. Zimmerman v. Wilson 81 F.2d 847, 849 (3d Cir. 1936); Brex v. Smith, 104 N.J. Eq. 386, 391-92, 146 A. 34, 36 (1929) (defendant liable for intrusion where, seeking evidence for use in civil action against

plaintiff, he obtained access to plaintiff's personal bank account by using a forged court order).

32. See Frey v. Dixon, 141 N.J. Eq. 481, 485 58 A.2d 86, 88 (1948).

33. See Monroe v. Darr, 221 Kan. 281, 559 P.2d 322 (1977) (cause of action existed for nonconsensual entry by sheriff's deputies into plaintiff's apartment because entry was unsupported by probable cause or a valid search warrant).

34. See Fowler v. Southern Bell Tel & Tel Co., 343 F.2d 150, 156 (5th Cir. 1965) (wiretap by I.R.S. agents was sufficient to constitute tort of privacy invasion without proof of publication); Hamberger v. Eastman, 106 N.H. 107, 112, 206 A.2d 239, 242 (1964) (landlord's installation of recording and listening device in plaintiff's bedroom constituted privacy intrusion beyond the limits of decency).

35. Nader v. General Motors, 255 N.E. 2d 765, 25 N.Y. 2d 560, 565 (1970). (Nader alleged G.M. was harrassing him by 1) interviewing acquaintances, 2) keeping him under surveillance in public places, 3) causing him to be accosted by women for illicit relations, 4) making threatening phone calls to him, 5) tapping his telephone, 6) conducting investigations of him. Court said interviewing acquaintances did not violate privacy right since information confided to acquaintances could no longer be regarded as private. Neither harassing phone calls nor solicitations by hired women constituted privacy invasions since neither involved intrusion for the purpose of gathering information of a private and confidential nature). Id., at 569.

36. Id., at 567.

37. See, e.g., Id. See also Hamberger v. Eastman, 106 N.H. 107, 206 A.2d 239, 242 (1964) (court sympathized with plaintiff and awarded damages for emotional pain and suffering resulting from wiretap of plaintiff's bedroom activity); Sidis v. F.R. Publishing Corporation, 113 F.2d 806 (1940). (New York Magazine wrote a profile of math prodigy who went into seclusion. The court said the article was a "ruthless exposure" Id., at 807. But Sidis did not recover any damages because the court said Sidis had been a public figure and his activities were a legitimate subject of public interest).

38. See Pavesich v. New England Life Insurance Company, 120 Ga. 190, 50 S.E. 68 (1905) (unauthorized use of plaintiff's likeness for life insurance advertisement); Roberson v. Rochester Folding Box Company, 171 N.Y. 538, 64 N.E. 442 (1902) (unauthorized use of plaintiff's likeness to sell flour). For a discussion of English cases based on this branch of privacy law see Seipp, supra note 24, at n.157.

39. See Miller, supra note 2, at 174.

40. See R. Wacks, The Protection of Privacy, 165 (Sweet & Maxwell: London, 1980) [hereafter cited as Wacks].

41. See Miller, supra note 2, at 177.

42. See Wacks, supra note 40, at 170. See also Prosser, supra note 29, at §112.

43. Miller, supra note 2, at 180.

44. Id. It may be possible to argue that such pressure constitutes coercion or compelled self-incrimination.

45. 5 U.S.C. §552a (1976).

46. 5 U.S.C. §552a(b) states:

> No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior consent of, the individual to whom the records pertains, unless disclosure of the record would . . . [the Act then lists 10 exceptions to this provision].

Individuals on whom records have been maintained may have access to those records and may request amendment of those records, 5 U.S.C. §552a(d). Only those records "relevant and necessary to accomplish a purpose or required by statute or by executive order may be maintained." 5 U.S.S. §552a(e)(1). Individuals must also be informed of the uses to which such information will be put on the forms used to collect such information. 5 U.S.C. §552a(e)(3).

47. 18 U.S.C. §§1701, 1702 (1909).

48. Fair Credit Reporting Act, 15 U.S.C. §1681 (1970); Equal Credit Opportunity Act, 15 U.S.C. §1691 (1978).

49. Omnibus Crime Control and Safe Streets Act, Title III, 18 U.S.C. §2510 to 2520 (1968).

50. Privacy Protection Act of 1980, Pub. L. No. 96-440, 94 Stat 1879, 42 U.S.C. §§2000aa-2000aa-12.

51. Communications Act of 1934 c. 652, Title VI, §605, 47 U.S.C. §605 (amended 1968 and 1982).

52. Privacy Protection Act of 1980, Pub. L. No. 96-440, 94 Stat. 1879, 42 U.S.C. §2000aa-11(3).

53. Family Educational Rights and Privacy Act of 1974, P.L. 98-380, 88 Stat. 484 §513, 20 U.S.C. §1232q (1974). Federal funds are denied under this statute to any eligible agency or educational institution that denies its students or their parents the right to inspect and challenge the accuracy and completeness of educational records maintained on its students. 20 U.S.C. §1232g(a). Funds are also denied to any agency or educational institution that permits release of educational records (or personally identifiable records contained therein). 20 U.S.C. §1232g(b).

54. See, e.g., Ariz. Rev. Stat. Ann. §16-802 (1977). The Arizona Information Practices statute provides for the establishment of an Information Practices Board to implement the legislative intent set out in §16-802. The aforementioned section lays out fair information procedures for, inter alia, providing subjects with notice when information about them is used, maintaining security, updating inaccuracies, purging irrelevancies, and preventing other misuses of personal information. Data subjects' rights are defined in §16-806. Other information practice statutes, for example, the Utah statute, Utah Code Ann. §60-50-1 (1975), provide that fair information practices shall be established and maintained by the Secretary of State. See also National Telecommunications and Information Administration, Privacy Protection Law in the United States, N.T.I.A. Report Series, Report 82-78, May 1982, at App. I5 [hereafter cited as Privacy Protection Law]. For further information see generally R. Smith, "Selected 1983 Federal Privacy and Security Legislation; Compilation of State and Federal Privacy Laws," Privacy Journal, Washington, D.C. (1981).

55. See, e.g., Ind. Cod Ann. §4-1-6-1 (West 1979); Mass. Gen. Laws Ann. ch. 66A §§1-3 (West 1976); Va. Code Ann. §§2.1-377 (1976).

56. See, e.g., Nev. Rev. Stat. §629.061 (1977); Va. Code §2.1-342 (1979).

57. See Wacks, supra note 40, at 10-23; see also R. Posner, Privacy, Secrecy and Reputation, 28 Buffalo L. Rev. 1 (1979); R. Posner, The Right to Privacy, 12 Ga. L. Rev. 393 (1978); J. Thomson, The Right to Privacy, 4 Phil & Pub. Aff. 295 (1975).

58. Gavison, supra note 8, at 424.

59. Wacks separates at least eight other categories that have become "entangled" with privacy: 1) privacy and autonomy, 2) privacy and other liberties including freedom from unreasonable search, freedom of association, freedom of expression, 3) privacy and confidentiality, 4) privacy and secrecy, 5) privacy and defamation, 6) privacy and property, 7) privacy and computers, 8) privacy and privilege. Wacks, supra note 40, at 10-22.

60. Wacks argues:

> "Privacy" has become as nebulous a concept as "happiness" or "security". Except as a general abstraction of an underlying value, it should not be used as a means to describe a legal right or cause of action. Id., at 21.

61. See W. Renquist, Privacy and Effective Law Enforcement, 23 Kansas L. Rev. 1 (1974).

62. See Appendix B for explanations of these terms. See also Nash & Smith, supra note 2, at 6-9. See generally "Information Management, Locking The Electronic File Cabinet," Business Week, October 18, 1982, at 123.

63. See R. Parker, A Definition of Privacy, 27 Rutgers L. Rev. 275, 277-78 (1974).

64. A. Westin, Privacy and Freedom (Atheneum: New York, 1967). Westin has subsequently written several articles and books on information technology and privacy. See articles cited in notes 1 and 2 supra. See also: A. Westin & M. Baker, Databanks in a Free Society, Computers, Record-Keeping and Privacy (Quadrangle Books: New York, 1972) [hereafter referred to as Databanks]. Databanks examines the conflict between society's right to know and individual privacy concerns, and is based on information gathered from visits, interviews, and surveys conducted from 1970 to 1972 at 55 leading educational and professional institutions in business, government, and welfare systems.

In Databanks Dr. Westin writes that the definition of privacy " . . . involves the social policy issues of what information should be collected at all and how much information should be assembled in one information system." Id., at 393.

According to Dr. Westin, he has not changed his basic definition of privacy. Rather, Westin claims his earlier definition in Privacy and Freedom is "generic," and applies to a variety of social and cultural contexts. The Databanks definition is "aimed at the organizational ethos and is limited. It assumes the existence of a society in which records are being kept." Conversation with Dr. Alan F. Westin, June 10, 1983.

65. See, e.g., L. Lusky, Invasion of Privacy: A Clarification of Concepts, 72 Colum. L. Rev. 693 (1972).

66. American Heritage Dictionary of the English Language 246 (1976 ed.).

67. More than three quarters of the public say they are "very" or "somewhat" concerned about threats to their personal privacy. See supra note 5, at 7.

68. See Palko v. Connecticut, 302 U.S. 319 (1937) (Butler, J. dissenting). Justice Cardozo noted that freedoms of thought and speech are the "matrix, the indispensable condition of nearly every other form of freedom." Id., at 327. See also the Pentagon Papers cases, New York Times Co. v. United States, and United States v. Washington Post, 403 U.S. 713 (1971) (United States brought action to enjoin publication of certain classified material against The New York Times and Washington Post).

69. Lusky, supra note 65, at 706. Lusky makes this argument criticizing Professor Arthur Miller's definition of privacy as a "right," but the same criticism applies to the word "claim." Values that conflict with individual privacy are cited at note 50. See also Westin, Databanks, supra note 64.

70. Professor Miller has defined privacy as a right: "[T]he basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to him." Miller, supra note 2, at 25.

71. Because individual viewpoints vary considerably on what constitutes personal information, and because the law must take into account competing interests and considerations, it would be unrealistic and inefficient to attempt to accommodate everyone's conception of what personal information should be protected from disclosure. Private, personal, and confidential information will be used interchangeably hereafter.

72. It might be asserted that it would be most accurate and responsive to privacy concerns to let individuals define what is "personal information" themselves rather than imposing a community standard. But it has been asserted by various political theorists that the notion of a popular consensus may be somewhat idealistic, if not presumptuous. See J. Ely, Democracy and Distrust 63-69 (Harvard University Press: Cambridge, 1980). In his book on the legitimacy of judicial review, Ely argues there is rarely such a thing as a popular consensus.

Moreover, the notion of a popular consensus raises definitional problems of how and whom to trust to devise the standard. Finally, the assumption of a popular will also assumes the existence of a political process that is open, or at least, representative of all citizens fairly -- rich, poor, influential, and weak. This may not be an accurate portrayal of the political process, however.

73. It is recognized that certain communications and information may be more or less protected depending on whether one is a "public figure" or not. However, because this factor is mainly relevant to defamation rather than privacy issues, the distinction will not be made in this paper. Moreover, private information may be subject to qualified disclosure when there are competing law enforcement considerations.

74. See Warren & Brandeis, supra note 25.

75. Id., at 195. See also, E.L. Godkin, "The Rights of the Citizen to His Own Reputation," Scribner's Magazine Illustrated 60, 66-67 (July 1890). In his article on the natural rights of citizens, Godkin warned of the dangers to privacy posed by the newspaper:

> The chief enemy of privacy in modern life is that interest in other people and their affairs known as curiosity, which in the days before newspapers created personal gossip . . . In all this the advent of the newspapers, . . . has made a great change . . . [G]ossip about private individuals is now printed, and makes its victim, with all its imperfections on its head, known hundreds or thousands of miles away from his place of abode . . . It thus inflicts what is, to many men, the great pain of believing that everybody he meets in the street is perfectly familiar with some

> folly, or misfortune, or indiscretion, or weakness, which he had previously supposed had never got beyond his domestic circle. Id., at 66.

76. See, e.g., Pugh v. Telephone Company (a Kentucky court upheld the telephone company's right to cut off a defendant's telephone service for "damning the telephone company" over the telephone wire). The court said:

> [T]he inventors have a right to be protected, and have their instrument placed in a respectable light before the world, otherwise it might go out of use.

"Improper Use of Telephone," 6 The Legal News 105 (1883). Fears such as these are often proven unfounded after time.

Another article, written in 1882 on legal issues likely to be posed by the telephone, stipulated that whether an affiant could make an affidavit by telephone would become an "interesting question of law." "Swearing by Telephone," 26 The Albany Law Journal 326 (1882). The article said the answer would depend on whether telephones were "a mere carrier" or whether they "annihilate[d] space." Id. If the latter view were espoused by the courts, the article posited that there might be danger of "counterfeit affiants." Id. This question never became a legal issue raised in court.

Finally, in an article that appeared at the inception of television, the author speculated that several privacy issues might raise legal questions that would have to be resolved. For instance, the writer questioned the privacy rights of televised sports spectators, and the privacy rights of performers in old movies. The article says injecting commercials in the wrong place, which would interrupt a movie, might subject television stations to greater risks of being sued. The writer also speculated that performers might sue stations for distorted, uncomplimentary likenesses that might injure people's reputations, that camera quirks might give rise to defamation suits, and that "the television broadcaster's inability to 'cut' would present an incalculable hazard." D.M. Solinger, "Television and the Law," Fortune Magazine, at 160-163 (1948). Most of these questions never evolved into harms that were realized, however, either because the speculations were premature, or because technology improved.

77. According to Alan G. Merten, professor of computer and information systems at the University of Michigan, "[t]he places doing the best jobs [of protecting their information] are those that have had previous problems." Thus, experience may be the best guide to protecting information, and the best policy to protect information privacy may be to wait for harms to materialize. See "Information Management, Locking the Electronic File Cabinet," in Business Week, October 18, 1982, at 123 [hereafter cited as "Information Management"].

78. Warner Amex Cable Communications set the industry standard in 1981 by enacting its Privacy Code. Cox Cable Communications Inc. and Storer Cable Communications have enacted less comprehensive Privacy

Codes. The Cable Association of New York has also adopted a Privacy Code. The National Cable Television Association was considering adopting an industry-wide privacy code, but no further action was taken after 1983 because of the introduction in Congress of the federal cable television bills that contained privacy provisions. Telephone interview with James McElveen, Director of Public Relations, National Cable Television Association (April 9, 1984). The Cable Franchise Policy and Communication Act, 98th Cong., 2nd Sess. (1984), contains a section called subscriber privacy protections. See §631 "protection of subscriber privacy" and §634 "unauthorized reception of cable service." Id. See also Federal Regulations herein.

79. According to one source, approximately 5 million personal computers are expected to be in use in 1985 and industry forecasts for 1990 range from lows of 8 to 10 million to highs of 15 to 25 million. See Westin, Personal Computing, supra note 1, at 113-114.

80. Analysts' projections of a nation inundated with two-way cable have been moderated. According to Paul Kagan Associates, Inc., only 10% or fewer of the projected 53 million subscriptions to cable in 1990 will be two-way. Paul Kagan Associates, Inc, 62 Cable T.V. Technology, Dec. 14, 1983, at 1. The industry has been plagued by unexpected competition from alternative forms of technology such as DBS, STV, MDS, LFTV and microwave which can beam entertainment programs onto television screens for less money than cable (see J. Thomas, "Cable: The Possible Dream?" Boston Globe, March 23, 1984, at 70); lower-than-projected profit margins, losses of programming sources, and struggles among the cable industry, its competitors, cities, states, and the federal over the control of program content; rate regulation and general jurisdiction (see S. Salmans, "Cable Operators Take a Bruising," The New York Times, March 4, 1984 at 22). Still, analysts anticipate that despite growing pains, two-way services in the home, whether cable or hybrid technology, will simply be longer in coming than predicted. See comments of Ed Dooley, vice president of National Cable Television Association, and of Art Thompson, general manager of Cablevision of Boston cited in Thomas, Id., at 69, 70. See also comments of Dennis Leibowitz, cable analyst with Donaldson, Lufkin & Jennrette cited in Salmans, Id., at 22.

81. Although the most publicized interactive cable system is Warner Amex's Qube, other interactive systems have been or are being tested in the United States by Cox Cable Communications, Inc., Storer Cable Communications, Times Mirror Cable, and other local companies. See Salmans, supra note 80, at 22.

82. See J. Pearl, "The Software Channel," Forbes Magazine, June 18, 1984, at 158.

83. Nash & Smith, supra note 2, at 10.

84. See Wicklein, supra note 3, at 19.

85. Times-Union, January 12, 1983, at 2-3. Warner is proposing to reduce the scope of its two-way system in Milwaukee, however. See S. Cobb, "Milwaukee, Cincinnati Officials Question Cutbacks by Warner

Amex," Multichannel News, February 6, 1983 1, at 44. The Company also hopes to sell its franchise in Pittsburgh, Pennsylvania to Telecommunications, Inc. to avoid the high costs of operating its state-of-the-art system there. "Warner Amex's Lowering Expectations," Broadcasting, March 19, 1984, at 37-38.

86. Wicklein, supra note 3, at 18, but see Nash & Smith supra note 2, at 45. They claim a poll is conducted once every 20 seconds.

87. Nash & Smith, supra note 2, at 41.

88. Id.

89. Id.

90. Nash & Smith, supra note 2, at 45. Not all operators, however, monitor their systems all the time. The Cox Communications System, for example, only monitors the network when the interactive cable television is in use. Conversation with Ben Compaine, Program on Information Resources Policy, Harvard University, 1982.

91. Nash & Smith, supra note 2, at 40.

92. The leading videotex systems outside of the United States are Prestel in Britain, Antiope in France, and Telidon in Canada. Telidon, which was developed by Bell Canada, may also be transmitted over other media such as optical fibers, cable or broadcast channels, or other link technologies that may evolve. See generally Id., at 63-78.

93. Companies that have substantial investments in U.S. development of videotex or electronic databases include publishers, Knight-Ridder and Dow Jones; financial institutions, Chemical Bank, American Express, and Merrill Lynch, Pierce, Fenner & Smith; retailers, Federated Department Stores and Sears Roebuck; cable television operators, Cox Broadcasting and Warner Amex; and instrument makers, Tandy, Texas Instruments, and Zenith. See "Window on the World, The Home Information Revolution," Business Week, June 29, 1981, at 74-76.

94. See Martin, supra note 3, at 128. See also D. Sanger, "Technology, An Electronic O.E.D. Edition," The New York Times, July 5, 1984, Id., at 2. The publishers of the Oxford English Dictionary plan to input and revise it on a database.

95. Id., at 87.

96. See M. Tyler, "Videotex, Prestel and Teletext and the Economics and Politics of Some Electronic Publishing Media," 3 Telecommunications Policy 37, at 42 (March 1979).

97. See Martin, supra note 3, at 92.

98. Although most computer systems are not connected to an information provider, Nabu Network Corp., an Ottawa, Ontario based company, is currently test marketing software programs transmitted over

cable wire. One market in Ottawa has 1,400 subscribers, or 2% of that city's cable subscribers. In Alexandria, Virginia, the service has been introduced to 20,000 cable TV subscribers through Tribune Cable System. See Pearl, supra note 82, at 157.

Subscribers get an assortment of 50 education, information, and game software for a basic charge of $14.95 per month. Additional programs, word processing, spread sheet software, and business information are available in ranges from $4.95 for a few programs to $27.95 for an entire package. Software similar to the package if purchased at retail in disks would cost approximately $2,500. See Id., at 158.

99. See Westin, Personal Computers, supra note 1, at 114 for current estimates and projections of the number of computers being operated by home users.

100. Id.

101. Id.

102. Id.

103. See Martin, supra note 3, at 101. See generally P.P.S.C., Info. Society, supra note 2, at 101; National Commission on Electronic Funds Transfer, EFT and the Public Interest (Interim Report, Feb. 1977) [hereafter cited as NCEFT]; K. Colton & K. Kraemer (ed.), Computers and Banking, Electronic Funds Transfer Systems and Public Policy (Plenum Press: New York, 1980) [hereafter cited as Computers & Banking].

104. See Comment, Financial Privacy in an Electronic Fund Transfer Environment: An Analysis of the Right to Financial Privacy Act of 1978 and California Financial Privacy Law, 23 U.S.F.L. Rev. 485, 486 n.6 (1979) [hereafter cited as San Francisco].

105. Horan, "Outlook for EFT Technology," in Computers & Banking, supra note 103, at 27.

106. Id.

107. Id.

108. Id.

109. Id.

110. Id.

111. Id., at 24.

112. Id.

113. Id., at 35.

114. Id.

115. See San Francisco, supra note 104, at 487, n.6.

116. See Horan, supra note 103, at 25.

117. Id., at 32.

118. See Martin, supra note 3, at 79.

119. Computer Fraud and Electronic Trespass: Hearings on H.R. 3570 Before the Subcommittee on Crime, Committee on the Judiciary. U.S. House of Representatives (November 10, 1983) (testimony by Peter C. Waal, GTE Telenet Communications Corporation), at 4 to 5 (hereafter cited as Computer Fraud).

120. Id. The federal government has almost completed arrangements for establishing 24-hour-a-day direct electronic links among approximately 100 federal agencies and 7 major private credit reporting companies. Once the links are in place, agency personnel will be able to examine the status of bank loans, liens, divorce records, and department store, oil company, and credit card accounts. See D. Burnham, "Agencies Creating System To Check Citizens' Credit," The New York Times April 8, 1984, at 17. While such information has been used by the government in the past, the combined developments of new regulations passed pursuant to the Fair Credit Reporting Act and computerized links "are expected to make such checks far more extensive." Id., at col. 2. See also P.P.S.C., Info. Society, supra note 2, at 12. The Privacy Commission concluded in its report on stored records:

> the broad availability and low cost of computer and telecommunications technologies provide both the impetus and the means to perform new record-keeping functions . . . On one hand, they can give [an individual] easier access to services that make his life more comfortable or convenient. On the other, they also tempt others to demand, and make it easier for them to get access to information about him for purposes he does not expect and would not agree to if he were asked . . . The real danger is the gradual erosion of individual liberties through the automation, integration and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent and wholly justifiable.

121. Computer Fraud, supra note 119, at 5 to 6.

122. Id.

123. See supra notes 7 to 11 of text, and Appendix B.

124. In part three of Databanks, supra note 64, Dr. Westin describes the changes in organizational record-keeping, which many commentators assumed to be occurring as a result of increased computerization, but which were not observed among the organizations

studied from 1970 to 1972. These assumptions were: 1) agencies were collecting more sensitive information, 2) there would be an increase in the intra- and inter-organizational exchange of sensitive information, and 3) individuals would have less opportunity to know about what information about them was being collected.

However, Dr. Westin found some of the reasons why these phenomena had not occurred were because of high cost and software inflexibility. Spokesmen for some of the organizations interviewed said they felt more information should be retained on individuals, and that they would have collected more information if they were not prevented by technological or legal restrictions.

125. See Nash & Smith, supra note 2, at 9. The following surveillance sheet is an example of one writer's vision of the kind of projections which could be made based on information likely to be stored in electronic database systems:

NATIONAL DATA BANK
DAILY SURVEILLANCE SHEET
CONFIDENTIAL
JULY 11, 1987

SUBJECT. Dennie Van Tassel
San Jose State College
Male
Age 38
Married
Programmer

| | | |
|---|---|---|
| PURCHASES. | Wall Street Journal | .40 |
| | Breakfast | 2.65 |
| | Gasoline | 10.00 |
| | Phone (328-1826) | .10 |
| | Phone (308-7928) | .10 |
| | Phone (421-1931) | .10 |
| | Bank (Cash Withdrawal) | (120.00) |
| | Lunch | 2.00 |
| | Cocktail | 1.00 |
| | Lingerie | 21.85 |
| | Phone (369-2436) | .35 |
| | Bourbon | 8.27 |
| | Newspaper | 8.10 |

** COMPUTER ANALYSIS **

Owns stock (90 percent probability)

Heavy starch breakfast. Probably overweight.

Bought $10.00 gasoline. Owns VW. So far this week he has bought $40.00 worth of gas. Obviously doing something else besides just driving the 9 miles to work.

Bought gasoline at 7:57. Safe to assume he was late to work.

Phone No. 328-1826 belongs to Shady Lane. Shady was arrested for bookmaking in 1972.

Phone No. 308-7928. Expensive men's barber -- specializes in bald men or hair styling.

Phone No. 421-1931. Reservations for Las Vegas (without wife). Third trip this year to Las Vegas (without wife). Will scan file to see if anyone else has gone to Las Vegas at the same time and compare to his phone call numbers.

Withdrew $120.00 cash. Very unusual since all legal purchases can be made using the National Social Security credit card. Cash usually only used for illegal purchases. It was previously recommended that all cash be outlawed as soon as it becames politically possible.

Computers and People, 31 (Aug. 1979). The amounts spent for The Wall Street Journal, breakfast and gasoline have been increased to reflect more realistic prices.

126. See comments of New York Attorney General Robert Abrams before New York State assembly committee hearing on two-way cable privacy but reported in Breznick, "NY Attorney Gen'l Favors Cable Bill," Multichannel News, March 26, 1984, at 33.

127. See Westin Popular Computing, supra note 1, at 1.

128. Moody responded to this attack by admitting that he watches adult movies, but does so as part of his civic duty. "It's part of my job," he stated, "like going to look at the site of a flood." See Panorama, February 1981, at 59.

129. Although the movie theater proprietor sought specific names, the judge in the case narrowed the subpoena to limit the information disclosed to the number of viewers. See The New York Times, January 12, 1982, at B2.

130. See Nash & Smith, supra note 2, at 6.

131. See Westin, Popular Computing, supra note 1, at 115.

132. See C. Tapper, Computer Law (Longman: London and New York, 1978), at 120.

133. Id.

134. According to Herman MacDaniel, president of Management Resources International in 1982, "most frauds have been [done] by people who were not technically [sophisticated]." See "Information Management," supra note 77, at 124.

135. Id.

136. The Bank Secrecy Act, Pub. L. 91-508, Oct. 26, 1970, 84 Stat. 1118, 12 U.S.C. §§18296, 1951-1959. Section 1829 requires insured banks to retain records on persons having accounts and authorized to act with respect to such accounts, and to make and keep reproductions of every instrument presented for payment or deposited together with the identification of the party for whose account it is to be deposited or collected (unless the person's account is already on record). Records are not required to be kept for more than 6 years. 12 U.S.C.A. §1829b(g). Sections 1951 to 1959 contain similar record-keeping requirements applicable to uninsured banks.

137. P.P.S.C., Info. Society, supra note 2, at 15 n.7 citing U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens 41 (1973).

138. The Fair Credit Reporting Act of 1971, Pub. L. 90-321, Title U1, §602, Oct. 26, 1970, 84 Stat. 1136, 15 U.S.C. §1681. This Act requires consumers to be notified and supplied with the names and addresses of consumer reporting agencies making adverse decisions about consumers, 15 U.S.C. §1681m; requires notification to consumers when an investigative report is being compiled on them not later than three days after the report is first requested; 15 U.S.C. §1681d (the term investigative report does not include factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when such information was obtained directly from a creditor or from the consumer) 15 U.S.C. & 1681a(e); sets forth permissible purposes for consumer reports, 15 U.S.C. §1681b; prohibits reporting of obsolete information (the Act exempts credit transactions including principal of $50,000 or more, the underwriting of life insurance for $50,000 or more, and employment decisions involving salaries expected to equal $20,000 or more, 15 U.S.C., §1681c; sets forth required reporting procedures and disclosures to consumers, 15 U.S.C. §§1681c-1681h; and establishes procedures in case of disputed accuracy §1681i.

139. 15 U.S.C. §§1601-1677. Pub L. 93-495, Title III, §302 Oct. 28, 1974, 88 Stat. 1511 (amended March 23, 1976). The Act was passed to mandate disclosure of credit terms to consumers so consumers will be able to compare more readily the terms available to them, and to avoid uninformed use of credit. 15 U.S.C. §1601(a).

140. 5 U.S.C. §552, Pub. L. 89-554, Sept. 6, 1966, 80 Stat. 383 (amended Sept. 13, 1976).

141. Individuals do not have the right to examine information that is exempt from FOIA's disclosure provisions, however. These matters are essentially those that are:

1) specifically established under Executive order to be kept secret;
2) related to the personnel rules and practices of an agency;
3) specifically exempt from disclosure by statute;

4) trade secrets;
5) inter-agency or intra-agency memorandums;
6) personnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of privacy;
7) investigatory records compiled for law enforcement;
8) contained in or related to examination, operation, or condition reports prepared by or on behalf of an agency responsible for regulating financial institutions;
9) geographical and geophysical information concerning wells.

See 5 U.S.C. §552(b)(1)-(b)(9).

142. 20 U.S.C. §1232g, Pub.L. 93-380, 88 Stat. 484, §513, Aug. 21, 1974.

143. 5 U.S.C. §552a, Pub.L. 93-579, §5 (amended June 1, 1977).

144. The disclosures authorized by the Privacy Act are essentially those that are:

1) to agency officers and employees who have a need for a record in the performance of their duties;
2) required by the Freedom of Information Act;
3) for a routine use;
4) to the Bureau of Concensus in order to conduct surveys;
5) to be used for surveys and which are to be transferred in a form that is not individually indentifiable;
6) to the National Archives for historical use;
7) to another agency for law enforcement upon written request by the head of the agency;
8) pursuant to a showing of compelling circumstances for the health or safety of an individual if notice is transmitted to that individual;
9) to either House of Congress;
10) to the Comptroller General for use in the course of his duties;
11) pursuant to a court order;
12) to a consumer reporting agency.

5 U.S.C. §552a(b).

145. 5 U.S.C. §552a(d)(1).

146. 5 U.S.C. §552a(d)(2)(B).

147. 5 U.S.C. §552a(e)(B).

148. 5 U.S.C. §552a(e)(1).

149. 5 U.S.C. §552a(b)(3).

150. 5 U.S.C. §552a(a)(7).

151. P.P.S.C., Info. Society, supra note 2, at 517-518. For example, Subsection 3(b)(7) of the Privacy Act requires that the head of an agency request information in writing and that the legitimate law enforcement activity for which the information is desired be specified before information can be released. The "routine use" provision has been used to circumvent this requirement. Id., at 517.

152. See §6 of Pub. L. 93-579.

153. See 40 Fed. Reg. 45877-8 (Oct. 3, 1975); 41 C.F.R. §§101-36000 to 361207 (1980)(regulations governing management of automatic data processing equipment used by the federal government).

154. See Privacy Protection Act of 1984: Hearings on H.R. 3743 Before the Committee on Government Operations, 98th Cong., 1st Sess. (1983). In the words of one witness, "OMB has 'virtually abdicated responsibility' for The Privacy Act." Id., at H6344.

155. See definition of agency 5 U.S.C. §552a(1); 5 U.S.C. §552(e). H.R. 3743 (the Glen English Bill), which was introduced into Congress in 1983, would have established a Privacy Protection Commission as an independent agency of the executive branch. The Commission would have been responsible for proposing legislation to improve protection of information privacy, and for assisting in "the development and implementation of private sector data protection standards." Privacy Protection Act of 1984: Hearings on H.R. 3743 Before the Committee on Government Operations, 98th Cong., 1st Sess. (1983). The bill died in committee. Telephone interview with Robert M. Gellman, Counsel, Government Operations Committee, House of Representatives, United States Congress (March 15, 1984).

156. Privacy Act of 1974, Pub. L. No. 93-579, §5, (amended June 1, 1977).

The Privacy Protection Commission was not the first Presidential commission to address the need to protect stored data and individual privacy. In 1974 the President established the Domestic Council Committee on the Right of Privacy, which was chaired by the Vice President. The Committee endorsed initiatives addressing military surveillance of civilian political activities, criminal justice information, electronic funds transfer systems, the confidentiality of taxpayer records, federal mailing lists, customer records maintained by financial institutions, federal employee rights, and security guidelines for federal computers and communications systems. The Committee and the Council of State Governments co-sponsored a 1974 seminar on privacy, which led to a resource document entitled "Privacy, A Public Concern" (K. Larsen ed. 1975).

157. Privacy Act of 1974, 5 U.S.C. §552a(b).

158. P.P.S.C., Info. Society, supra note 2, at 362 to 363. (emphasis added).

159. Id.

160. The Privacy Commission proposed by the Glen English Bill would have been responsible for developing principles to improve private sector data protection. See supra note 155.

161. United States v. Miller, 425 U.S.435 (1976). See supra text accompanying notes 15 to 17.

162. Right to Financial Privacy Act of 1978, 12 U.S.C. §§1101-1122, §§3401-3422 (amended 1980 and 1982).

163. Id., at §§3404(c), 3405(2), 3406(c), 3407(2), 3408(4), 3412(b), and 3410.

164. Electronic Fund Transfer Act, 15 U.S.C. §1693-1693r (1978 amended 1982).

165. Id., at 15 U.S.C. §1693d.

166. Id., at 15 U.S.C. §1693f.

167. Id., at 15 U.S.C. §1593c.

168. Id., at 15 U.S.C. §1693b, 12 C.F.R. Part 205, App. A, Supp. I & II.

169. Regulation E includes provisions on disclosure of account information and terms to customers, Id., at §205-7; procedures for error resolution Id., at §205.8; documentation of transfers, Id., at §205.11; and procedures for preauthorized transfers, Id., at §205.10.

170. See the Bank Secrecy Act, 12 U.S.C. §1829b, 1951-1959 (1970).

171. See Heller, "EFT, Privacy and the Public Good," in Computers & Banking, supra note 103, at 86.

172. See Horan, Outlook for EFT Technology, supra note 103, at 29-36.

173. Pub. L. 96-440, §§101, 105-107, 201, 202, 94 Stat. 1879-1883, Oct. 13, 1980, 42 U.S.C. §§2000aa, 2000aa-5 to aa-7, 2000aa-11, 2000aa-12.

174. Id., at 42 U.S.C. § 2000aa.

175. The Omnibus Crime Control and Safe Streets Act of 1968, Title III, 18 U.S.C. §2510-2520 (1968).

176. The Communications Act of 1934, c.652, Title VI, §605, 47 U.S.C. §605 (amended 1968, 1982).

177. 18 U.S.C. §2510(1).

178. 18 U.S.C. §2511, 2516.

179. See F. Lloyd, Cable Television's Emerging Two-Way Services: A Dilemma for Federal and State Regulators, 36 Vand L. Rev. 1045 (1983) for a discussion of the FCC's attempt to impose common carrier status on two-way cable television. See Koenig, supra note 4 for an argument that cable service is a form of local utility that should be regulated like common carrier. Koenig writes

> Subscribers who sign up are not merely dealing with a commercial merchant but are obtaining basic communications services. Under this view, cable service would appear more as a right or necessity of local residents rather than a merely optional entertainment. This would be consistent with the special legal status cable systems enjoy in many jurisdictions, such as zoning exemptions, utility tax treatment, condemnation power, and entry rights into apartment houses. Id., at 108.

180. A number of companies now offer shopping services over the telephone. Teleshopping is currently provided by Comp-U-Card International, Inc. of Stamford Connecticut, Byvideo Inc. of Sunnyvale, California, and Viewdata Corporation of America, a Knight-Ridder subsidiary in Florida. Times Mirror Videotex Services and Keycom Electronic Publishing are expected to start services in Chicago and Orange County, California, in 1984. "New Video Game: Shopping, Items Offered At Home and in Stores," The New York Times, April 26, 1984, §4, at 1.

181. See United States v. Seidletz, 589 F.2d 152, 157 (4th Cir. 1978) cert. denied 99 S. Ct. 2030 (1978).

182. See Smith v. Maryland, 442 U.S. 735, 742 (1978) (petitioner had no legitimate expectation of privacy in the telephone numbers he dialed).

183. Communications Act of 1934, c.652 title VI, §605 47 U.S.C. §605 (amended 1968, 1982).

184. Id., at §605 as amended.

185. See Bubis v. United States, 384 F.2d 643 (9th Cir. 1967); United States v. Russo, 250 F. Supp. 55 (E.D. Pa. 1966) and n. 289; United States v. Butenko, 494 F. 2d 593, 600 (3rd Cir.), cert. denied, 419 U.S. 881 (1974). United States v. Zarkin, 250 F. Supp. 728 (D.D.C. 1966). All of these cases, except Butenko, were decided prior to the amendment of §605. The original trial in Botenko concluded in 1964. Butenko, 494 F.2d at 596. Therefore, none of these cases supports the proposition that §605 continues to protect wire transmissions. Cited in R. Neustadt, G. Skall, & M. Hammer, The Regulation of Electronic Publishing, 88 Fed. Com. L.J. 404, at n. 287 and 289 (n. 288 omitted)(1981).

186. The Omnibus Crime Control and Safe Streets Act of 1968 Title III, supra note 62, S. Rep. No. 1097, 90th Cong., 2d Sess., reprinted in

1968 U.S. code Cong. & Ad. News 2112, 2196. See United States v. Seidlitz, 589 F. 2d 152 (1978).

187. See United States v. McGuire, 381 F.2d. 306 (1967), cert. denied, 389 U.S. 1053 (1968) (court said the prohibition against interception of a communication does not mean that a party to a telephone conversation may not disclose it). See also United States v. Butenko, 494 F.2d 593 (3rd Cir. 1974) cert. denied (telephone company did not violate §605 by monitoring foreign intelligence telephone conversations and turning over contents of conversations to law enforcement agencies); Coates v. United States, 307 F. Supp. 677 (D.C. No. 1970) (where a recipient of a telephone call consented to eavesdropping by a government agent unknown to the other party, there was no interception or divulgence under the Communications Act).

188. Cable Television Clarification, 46 F.C.C. 2d 175 (1974).

189. Id., at 183. A similar fear was expressed by Edward P. Kearse, Executive Director of the Commission on Cable Television for New York State. "We should not be overly concerned about a problem that does not currently exist and thereby discourage the building and implementation of the interactive cable system," he stated in 1982. Times Union, January 12, 1982, at 2-3.

190. Cable Television Clarification, 46 F.C.C. 2d 175 (1974).

191. Id., at 184.

192. Id.

193. Cable Television Clarification, 46 F.C.C. 2d 175 (1974). See generally C. Ferris, F. Lloyd, T. Casey, "Cable Two-Way Services: An Area of Federal-State Conflict," in Cable Television Law: A Video Communications Practice Guide, ch. 14 (Mathew Bender Publications: New York and Washington D.C., 1983) for a discussion of the confusion over the FCC's jurisdiction over two-way cable services.

194. See Introduction and Appendix B: Definitions in this paper for a discussion of potential privacy concerns created by electronic technology.

195. This study is intended to be a general overview and is not intended to be comprehensive. For a more comprehensive study of state privacy statutes See Smith, supra note 54.

196. Cal. Const. Art 1 § 1. The California courts have stated that "'the right of privacy' is the right to live one's life in seclusion, without being subjected to unwarranted and undesired publicity." See Gill v. Curtis Publishing Company, 239 P.2d 630, 38 Cal.2d 273 (1952). The right, according to at least one California court, exists independent of the comon rights of property, contract, reputation and physical integrity. Id.

197. See Doe v. Roe, 400 N.Y.S.2d 668 (Sup. Ct. 1977). (Husband co-authored book with wife's psychiatrist disclosing confidential information about marriage and wife without wife's consent. The court held that husband and psychiatrist had breached an affirmative duty imposed by statute banning disclosure of confidential medical information).

198. Id., 400 N.Y.S.2d 668 at 676. (The court said every physician makes an implied promise of confidentiality to his patient. The court also said that although no case to date had recognized a common law right of privacy, it had been predicted that the New York Court of Appeals would abandon the holding of Robertson v. Rochester Folding Box Company, 171 N.Y. 538, 64 N.E. 442 (1902), that no cause of action would be recognized for invasion of privacy apart from that authorized by Civil Rights Law. Id.).

199. See Privacy Protection Law in the United States, N.T.I.A. Report Series, Report 82-78, May 1982, at 10 [hereafter cited as Privacy Protection Law].

200. See Ind. Code Ann. § 4-1-6-1 (West 1979); Mass. Gen. Laws Ann. Ch. 66A §§ 1-3 (West 1976); Va. Code Ann. §§ 2.1-377 (1976).

201. See, e.g., Ind. Code Ann. § 4-1-6-2(b) (Burns 1977); Va. Code Ann. § 2.1-382(2) (1976).

202. See, e.g., Utah Code Ann. § 63-50-7 (1975).

203. See The Privacy Act of 1974, 5 U.S.C. § 552a (1976); The Freedom of Information Act, 5 U.S.C. § 552 (1967).

204. See, e.g., Ariz. Rev. Stat. Ann. § 16-806 (1977). The Arizona statute provides that information shall not be used for any purpose other than as stated and filed in writing in accordance with subsection (a). But subsection (d) says information may be used for a purpose other than that for which it was collected if information is filed and publicly available as provided in subsection (a). Subsection (a) does not require prior notice to the data subject of the use of information. Subsection (e) says a person shall be notified when he is the subject of stored information, but excepts information which is defined by statute as confidential or records relating to medical or psychiatric treatment . . . or information compiled in reasonable anticipation of a civil action or proceeding. Id., at § 16-806(e); Hawaii Rev. Stat. §§92E-1 to 92E-13, Hawaii's Fair Information Practice Statute, requires each agency that maintains any accessible personal record to make that record available to the individual on whom it pertains. Id., at §92E-2. The statute does not provide for agencies to notify such individuals when information is being collected or maintained, however. See also Conn. Gen. Stat. Ann. § 4-193d (1977).

205. Larceny is a form of theft.

206. This conclusion based on a review of approximately 10 state theft statutes and the Model Penal Code (1974). The study is not meant

to be exhaustive. The New York statute, however, together with the Model Penal Code, are assumed to be representative of, or perhaps more progressive than, theft statutes in most states. Larceny and theft provisions vary among different jurisdictions.

207. See Model Penal Code §§ 223.0 (1), 223.2 (1) (1974). The basic theft provisions in most jurisdictions are similar to the provisions in the Model Penal Code.

208. See N.Y. Penal Law § 155.05 (McKinney 1969).

209. See, e.g., N.Y. Penal Law § 155.00(3) (1969); Model Penal Code § 223.0(1) (1974).

210. See N.Y. Penal Law § 155.05 (McKinney 1969); Model Penal Code § 223.2(1)(1974).

211. 248 U.S. 215(1918).

212. International News Service v. Associated Press, 248 U.S. 215, 239 (1918).

213. Id.

214. See Goldstein v. California, 412 U.S. 546 (1973). (State law against record piracy not preempted merely because Congress has the power to legislate in this area. Goldstein also says Sears and Compco, infra, at note 215, did not overrule INS and the misappropriation doctrine.) See also Aronson v. Quick Point Pencil Company, 440 U.S. 257 (1979) (trade secret royalty liability of indefinite duration under state law not preempted); American Television & Communications Corporation v. Manning (Colo. App. 1982) (pirating plaintiff's exclusive right to deliver HBO programs via microwave and selling such programs in competition with plaintiff constituted misappropriation and unfair competition). See also Data Cash Systems Inc. v. JS&A Group, Inc., 480 F. Supp. 1063 (N.D. Ill. 1979), aff'd 628 F2d 1038 (1980); Adolph Coors Company v. Genderson & Sons, Inc. 486 F. Supp 131 (D. Colo 1980). See generally 2 R. Callman, The Law & Unfair Competition ch. 15, at 9 and cases cited in §15.08 (3rd ed. and 1981 Supp).

215. See Sears, Roebuck & Company v. Stiffel Company, 376 U.S. 225 (1964). (Stiffel had been granted design and utility patents on a lamp. Sears marketed a substantially identical lamp without placing identifying labels on the lamp. The Supreme Court said the effect of a patent is a statutory monopoly; accordingly, it cannot be used to secure any monopoly beyond that inherent in the patent or in violation of the antitrust laws. The Court continued, to allow a state by use of its law of unfair competition to prevent the copying of an article that represents too slight an advance to be patented would be to permit the state to block off from the public something that federal law has said belongs to the public.) 376 U.S., at 230-232. See also Compco v. Day-Brite Lighting, Inc., 376 U.S. 234 (1964).

216. See The Copyright Revision Act of 1976, Pub. L.94-553, Title I, §101, Oct. 19, 1976, 90 Stat. 2572, 17 U.S.C. §301.

217. International News Service v. Associated Press, 248 U.S. 215, 250 (1918).

218. See Triangle Publications v. New England Newspaper Publishing Company, 46 F. Supp 198 (D. Mass. 1942). (Judge Wyzanski said Massachusetts courts do not accept INS because "I could hardly be unmindful of the probability that a majority of the present Justices of the Supreme Court of the United States would follow the dissenting opinion of Justice Brandeis . . . because they share his view that monopolies should not be readily extended . . . ." 46 F. Supp., at 204).

219. The Copyright Revision Act of 1976, 17 U.S.C. § 301.

220. Id.

221. Such subject matter is expressly excluded from the scope of federal copyright preemption by Sections 301(a) and (b)(1). See also Zacehini v. Scripps-Howard Broadcasting Company, 433 U.S. 562 (1977) (performance recorded against will of the performer may be protected by state law without interference from federal law).

222. The law of unfair competition (or misappropriation) and copyright are not intended to protect to same interests, however. Copyright law is intended to foster literary and artistic creation, and prevents competition. The law of unfair competition is intended to protect the viability of a business system and to spur competition by preventing paracitism.

223. See, e.g., Synercom Technology, Inc. v. University Computing Company, 474 F. Supp. 37 (N.D. Tex 1979) for an analogous argument.

224. For instance, it has been held that an unauthorized person (i.e., a customer) who attempts to benefit from pay T.V. by intercepting signals without paying for it, and anyone who assists him in doing so, is in violation of §605 of the Communication Act and there is an implied private right of action for an injunction and damages. 47 U.S.C. §605. See Callman, supra note 225, at Cumulative Supp. v. 2 at 33, n. 21 and cases cited therein.

225. See Mass. Gen. Laws Ann. C. 266 §30(2) (West). The term "property" includes "a security deposit received pursuant to section fifteen B of chapter one hundred and eight-six, electronically processed or stored data, either tangible or intangible, data while in transit . . . ." Id. Additionally, Massachusetts has amended the term "trade secret" to include "anything tangible or electronically kept or stored, which constitutes, represents, evidences or records a secret scientific, technical, merchandising, production or management information, design, process, procedure, formula, invention or improvement." Id., at §30(4). See also N.Y. Penal Law §155.05 (McKinney 1969). "Property" is defined by the New York statute as "any money, personal property, real property, thing in action, evidence of debt or contract or any article, substance

or thing of value." While this definition is broad enough to include electronically stored and processed data, much personal information retrievable from videotex or personal computers will have only "economic value" to the person about whom the information pertains.

226. See, e.g., Ariz. Rev. Stat. Ann. §13-1802A6(1977); Alaska Stat. §11.46.200; Ill. Rev. Stat. c. 38 §16-10; N.Y. Penal Law §165.15 (McKinney 1967, amended 1982).

227. For instance, Illinois specifically limits its statute to "cable television services." Cable television service means any cable television system or closed circuit coaxial cable communication system, or any microwave or similar transmission service used in connection with any cable television system or similar closed coaxial communications service. Ill. Rev. Stat. c. 38 §16-10(a)(1). See also Mass. Gen. Laws Ann. c. 266 §37D (West); N.Y. Penal Law §165.15 (McKinney 1981).

228. See, e.g., Ariz. Rev. Stat. Ann. §13-1802 A.6. (1977); N.Y. Penal Law §165-15 (McKinney 1981).

229. See Mass. Gen. Laws Ann. c. 266, §37D (West 1981).

230. See R. Couch, Note, A Suggested Legislative Approach to the Problem of Computer Crime, XXXVIII Wash & Lee L. Rev. n.4, 1173 (1981).

231. Id.

232. The following states had adopted cable television privacy acts as of July 1984: Illinois, Wisconsin, California, Minnesota, Connecticut, New York, and Rhode Island.

233. The Communications Consumer Privacy Act, Ill. Ann Stat. c. 38 §§87-1-87-3 (Smith-Hurd 1983).

234. Id., at §87-3(a). Damages for violations of the act are punishable by fines of up to $10,000. Id., at §87-3(b).

235. Wis. Stat. Ann. §134.45(1)(a). Although franchises in Wisconsin are granted by each municipality, the law applies a statewide standard to all Wisconsin franchises. Wis. Stat. Ann. §134.43 (West 1983). The above provision expressly excludes devices "related to security, fire and utility service." Wis. Stat. Ann. §134.45(1)(b).

236. Id., at §(2). The Wisconsin act does not prohibit cable operators from collecting billing information and from conducting system sweeps to verify system integrity. Violations of this act may be assessed at fines of up to $50,000 for the first offense and up to $100,000 for a second offense. Id., at §(4).

237. Cal. Penal Code §637.5(a)(1). This conduct may occur with the subscriber's express written consent or for electronic sweeps to monitor signal quality. Id.

238. The California Act says individually identifiable information shall include but not be limited to subscriber television viewing habits, shopping choices, interests, opinions, energy uses, medical information, banking data or information, or any other personal or private information. Id., at §637.5(2). Such information may be disclosed with the subscriber's express written consent. Id.

239. The act states that individual subscriber viewing responses or other individually identifiable information derived from subscribers shall be retained and used by cable companies only to the extent reasonably necessary for billing purposes and internal business practices, and to monitor subscriber terminals for unauthorized reception of services. Id., at §637.5(b).

240. The act provides, however, that nothing in this section shall be construed to prevent local franchising authorities from obtaining information necessary to monitor franchise compliance. Id., at §637.5(c).

241. A cable operator must correct the information upon a reasonable showing by a subscriber that the information is inaccurate. Id., at §637.5(d).

242. Id. §637.5(e). Violations of these provisions are misdemeanors punishable by fines not exceeding $3,000, and/or by imprisonment not exceeding one year. Id., at §637.5(i) and (j).

243. Minn. Stat. §238.05, subd. 2(b), subd. 8.

244. State of Connecticut Cable Television Subscribers Protection of Personal Privacy, Pub. Act No 83-33 (1983) amending §16-331(d).

245. The Minnesota cable regulatory agency is the state Cable Communications Board. The Connecticut Department of Public Utilities has jurisdiction over cable television regulation in this state.

246. See 4 Minn. Code Agency R. §4.202(W); Conn. Pub. Act No. 83-33 (1983), amending §16-331(d).

247. See 4 Minn. Code Agency R, §4.202(W).

248. The New York cable regulatory authority is the New York State Commission on Cable Television.

249. Rhode Island's cable television is under the aegis of the Rhode Island Division of Public Utilities and Carriers.

250. The New York cable operating rules specify that signals may not be transmitted without a subscriber's consent, terminals must be designated to allow subscribers to prevent return signals, and subscribers who are provided with two-way terminals must receive written notice of these rights and instructions to enable them to activate and deactivate their terminals. N.Y. Admin. Code tit. 9, §596.3(e). See also State of New York Commission on Cable Television, In the Matter of

The Establishment of Rules and Regulations Concerning Cable Television Subscriber Privacy, Notice of Proposed Rulemaking, Docket No. 90221, 83-045, Released March 3, 1983. The Commission Notice sets forth a number of findings on subscriber privacy including the following: 1) two-way and interactive television subscribers risk invasion of their privacy; 2) the danger of interception of subscriber-generated data exists; 3) information about subscribers is now released by cable operators to outsiders, and 4) cable operators do sell subscriber lists to outsiders. §11., at 3-4. The Commission invites comments, and sets forth a detailed proposal for cable subscriber privacy regulations. This Notice is currently circulating for comments.

The Rhode Island regulations provide that no signals of a Class IV CATV channel (defined in §1.9(b) of the regulations and, except for the substitution of "CATV" in the Rhode Island regulation for "cable television" in the FCC regulations, in FCC Rules and Regulations, 47 C.F.R., part 76, § 76.5(cc)) shall be transmitted from a subscriber terminal for the purposes of monitoring individual viewing patterns without the express written consent of the subscriber. Rules governing Community Antenna TV Systems, (1981) as amended, January 14, 1983 §1.9(b).

251. As of the date of this writing, two-way cable subscriber privacy legislation had been introduced in at least five states since the beginning of 1984: New York, A.7327--A, 1983-1984 Reg. Sess. Cal. No. 439 (1983); New Jersey A.731, P.L. 1972, c. 186 (c. 48:5A-1 et seq.); Pennsylvania S.508, Printer No. 1725, as amended, Feb. 14, 1984, Connecticut LCO No. 1528, Gen. Ass., Committee Bill No. 5878, February Sess. 1984; Maryland H.B. 1320/83-Cal., No. 255, Introduced Jan. 11, 1984.

The New York Cable Telecommunications Privacy Act, introduced by Assemblyman Melvin Zimmer has received considerable publicity because it would establish strict cable subscriber privacy standards in New York, and would set a precedent for other states to pass similar legislation.

The bill prohibits all persons from monitoring, observing, recording, intercepting, or transmitting any conversations or activities of a cable subscriber, A.7327--A, 1983-1984 Reg. Sess., Cal. No. 439 (1983) §833-b; from aggregating any individually indentifiable information concerning subscriber viewing patterns or responses (except for billing and when necessary to render a service requested by the subscriber), Id., at §833-c1; from conducting research or collecting identifiable information from subscriber mailing lists or other cable television company records, Id., at §833-b3; and from disclosing any subscriber information absent legal compulsion without prior written authorization from the subscriber. Id., at §833-f. Separate authorization is required for "each type of information collected or disclosed," and subscribers may revoke this authorization at any time. Id. Subscribers must be notified prior to or contemporaneous with each request to a cable operator for information, and must be given the opportunity to decline to allow disclosure of such information. Id., at §833-e3. Subscribers will be able to request all information compiled on them, and require correction of information upon a reasonable showing

that it is misleading or inaccurate. Id., at §833-h. Information compiled on subscribers must be destroyed upon completion of the uses for which such information was collected, or upon the termination of service by a subscriber. Id., at §833-d. Cable operators must also maintain adequate safeguards to protect the physical and electronic security of any individually identifiable subscriber information. Id., at §833-c3.

A court may award up to $10,000 in addition to damages to each aggrieved subscriber, if it finds the violation was intentional and/or the defendant has frequently or persistently violated the Act. Id., at §833-i. Section 833-j imposes criminal sanctions of $5,000 and/or imprisonment of not longer than one year for violations by an individual. Violations by a corporation are punishable by fines of up to $50,000 for each violation.

252. The conclusions of this section are based on an examination of the following state computer fraud statutes: Ariz. Rev. Stat. Ann. §13-2316; Del. Code Ann. tit. 11 §858; Fla. Stat. Ann. §815 (West); Ga. Code Ann. §§16-9-91 to 16-9-94; Minn. Stat. Ann. §§609.87 to 609.89; Mo. Ann. Stat. §§569.095 to 569.099; Mont. Rev. Codes Ann. §§45-6-310 to 45-6-311; N.M. Stat. Ann. §30-16A; R.I. Gen. Laws §§ 11-52-1 to 11-52-4; Utah Code Ann. §§76-6-701 to 76-6-704; Wis. Stat. §943.70.

253. See statutes listed in note 251, supra.

254. See, e.g., Fla Stat. Ann. §815.04, offenses against intellectual property, and §815.05, offenses against computer equipment or supplies. Mo. Ann. Stat. §569.095 deals with information classified as intellectual property, and §669.096 regulates tampering with computer equipment. Wis. Stat. §943.70(2) punishes offenses against computer data and programs, and §943.70(3) punishes offenses against supplies and equipment.

255. These crimes, often called "fraud" or "fraud in the first degree," are usually punished more harshly than other computer crimes. See, e.g., Ariz. Rev. Stat. Ann. §13-2316C; Del. Stat. Ann. §858(a); Ga. Code Ann. §16-9-93(a).

256. The penalty for these crimes, often called "fraud in the second degree" or "misuse," is usually less harsh than for crimes involving artifice, schemes to defraud fraudulent pretenses, or misrepresentation. See, e.g., Ariz. Rev. Stat. Ann. §13-2316C; Del. Stat. Ann §858(b); Ga. Code Ann. §16-9-93(b).

257. See Mo. Rev. Stat. §569.099.2.

258. See Ga. Code Ann. §16-9-93(b).

259. See Ga. Code Ann. §16-9-93(a). The penalty for this Section is one and one-half times the amount of the fraud, or imprisonment for not more than 15 years or both. See also Minn. Stat. Ann. §§609.87 to 609.89 (the penalty is based on the "loss to the owner"); Mont. Rev. Codes Ann. §45-6-311(2), is based on the value of the property lost or

misused; N.M. Stat. Ann. §30-16A-4 and Utah Code Ann. §76-6-703 gauges the amount of recovery to the vlaue of the computer system. The recovery may bear no relation to the harm to the data subject, however.

260. Cable operators must obtain franchises from local governmental authorities before they can operate. Subscriber privacy protection may be a condition to the grant of a franchise.

261. "Will CATV Become a Super Snooper?" Cablelines, July 1974, at 11.

262. A local ordinance mandates a separate penalty for violations of subscribers' privacy rights. Remarks of Richard Berman, General Counsel, Warner Amex Cable Communications, New York University School of Law Conference on Television and the Law, 1981.

263. See Standard Franchise Agreement, available from Massachusetts Attorney General's office, Cable Television Division, §31, at 26-27. See also The Boston Cablevision Franchise Agreement in Ferris, Lloyd & Casey, supra note 193, at Appendix C., State Forms, at C-377.

This agreement contains more comprehensive cable subscriber privacy protections than the Massachusetts Standard Agreement.

264.See Westin, Datamation, supra note 2, at 106.

265. See the New York Cable Telecommunications Act, A.7327--A, 1983-1984 Reg. Sess., Cal. No. 439 (1983) §833-b.

266. See A. Breznick, "N.Y. Association Sets Priorities," Multichannel News, March 5, 1984, at 37. New York Attorney General Robert Abrams has countered this claim in New York, stating that the proposed bill covers all home information and telecommunications systems. Moreover, he argued, the legislation should not be rejected "simply because it does not solve every privacy problem immediately, or because other legislation is needed to insure that privacy abuses do not occur elsewhere." Breznick, supra note 3, at 33.

Cable television may be receiving more attention from regulators than other industries do because it is newer than other industries. But other industries are also regulated where danger to consumers has been perceived. For example, telephones are regulated utilities subject to the Communications Act of 1934 and FCC regulations. Banks are regulated by the Bank Secrecy Act and the Financial Right to Privacy Act, see text accompanying notes 161 to 170, supra. Banks also owe their customers a common law duty of confidentiality, see Peterson v. Idaho First National Bank, 83 Idaho 578, 367 F.2d 284(1961) (bank-customer relationship subject to the rules of agency law which imply a duty of the bank not to use or communicate confidential customer information, and a contractual duty to refrain from disclosure unless authorized by law): 367 F.2d, at 290. See also Brex v. Smith, 104 N.J. Sq. 386, 146A.34 (1929) ("there is an implied obligation . . . to keep [depositors' bank records] from scrutiny until compelled by a court of competent jurisdiction to do otherwise"): 146A 34, at 36.

At least nine states have also enacted explicit statutory obligations requiring prior notice to customers if bank records are disclosed without customer authorization, and imposing a duty of confidentiality on banks. See Alaska Stat. §06.05.175 (1978); Cal. Banking Code §7470 (West 1976); Conn. Gen. Stat. § 36-9j to 36-9n; Ill. Rev. Stat. Ch. 17, § 360 (1980); La. Rev. Stat. Ann Art.9 § 3571 (West 1980); Me. Rev. Stat. tit. 9-b § 163 (1977); Md. Fin. Inst. Code Ann. § 1-301 (1980); N.H. Rev. Stat Ann. 359-C (1977); Okla. Stat. Ann tit. 6 § 2201 (West 1979).

267. See Ferris, Lloyd, & Casey, supra note 193, at §§14.06-14.07. If cable operators were subject to common carrier restrictions they could be required to file applications with state commissions to be allowed to enter a market, and to file for approval of their rates and tariffs. Cable operators might also be required to use uniform systems of accounts for bookeeping, or to provide non-video services through a separate subsidiary.

268. See Westin, Datamation, supra note 2, at 106.

269. Remarks of New York Attorney General Robert Abrams to the New York State Commission on Cable Television in 1982, cited in Id., at 111. Negative publicity may be particularly damaging to the future of two-way cable because cable operators are being hurt by higher-than-expected materials and installation costs, and competitors providing similar services for lower prices. See §[4] herein.

270. See Breznick, supra note 3, at 33. New York Attorney General Robert Abrams argues that "cable privacy is a problem which can be expected to arise," however. Id.

271. Koenig, supra note 4, at 113.

272. See Warner Amex Cable Communications, Code of Privacy (1981) reproduced at Appendix A; Cox Cable Communications, Inc. Code of Subcriber Privacy (1982); New York State Cable Association, Code of Privacy cited in Westin, Datamation, supra note 2, at 104. A committee was named by the National Cable Television Association to consider drafting an industry-wide privacy code. See R. Wiley & R. Neustadt, "S.66 Privacy Issues: Collection, Interception are Areas Addressed," Cable TV Law & Finance, March 1983, at 1. No further action has been taken on this matter, however. Telephone interview with James McElveen, Director of Public Affairs, National Cable Television Assoication (April 9, 1984). Storer Cable Communications also reported that it has a Privacy Code. Telephone interview with Pedro Policio, Coordinator of Research and Planning, Storer Cable Communications, Inc. (March 22, 1982).

273. See Westin, Datamation, supra note 2, at 104.

274. Introduction to Warner Amex Cable Communications Code of Privacy (1981).

275. Warner Amex's Chairmain in 1978 stated, "people who buy interactive service will have to accept that they give up a bit of their privacy for it. Beyond that, we'll try to protect their privacy all we can." The New York Times, August 8, 1978, SC, at 1.

276. Westin, Datamation, supra note 2, at 104.

277. Warner Amex is a wholly-owned subsidiary of American Express Company.

278. Westin, Datamation, supra note 2, at 104. See also Comments of New York Attorney General Robert Abrams cited in Breznick, supra note 3, at 33. Cox Cable Communications, Inc. has adopted a Code of Subscriber Privacy that provides that personal information about an individual subscriber not otherwise generally available will not be disseminated to any third party except 1) with the consent of the subscriber, 2) under court order, or 3) as required incidental to an audit. The Cox Code further provides that Cox will use its best efforts to prevent unwarranted disclosure of subscriber information, that subscribers may review their files for accuracy, and that the Code is subject to all applicable laws of the local franchising authority, the state, and federal governments.

The Cox Code does not address the issues raised in the discussion of the Warner Amex Code above, nor does it prohibit subscriber privacy violations such as aggregation and interception of data, or intrusion into subscribers' terminals using electronic monitoring devices. The Cox Code does not provide for prior notice to subscribers in the event of a court order or subpoena for a subscriber's records, and does not require Cox to maintain physical safeguards to protect subscriber data.

279. Cable Communications Policy Act of 1984, 98th Cong. 2nd Sess., P.L. 98-549 (1984).

280. Community Antenna TV Association (CATA) said it was officially reconsidering "advisability" of continuing to support the proposed bill in July 1984. See "Cable at Deregulatory Crossroads," Communications Daily, July 5, 1984, at 1-2. California Cable Television Association (CCTA), the most powerful cable television association, also determined the bill was "not in the interests of the cable TV industry or the general public," and voted to withdraw its support for the proposed bill. See "Cal. Cable TV Ass. Rejects HR-4103," Communications Daily, July 6, 1984, at 1.

281. The FCC recently affirmed its Community Cable Las Vegas decision preempting local rate regulation of all tiers except basic service, which it said can contain only must-carries, and deciding that an operator is free to add, delete or move around other signals. In re Community Cable TV, FCC No. 83-525 slip op. (Nov. 15, 1983). See "Disturbed By 'Timing,' FCC Affirms Cities Can Regulate Only Basic Cable Rates," Communications Daily, July 13, 1984, at 1. The FCC ruled in its Miami franchise ruling that total fees paid to cities cannot exceed 5%, that all money must be used to defray regulatory costs, and that payments for support by access must be for services available to all

users. See Memorandum Opin. & Order, Daily Digest, In re City of Miami, Florida June 29, 1984, at 84,737.

282. Capital Cities Cable, Inc. v. Crisp, Director, Oklahoma Alcoholic Beverage Control Board, No. 82-1795 (U.S. June 18, 1984).

283. See Capital Cities Cable, Inc. v. Crisp, Director, Oklahoma Alcoholic Beverage Control Board, No. 82-1795 (U.S. June 18, 1984), at 12, 21 to 22, 23.

284. See "Cable at Deregulatory Crossroads," Communications Daily, July 5, 1984, at 1.

285. Cable Franchise Policy and Communications Act of 1984, 98th Cong., 2nd Sess., Report 98-934 (1984), Part IV, §631(a)-631(h).

286. Id., at §634(a).

287. See Federal Computer Systems Protection Act, (FCSPA) S. 240, 96th Cong. 2d Sess. (1980); H.R. 6192, 96th Cong. 1st Sess, 125 Cong. Rec. H. 12352 (daily ed. Dec. 19, 1979). See Couch, supra note 230.

The FCSPA would have prohibited the use or attempted use of a computer, either as an instrument or a symbol, for any fraudulent purpose. S.240, 96th Cong., 2nd Sess. §3(a)(1980). The FCSPA would have also prohibited the unauthorized intentional damaging of a computer. Id., at §3(b). The bill's prohibitions applied to any computer used by the federal government, Id., at §3(a)(1)(A), or any financial institution, Id., at §3(a)(1)(B), and to all computers which affect interstate commerce, Id., at §3(a)(2). The authors of the FCSPA intended the term "operates in interstate commerce" to have an expansive meaning. 1978 Hearings on S. 1766 Before the Subcomm. on Criminal Law and Procedures of the Judiciary, 95th cong., 2nd Sess. 4 cited in Couch, supra note 230, at n.62, 1179.

288. 17 U.S.C. §102(b) (1976).

289. 35 U.S.C. §101 (1952).

290. See 18 U.S.C. §1341 (1949); 18 U.S.C. §1343 (1956).

291. Cable Franchise Policy and Communications Act, 98th Cong., 2nd Sess., Report 98-934 (1984) Part IV.

292. The Omnibus Crime Control and Safe Streets Act of 1968, Title III, 18 U.S.C. §2510-20.

293. Title VI §605, 47 U.S.C. §605 (amended 1968 and 1982).

294. E.g., Title III applies only to "common carrier." The Communications Act applies to radio transmissions.

295. See 47 U.S.C. §605.

296. See 18 U.S.C. §2510 (4).

297. Further discussion of the policy headings in this paper may be found in D. Marchand, "Privacy, Confidentiality and Computers: National Implications of U.S. Information Policy," 3 Telecommunications Policy 192, 197 (September 1979) [hereafter cited as Marchand]. Donald A. Marchand was Associate Director of the Bureau of Governmental Research and Service and Assistant Professor of Government and International Studies at the University of South Carolina, Columbia, at the time this article was published in 1979.

298. See P.P.S.C., Info. Society, supra note 2, at 15.

299. The Internal Revenue Code is a good example of this. The specificity of the Code is a map for taxpayers to avoid its provisions.

300. See Wicklein, supra note 2, at 208.

301. Federalism originated in the "Lockner Era." See Lockner v. New York, 198 U.S. 45 (1905). (Court struck down statute regulating hours of work as unnecessary infringement of contract. "Economic liberty" was the justification for suppressing government-imposed legislation that would have protected individuals from working under dangerous conditions.)

302. See, e.g. Ferris, Lloyd, & Casey, supra note 193, at ch. 14 for a discussion and the history of the struggle among the cable industry, its competitors, and municipal, state, and federal officials for jurisdiction to regulate cable television.

303. See M. Epperson, Legal Aspects of the Information Order: A Forecast, 13 (May 23, 1980) (unpublished research report). Epperson discusses datahavens in the international context, but his observations could have application to domestic privacy policy as well.

304. See generally Privacy Protection Law in the United States, N.T.I.A. Report Series, Report 82-78, May, 1982, at App. I.

305. See Marchand, supra note 297, at 199.

306. The cable industry is, in fact, so opposed to externally imposed regulations that during a meeting in February 1983, the National Satellite Cable Association adopted what amounts to a bill of rights for the private cable industry or satellite master antenna television industry. This bill of rights, which was presented to the Senate Communications Subcommittee, demands: 1) the right to exist and compete; 2) the right to be free from unwarranted state and municipal regulation; 3) the right to deal with real estate owners without government interference; 4) the right to equal access to the microwave spectrum; 5) the right of access to diverse program services. See "Bill of Rights," Broadcasting, February 21, 1983, at 10.

307. Communications Act of 1934, c.652, Title IV §605, 47 U.S.C. §605 (amended 1968 and 1982).

308. The Omnibus Crime Control and Safe Streets Act, Title III, 18 U.S.C. §§2510-20 (1968).

309. See Couch, supra note 230, at 1180.

310. Id.

311. See Nash & Smith supra note 2, at 67 to 71 for a description of Prestel.

312. See Wicklein, supra note 2, at 163.

313. According to a study concluded in 1981, encryption kits have not become widespread because: 1) managers do not believe the high cost ($200 to $300 for one chip) is justifiable, and many kits also require auxiliary hardware and software development to become operational; 2) managers believe that perpetrators will seek the cheapest and easiest methods to access confidential data (it may be far easier to give $50 to a terminal operator than to tap a line); 3) encryption is complicated, and there is no proof that it solves data security problems; 4) there are different export restrictions on cryptographic products, and exporting a device requires a license from the Office of Munitions Control at the State Department. See J. Ferguson, Private Locks, Public Keys and State Secrets; New Problems in Guarding Information With Cryptography, Report, Program on Information Resources Policy, Harvard University, 37-39, (1981).

314. Pamphlets from corporations marketing computer security contain instructions to assemble "eavesdropping kits" with readily available computer parts from electronic supply stores for approximately $500. Id., at 12-13. Mini-computers can be purchased to monitor dial up communications lines. Also, groups have organized to launch massive attacks to crack the Federal Data Encryption Standard. Id., at 13.

315. Different encryption codes are derived for every communication transmitted over the Washington-Moscow "hot line." Id., at 1.

316. See Couch, supra note 230, at n.77, 1181.

317. Id.

318. The term "operator" includes videotex or database operators, and private business and organizations that use computer systems. Government computer operators are regulated by the Privacy Act, FOIA, and certain other regulations and security procedures that do not apply to computer systems in the private sector. See, e.g., 5 U.S.C. §552a(1974); 5 U.S.C. §552 (1976); 41 C.F.R. §§ 101-36.000 to 36.127 (regulations governing management of automatic data processing equipment used by the federal government).

319. See generally Couch, supra note 230, at 1181 to 1195.

320. See §VB(i) Physical Security Measures and accompanying notes, supra. No security system is foolproof and a determined thief may eventually break any security system. However, security systems will prevent most crimes. Documentation of all computer operations and controlling access to the computer system may provide a trail for audit or investigation if suspicious employee activities arise. See Couch, supra note 230, at n.86, 1182.

321. See Couch, supra note 313 for some of the reasons management may decide not to implement security codes.

322. See Couch, supra note 230, at n.86, 1183.

323. Id., at n.88, 1184.

324. Id., at n.90, 1184. It may be difficult to effectively adapt mandatory security measures to individual systems. Enforcement of such regulations would require the expenditure of significant resources by the federal or state governments.

325. Id., at 1184.

326. Id., at 1185.

327. Id., at 1187.

328. Id.

329. Personal computer owners and small businesses and partnerships that are not professionally audited would be less affected by the imposition of increased responsibility on auditors. Videotex subscribers and other commercial computer system users would be affected because operators and manufacturers are audited.

330. Accountants must follow standard auditing procedures promulgated by the American Institute of Certified Public Accountants (AICPA). The AICPA is a national professional society of certified public accountants.

AICPA Professional Standard AU §320.01 says the term "internal controls" refers to all the measures adopted within a business to safeguard assets, ensure accuracy and reliability of financial records, and encourage operational efficiency and adherence to prescribed procedures. Id., at §320.09.

331. Id., at §321.24.

332. Id., at §321.27.

333. Id., at §321.31.

334. Couch, supra note 230, at 1188.

335. Id.

336. Irregular accounting procedures and financial statements that do not conform with GAAP must be disclosed. See generally AICPA Professional Standards AU § 200 to 561. There may be substantial latitude in GAAP, however.

337. See Couch, supra note 230, at 1193.

338. Id., at 1192.

339. Id. The SEC has considered requiring all registered companies to file a certified report on the business' overall system of internal controls. See SEC Release No. 34-15772 (April 30, 1979) published in 17 SEC Docket 421 (May 15, 1979).

The SEC withdrew the proposed rule on June 6, 1980, because of the SEC's desire (and probably pressure from the accounting industry) to encourage the private sector to take voluntary steps toward examining internal controls and reporting weaknesses. The Commission said it would monitor voluntary efforts for three years, and might take regulatory action at that time. It recommended that companies that file with the SEC include audited reports on internal control with their other financial statements. See SEC Accounting Release No. 278, SEC Accounting Rules (CCH) 3282, 3802-03, 3817 cited in Couch, supra note 230, at 1190.

340. See, e.g., SEC Accounting Release No. 261, SEC Accounting Rules (CCH) 3265 (accounting changes for oil and gas producers).

341. According to one study, only one out of five detected computer crimes are reported. See Couch, supra note 230, at 1176. Much publicity has been generated about the computer break-in by the 414 group in Wisconsin and the break-in to ARPANET, however. See Computer Fraud, supra note 119, at 6.

APPENDIX A

WARNER AMEX CABLE COMMUNICATIONS

CODE OF PRIVACY

1. Warner Amex shall explain to its subscribers the information gathering functions of the cable communications services being provided.
2. Warner Amex shall maintain adequate safeguards to ensure the physical security and confidentiality of any subscriber information.
3. Warner Amex subscriber agreements shall include the following:
   A. Individual subscriber viewing or responses may be retained only where necessary to permit billing or to render a subscriber service. Any such information will be kept strictly confidential unless publication is an inherent part of the service (e.g., announcing a game show prizewinner).
   B. No other individualized information concerning viewing or responses will be developed unless the subscriber has been advised in advance and given adequate opportunity not to participate.
4. Warner Amex may develop bulk (non-individual) data concerning subscriber services for use in developing new services for improving existing services. Warner Amex will not make such bulk data available to third parties -- whether affiliated or nonaffiliated with Warner Amex -- without first ensuring that the

identity of individuals is not ascertainable from the data provided.

5. Warner Amex will refuse requests to make any individual subscriber information available to government agencies in the absence of legal compulsion, i.e., court order, subpoena. If requests for such information are made, Warner Amex will probptly notify the subscriber prior to responding if permitted to do so by law.

6. Subscribers may examine and copy any information developed by Warner Amex pertaining to them at Warner Amex premises upon reasonable notice and during regular business hours. Copying costs shall be borne by the subscriber. Warner Amex shall correct such records upon a reasonable showing by the subscriber that information contained therein is accurate.

7. Any individual subscriber information will be retained for only as long as is reasonably necessary, e.g., to verify billings.

8. Subscriber mailing lists shall not be made available to third parties -- whether affiliated or nonaffiliated with Warner Amex -- without first providing subscribers with the opportunity to have their names removed from such lists.

9. Warner Amex shall comply with applicable federal, state, and local laws respecting subscriber privacy and shall adhere to applicable industry codes of conduct which promote or enhance subscriber privacy.

10. Third parties who participate in providing services to Warner Amex subscribers shall be required to adhere to the Company's Code of Privacy and all Warner Amex arrangements regarding such services shall specifically incorporate this Code of Privacy by reference.

11. Warner Amex shall continously review and update its Code of Privacy to keep current with technological changes and new applications.

# APPENDIX B

## DEFINITIONS

As used in this paper,

1) "Access" is to approach, instruct, communicate with, store data in, retrieve data from, intercept from, or otherwise make use of any resources of a computer, computer system, or computer network.
2) "Aggregation" is the unauthorized collection of information that may or may not be individually significant or identifiable to create large banks of confidential information or "psychographic profiles" of individuals and/or households.
3) "Compression" is the compacting of information for retention and access into a micro-computer chip.
4) "Computer" is an electronic device or communications facility that performs logical, arithmetic, and memory functions, and includes all input, output, processing, and software connected or related to such devices and facilities.
5) "Computer software" is a series of instructions or statements, in human- or machine-readable form, that controls, directs, or otherwise influences the functioning of a computer, computer system, or computer network.
6) "Computer system" is a set of related, connected, or unconnected computer equipment; devices that employ standard data links, software, and computer terminals (rather than converted television sets). Services are provided by software programs that access different collections of data.

7) "Database" is any data, or other information compiled, classified, processed, transmitted, received, retrieved, originated, switched, stored, manifested, measured, detected, recorded, reproduced, handled, or utilized by a computer, computer system, computer network, or computer software.

8) "Hybrid system" is any interactive system that combines more than one form of interactive technology, including, but not limited to, components of interactive cable systems, videotex systems, and computer systems; radio, broadcast, and microwave transmissions; and any service qualifying as common carrier under 47 U.S.C. subchapter II.

9) "Interactive cable system" is a cable television system that transmits signals from a central operator to users' converted television sets and consoles and from users' sets back to a central operator via cable wire. Cable operators generally employ a computer (or a group of computers) to collect billing information, to poll subscribers for marketing information and general statistics, and to monitor system integrity.

10) "Hardware" is the physical components and all associated and related components of a computer system, videotex system, interactive cable system, or hybrid communications system.

11) "Interactive technology" is any interactive cable system, videotex system, computer, computer system, or hybrid system that transmits signals "downstream" from a central computer to a user's terminal or console, and "upstream" from a user's facility to a central processor or operator.

12) "Intrusion" is repeated or continuous monitoring or surveillance of a user's terminal for purposes other than billing or checking system integrity.

13) "Misuse of data" is use of data collected about an individual for reasons other than those authorized and understood by the subject. Misuse includes, but is not limited to, unauthorized transfer, disclosure, commercial sale, and failure to delete data that is or has become inaccurate.

14) "Network" is two or more computers or communications facilities that are interconnected.

15) "One way" information technology is computer, telephone, cable, or hybrid information communications systems that transmit information in only one direction from a center operator to a user's terminal.

16) "Piracy" is knowingly and willfully, directly or indirectly, without proper authorization, accessing, causing to be accessed, or attempting to access any computer, computer system, computer network, or communications facility for the purpose of obtaining money, property, or services for oneself or for another.

17) "Property" includes, but is not limited to, information, computer programs, and any proprietary, personal, or other information of value to the data subject; programs, data, services, and tangible and intangible items of value to a systems operator.

18) "Services" includes, but is not limited to, computer time, data programming, storage functions, banking, shopping, publications, broadcast and textual information, messages, programming, and monitoring provided by computers, videotex, interactive cable, or hybrid communications services.

19) "Videotex" is any interactive technology usually transmitting information and services over common carrier or cable line, which acts by retrieval of a specific information frame, selected and transmitted over a link such as a telephone wire. Sometimes the term videotex includes teletext, which is a system transmitting all available frames over a broadband channel, and subsequent selection, or frame-grabbing at the terminal. In contrast to typical computer systems, the display unit may be a conventional television set hooked up to a microprocessor-driven terminal adopter. Services available on videotex are transmitted to users by a central operator.