DOCUMENT RESUME

ED 225 264 EA 015 292

TITLE	Invited Papers on Privacy: Law, Ethics, and Technology.
INSTITUTION	American Bar Association, Washington, D.C.; American Federation of Information Processing Societies, Montvale, N.J.
SPONS AGENCY	National Endowment for the Humanities (NFAH), Washington, D.C.; National Science Foundation, Washington, D.C.
PUB DATE	82
GRANT	NSF-OSS-7924514
NOTE	35p.; Papers presented at the National Symposium on Personal Privacy and Information Technology (October 4-7, 1981). For related document, see EA 015 371.
PUB TYPE	Viewpoints (120) -- Speeches/Conference Papers (150)
EDRS PRICE	MF01/PC02 Plus Postage.
DESCRIPTORS	*Confidentiality; Data Collection; Disclosure; Ethics; Information Processing; *Information Services; Information Utilization; Laws; *Legal Problems; *Privacy; *Technology

ABSTRACT

These four papers were presented as background at a national symposium exploring the relationships among law, ethics, and technology as they relate to the individual's informational privacy. George B. Trubow's "The Development and Status of 'Informational Privacy' Law and Policy in the United States" discusses privacy as it relates to the collection, use, or disclosure of personal information. Trubow covers relevant common law and court decisions, fair informational practices, federal and state privacy laws, and eight questions about privacy that need resolution. Alfred R. Louch's "Morality and Privacy" ponders the philosophical, social, and moral bases of the concept of privacy. Fred W. Weingarten's "Information Technology and Privacy Trends in Products and Services" surveys likely developments in information technology over the next decade that will probably affect individual privacy. Weingarten identifies more than 14 trends in technological developments and in their effects at the individual level, at home, at work, and in broader social services. Finally, in "A Taxonomy for Privacy," Willis H. Ware proposes a framework within which to consider privacy litigation and legislation. Ware discusses the concepts of physical, visual, aural, and recordkeeping space and suggests defining "invasions" of these spaces rather than defining privacy itself. (Author/RW)

INVITED PAPERS ON PRIVACY: LAW, ETHICS, AND TECHNOLOGY

Presented at the National Symposium on Personal Privacy and Information Technology

Sponsored By

American Bar Association's
Section of Individual Rights and Responsibilities
Committee on Privacy

and

American Federation of Information Processing Societies
Special Committee on the Right to Privacy

INVITED PAPERS ON PRIVACY: LAW, ETHICS, AND TECHNOLOGY

Presented at the National Symposium on
Personal Privacy and Information Technology

October 4-7, 1981

Sponsored By

American Bar Association's
Section of Individual Rights and Responsibilities

Committee on Privacy

Elmer R. Oettinger, Chairman
Floyd Abrams
Martha W. Barnett
Barry Boyer
Charles W. Joiner
Mary Lawton

and

American Federation of Information Processing Societies

Special Committee on the Right to Privacy

Lance J. Hoffman, Chairman
Gordon C. Everest, Vice Chairman
Paul Armer
Robert Belair
Robert Bigelow
Robert Blanc
Robert P. Campbell
Robert C. Goldstein
Pender McCarter
William Moser
William Perry
Robert Smith
Rein Turn
Fred W. Weingarten

Support for the Symposium was provided by the National Science Foundation and the National Endowment for the Humanities, NSF Grant Number OSS-7924514. Any opinions, findings, conclusions or recommendations expressed herein are those of the authors and do not necessarily reflect the views of the National Science Foundation or the National Endowment for the Humanities.

This paper has not been approved by the House of Delegates or the Board of Governors and, until approved, does not constitute the policy of the American Bar Association.

Library of Congress Catalog Card No. 82-063661
Section of Individual Rights and Responsibilities
Invited Papers on Privacy: Law, Ethics and Technology
Washington, D.C.

TABLE OF CONTENTS

Page

Preface i

The Development and Status of "Informational Privacy" Law and Policy in the United States
GEORGE B. TRUBOW 1

Morality and Privacy
ALFRED R. LOUCH 10

Information Technology and Privacy Trends in Products and Services
FRED W. WEINGARTEN 15

A Taxonomy for Privacy
WILLIS H. WARE 27

PREFACE

The papers published here were prepared to provide the background for discussions at a National Symposium on Personal Privacy and Information Technology held in the Fall of 1981. Sponsored jointly by the American Bar Association's Section of Individual Rights and Responsibilities and the American Federation of Information Processing Societies, the Symposium was made possible by a grant from the National Science Foundation and the National Endowment for the Humanities.

The purpose of the Symposium was to explore the relationships between law, ethics and technology as relevant to the informational privacy of the individual. The report of that Symposium, published separately by the American Bar Association, presents the findings and recommendations distilled from three days of discussions among the 24 experts gathered for the Symposium.

The background papers are published separately as general resources on law and policy with respect to informational privacy, the relevance of morals and ethics to concepts of privacy, and the effects on privacy that may result from the rapid growth of computers and information technology. A word about the authors may be helpful.

George B. Trubow has been professor of law at the John Marshall Law School, Chicago, since 1976. He holds A.B. and J.D. degrees from the University of Michigan. During the administration of Gerald Ford, Professor Trubow was general counsel to the Committee on the Right to Privacy, Executive Office of the President, and prior thereto he was deputy counsel to a subcommittee of the U.S. Senate Judiciary Committee, and director of planning for the Law Enforcement Assistance Administration, U.S. Department of Justice. Professor Trubow was co-director of the Symposium for which the papers were prepared, and he has directed other projects on privacy for the American Bar Association.

Alfred R. Louch is professor of philosophy and chairman of the Philosophy Department at Claremont Graduate School. He was educated at the University of California, Berkeley, B.A. (1949), M.A. (1951) and Cambridge University, Ph.D. (1956), where he held a Rhondda Open Research Studentship at Gonville and Caius College. He has also taught at the Berkeley, Los Angeles and Riverside campuses of the University of California, Oberlin College and Syracuse University. Professor Louch is the author of Explanation and Human Action and is completing a further book, Power and Right. He has published numerous articles and reviews in the philosophy of behavioral sciences, action theory, and moral and legal philosophy. He serves on the editorial board of *Social Theory and Practice*, *Philosophical Investigations*, and *Humanities and Society*. Professor Louch recently completed a four-year term on the California Council for the Humanities in Public Policy and has served on committees to set up Law and Society and Legal Studies programs at the University of California, Riverside and at the Claremont Colleges. In the Summer of 1981, he taught a National Endowment for the Humanities seminar on the right to privacy to college teachers. In addition to teaching in the education, business and criminal justice departments, he currently directs a Dual Degree Program in humanities and management.

Fred W. Weingarten, then with Information Policy, Inc., was a consultant in privacy, computer security, and information policy. He received a M.S. degree in applied mathematics and a Ph.D. degree in mathematics and computer science from Oregon State University. Dr. Weingarten spent seven years at the National Science Foundation developing and managing a program to support research on computers and public policy. He also served with the staff of the Privacy Protection Study Commission, represented NSF on the State Department Task Force on Transborder Data Flow, and consulted for the Committee on the Right to Privacy (Executive Office of the President-Domestic Council). Dr. Weingarten is currently Program Manager, Communication and Information Technology for the Office of Technology Assessment of the U.S. Congress.

Formally educated in engineering, Willis H. Ware has long been concerned with the impact of computers and information technology upon society, and as early as the mid-1960s had begun writing and discussing his views on computers as a growing social force. He thus combines the sensitivities of a social scientist with the nuts-and-bolts knowledge of a technician. With the Rand Corporation since 1952, Dr. Ware has progressively been a member of the research staff, head of the Computer Sciences Department, deputy vice-president for Project RAND (U.S.A.F.) and is currently with the Corporate Research Staff. His areas of expertise include military information systems, technical assessment of Soviet computing technology, and nearly 30 years of interaction with the U.S. Air Force, the Department of Defense, and other federal agencies. Dr. Ware was vice-chairman of the Privacy Protection Study Commission.

George B. Trubow
Principal Investigator

The Development and Status of "Information Privacy" Law and Policy in the United States

by George B. Trubow*

Introduction

Privacy is a notion that has attracted considerable attention in this country during the past fifteen years;[1] the word has been used broadly to characterize claims involving matters such as the use of contraceptives,[2] the choice for abortion,[3] freedom from telephone wiretaps[4] and the confidentiality of financial records kept by banks.[5] Such broad references to "privacy" obscure the nature of the interest and contribute to difficulty in defining it. Almost everyone talks about "privacy" but no one seems to know exactly what it is. The principal purpose of this paper is to discuss the development and status of privacy mainly as it relates to the collection, use or disclosure of personal information, an aspect of privacy especially important to what has been characterized as the modern "information society."[6]

Much of the recent concern about privacy has resulted from the phenomenal growth of computer use, which has made it possible to collect, manipulate and disseminate personal information in dimensions never before contemplated.[7] People are worried about who has information about them, how it was obtained and to what uses it will be put. A national survey conducted by Louis Harris and Associates for the Sentry Insurance Company has been frequently cited as indicating the degree to which Americans are concerned about privacy and the growth of information technology.[8] The survey reported that 54% of all Americans consider the present use of computers to be an actual threat to personal privacy, and indeed 53% of those surveyed in the computer industry agreed.[9] "If privacy is to be preserved, the use of computers must be sharply restricted in the future," was the opinion of 63% of the survey sample, and 75% said that a right of privacy should be of equivalent stature to the inalienable American rights of life, liberty and the pursuit of happiness.[10] Arthur Miller warned of "The Assault on Privacy" in 1964, and the public is increasingly aware of the vast quantities of personal information gathered and shared by federal, state and local government, as well as the private sector. The Watergate scandal served to accentuate fears about the federal government, though personal information held by any entity can constitute a privacy threat. Almost every person who has a mailing address is the recipient of "personal" letters from unknown or surprising sources. Though there seems to be significant public consensus that "privacy" is important and in jeopardy, there is no general agreement as to what the reasonable expectations of informational privacy ought to be.

*George B. Trubow is Professor of Law at the John Marshall Law School, Chicago, Illinois.

To provide clarity in the ensuing discussion, some words and phrases should be explained. Personal information is defined as any information that can be referred to a specific individual by name, number or other identifying characteristics. Consequently, it is not the content of information which makes it personal but rather its reference. The notion of "information privacy" can be divided into these components: (1) What personal information is collected; (2) The circumstances in which someone can see personal information; and (3) How the personal information is protected. The terms justification, classification and protection can be used to characterize these three components of "informational privacy."

Justification. All too often, personal information is collected or kept without careful evaluation as to what information is really *necessary* for the record's purpose. Information is not an end in itself, it is a resource used in making decisions. When information in a file is justified, the recordkeeper has been discriminate in choice and has determined that a particular piece of personal information is proper and necessary to the purposes and objectives of the file. If program objectives are specific and understood, information systems managers should be able to account for why and how each item of program information has been collected and kept.

Classification. Once information itself has been justified, those who may have access to that information should be identified and the circumstances for access described. Confidentiality is defined by classification which establishes disclosure protocol. Classification is a principal concern of information policy because the question of who can see personal information is frequently a central issue in privacy disputes.

Protection. This involves the avoidance of unauthorized alteration, disclosure or loss of information. Once information has been classified, the degree of protection afforded will depend upon the kind and degree of risk attendant upon unauthorized access to that information. The safeguarding of data is a matter of security technology and procedures and is not within the principal focus of this paper.

The ensuing discussion is organized as follows: it begins with a summary of the relevant common law of the United States regarding the status of privacy prior to 1964, including reference to the common law of defamation, which also deals with information about individuals. The effect on the relevant common law of Supreme Court cases in 1964 and thereafter describes the *constitutional* basis for privacy in the United States. Next will follow a discussion of information privacy as characterized by "fair information

practices" proposed in recent federal studies and a brief survey of current federal and state statutes that protect personal information. (Because the purpose of this paper is to map the general contours of informational privacy as recognized in this country, it does not present a detailed legal analysis.) The discussion will conclude with a list of issues that this writer believes must be resolved in the development of a comprehensive information privacy policy.

Relevant Common Law Prior To 1964

The Development of "Privacy"

A concept of privacy is not part of the English common law and was not specifically recognized in early American law. The idea of a legal "right to privacy" was presented in 1890 in a law review article by Samuel D. Warren and Louis D. Brandeis:

> "Political, social and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society ... Instantaneous photographs and newspaper enterprise have 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.' For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers ..."[11]

Warren and Brandeis argued that, though not specifically designating it as "privacy," courts had in fact recognized such an interest. The authors declared privacy to be "a part of the more general right to the immunity of the person, the right to one's personality."[12] They borrowed the phrase, "the right to be let alone," from Judge Cooley[13] and used it to characterize the nature of privacy. Unfortunately, that phrase has been used repeatedly to describe privacy, but it does not precisely define the concept. Being "let alone" can also describe the interest violated by such torts as assault, battery, false imprisonment and trespass to property, which were really the context for Cooley's use of the phrase. Warren and Brandeis did, however, undertake to define more narrowly the boundaries of privacy:[14]

- Privacy does not prohibit publication of matters considered to be of general public interest.
- The same privileges of publication as apply in defamation also apply to privacy.
- A right to privacy ceases when the individual himself consents to or causes the publication of personal information.
- Privacy can be violated even if the information published is true.

Within these constraints, the right to privacy was identified as protecting an individual against the unwarranted publication of his name or picture or of sensitive personal information.[15]

Professor William L. Prosser[16] and the Restatement of Torts[17] gave further impetus to the development of privacy. These authorities built upon the Warren and Brandeis analysis and defined four kinds of privacy which they said had been recognized in the common law:

Intrusion upon physical solitude or seclusion. This involves unreasonable intrusion into an area wherein one has a reasonable expectation of being undisturbed. Most of the cases recognizing this tort involve a physical entry by the intruder similar to property trespass, but eavesdropping, peeping into windows, repeated telephone calls and spying with binoculars or cameras have also been considered privacy intrusions. Though there have been a few instances in which unwarranted prying into personal information or affairs was considered intrusion, that has not been the generally recognized thrust of this specie of the tort.

Public disclosure of private facts. This tort prohibits unreasonable publicity given to private information in which the public has no legitimate interest and tracks very closely the kind of privacy summarized above with which Warren and Brandeis were concerned. This privacy interest could be invaded even if the information disclosed was true.

Publicity placing one in a false light in the public eye. The gravaman of this tort is an affront to personal dignity, but it is difficult to distinguish it from defamation (discussed below) which protects reputation. Also, unlike the prior tort, but as in defamation, this privacy interest is violated only by the publication of false information.

Appropriation of one's name or likeness for the commercial benefit of another. This also was a problem identified by Warren and Brandeis and is the first privacy tort formally recognized by common law in the United States. This interest is sometimes protected by statute, in which case it is usually restricted to appropriations for commercial gain (such as product advertisements), though the common law often included non-commercial benefits achieved through use of name or picture to assert or imply an endorsement (e.g., support for a political candidate).

The publication-of-private-fact tort has most relevance to the confidentiality of personal information; intrusion into seclusion may be relevant to how information is obtained and is an informational privacy tort only if prying into personal records is recognized as an "intrusion." The appropriation tort addresses unauthorized publicity, and is more related to property rights than to informational privacy. For all practical purposes, "false light" privacy is indistinguishable from defamation.

There is little uniformity among the states as to which of these four privacy torts is recognized and what limitations may apply to any one of them. Neither Prosser nor the Restatement has helped to clarify "privacy" by grouping these four disparate interests under the same rubric, and informational privacy as discussed in this paper is not adequately

addressed by "common law privacy" in the United States as described by Warren and Brandeis, Prosser or the Restatement. It is important to remember the two privacy torts that do relate to the *publication of information*—publication of private facts and false light publicity—because it is the *publication* aspect of the torts that invite the conflict with First Amendment protection of speech and the press, to be discussed later in this paper.

Common Law Defamation

The common law of defamation is relevant to informational privacy because defamation involves the publication of false information that injures reputation. Further, the line of Supreme Court cases beginning in 1964, which places limitations on common law defamation, is deemed to apply to privacy whenever publication of information is an element of the tort. At common law defamation is the publication of false facts that injure another's reputation by subjecting him to hatred, shame or ridicule in the community.[18] It was the falsity requirement that initially avoided conflict with the Constitution, because the Supreme Court held early on that the First Amendment protects truth, but not falsehood.[19]

Whether the defendant realized he was telling a lie about a specific person was beside the point; common law defamation often brought harsh results by assessing liability for a statement which had not been appreciated as defamatory and for which there was no reason to suspect falsity. In a famous English case, the defamation was about a fictional character created in a story written by the defendant, when lo and behold, a plaintiff with the same name as the fictional character appeared and sued (interestingly, plaintiff was a lawyer!); the defendant was held liable for the defamatory statement.[20] A similar result has been reached in the United States, where one court said, "The question is not so much who was aimed at as who was hit."[21]

To summarize the status in 1964, of what loosely might be called "informational privacy law," and remembering that there are considerable variations among the several states regarding recognition of and the elements for various torts, these generalizations are permissable:

1. There was liability in damages for publishing a defamatory falsehood, perhaps even if the publisher was innocently unaware that the information was false and defamed a specific person.

2. There could be liability for publishing information which, though not defamatory, placed the plaintiff in an objectionable false light in the public eye. (This privacy tort is difficult to distinguish from defamation and seems almost to have been swallowed by that tort.)

3. To publish embarrassing or sensitive private information in which the public had no legitimate interest was a violation of privacy even if the information was true.

"Informational Privacy" Law Subsequent to 1964

In 1964, the Supreme Court decided the landmark case of *New York Times v. Sullivan*,[22] in which a public official (Commissioner of State Police) allegedly had been defamed by falsehoods. The Supreme Court held that there could be no liability for defamatory falsehoods about a public official unless the defendant knew that the publication was false or displayed reckless disregard as to whether the publication was false. In subsequent cases, the Supreme Court extended the "deliberate or reckless falsity" requirement to public *figures*[23] as well as public *officials*, saying that such individuals voluntarily seek the limelight and are better able to protect themselves against defamatory falsehoods than are ordinary citizens. Whether or not one agrees with those reasons, the court does protect publishers from the self-censorship that can result from the strict liability imposed by common law defamation. The court made it clear in *Sullivan* that the Constitution protects falsehoods in some circumstances to encourage free and open debate and comment.

In 1974, the Supreme Court decided *Gertz v. Robert Welch, Inc.*,[24] wherein plaintiff lawyer had been defamed in a publication of the John Birch Society. The court held that the plaintiff was not a public figure nor public official and that, as an ordinary citizen, did not have to meet the "deliberate or reckless falsity" test required in *Sullivan*, but did have to prove that the defendant was at least *careless* with regard to the falsity of the publication. There is disagreement as to whether *Gertz* applies only when the defamation defendant is of the news media; the opinion is unclear on this point and the states are divided on the issue.[25] Though the *Sullivan* and *Gertz* cases address defamation, it is considered that they also control privacy when publication is an element of the tort. Two Supreme Court cases dealing specifically with privacy are worth noting in this respect:

In *Cantrell v. Forest City Publishing Co.*,[26] the court reviewed a "false light" privacy invasion, wherein the parties to the case accepted the *Sullivan* test as applicable. The Supreme Court said, referring to *Gertz*, that the question remained open whether a less rigorous standard than *Sullivan* would apply to false light cases, suggesting that privacy will be controlled by cases limiting defamation.

Cox Broadcasting Corp. v. Cohn,[27] introduces perplexing privacy problems. That case involved the publication of private fact in Georgia, where the defendant had published the name of a rape victim, contrary to a state statute specifically prohibiting the publication of such information. The court ruled that because the name of the rape victim had been found by the defendant on the criminal indictment, a public document made available during the trial, publication of that information constitutionally could not be proscribed. Though the narrow holding of the court was that "states may not impose sanctions for the publication of truthful information contained in official

court records open to public inspection," the court did state that "the interests in privacy fade when the information involved already appears on the public record."[28] Though an indictment was the specific "public record" before the Court, the case opens the question whether, constitutionally, informational privacy rights cease once personal information has become available to the public. In some instances at common law, information probably not actionable when published because it was newsworthy and of general public interest at the time, was held actionable when dredged up again 10 or 20 years later.[29] It is not clear whether those cases of necessity are now in conflict with *Cox*. Additionally, the majority opinion in *Cox* specifically mentioned the matter of truth as a defense to the tort action and declared that question open. Clearly, if the First Amendment is interpreted as protecting all truthful information, then this common law tort of publication of private fact will be effectively eliminated. For informational privacy to survive, the Supreme Court must decide that in some instances the publication of truthful information can be penalized.

In summary, and with the same caveat previously applied to such generalizations, subsequent to 1964:

1. There is no longer strict liability, to news media at least, for defamatory falsehoods. For liability, there must be at least carelessness as to truth and perhaps deliberate or reckless falsity, depending on who is the defamation plaintiff.

2. Information gleaned from official public records cannot be the basis of privacy actions. It is not clear now whether information from unofficial sources available to the public is also constitutionally protected, or whether information once on the public record is forever after in the public domain.

3. The Supreme Court has not decided whether all truthful information can be published, regardless of source, content or utility. The survival of informational privacy depends upon the enforceable confidentiality of certain truthful information.

Constitutional Basis for Informational Privacy

The foregoing discussion addresses common law privacy, as limited by First Amendment constraints. The Constitution of the United States has itself been the source for privacy rights, apart from the common law, in instances involving abortion, the use of contraceptives, wiretaps and the reading of pornography.[30] Rights of "personal autonomy" in certain decisions, and freedom from government interference, have been the focus of these privacy claims; accordingly, they are not on point as to informational privacy.[31] The Supreme Court has been asked to expand constitutional privacy broadly into information policy areas and thus far has refused.

In the case of *Paul v. Davis*,[32] the defendant, a local police chief, had circulated to town merchants a bulletin which carried the pictures and names of individuals identified as "active shoplifters." The plaintiff's picture was in the bulletin; he had been arrested on suspicion of shoplifting but the charge had been dropped and he was never prosecuted for the offense. The plaintiff brought an action alleging violation of a constitutional right of privacy. The Supreme Court noted that "constitutional privacy" thus far had recognized rights "fundamental to the concept of ordered liberty," said the case at bar was not within those "zones," and refused to extend the concept of privacy to this particular matter wherein a police chief was performing a function related to his official duties.[33] The plaintiff was left to rely upon state laws of defamation or privacy for redress.

The precise thrust of this case regarding privacy thus far has not been refined or clarified. Some commentators argue that *Paul v. Davis* is a barrier to constitutional protection of a right of informational privacy; others interpret the case narrowly as dealing with procedural due process and suggest that avenues remain open for constitutional privacy development. Because privacy is nowhere specifically mentioned in the Constitution, and because of the specific protection of speech and press in the First Amendment, it is probably safe to venture that in the foreseeable future Congress or the states must be looked to for development and protection of informational privacy.

Privacy and Fair Information Practices

Information policy has received attention in forums other than the judicial system. A government report in the early 1970s often has been cited as the first major contribution to the development of a rational policy framework for the collection, management and use of personal information. That report, "Records, Computers and the Rights of Citizens," was issued in 1973 by a Special Advisory Committee to the Secretary of Health, Education and Welfare and was the result of a comprehensive study of personal information kept in federal computerized data banks.[34] The report noted the significant growth of the use of computers to process information and proposed a set of "fair information practices" whose purpose was to enhance personal privacy by protecting the confidentiality of personal information. These principles may be distilled as follows:[35]

1. Collect only that personal information necessary for a lawful purpose.

2. Use for decision-making only data that is relevant, accurate, timely and complete.

3. Give the data subject access to information about himself, and a procedure by which to challenge and correct the information.

4. Use data only for the purpose for which it was collected.

5. Protect the data against unauthorized loss, alteration or disclosure.

Though often regarded as the foundation for personal information privacy, these are sensible rules for the management of any information system; their relevance to privacy policy will be considered shortly.

The Privacy Protection Study Commission, established by the Privacy Act of 1974,[36] (discussed below) also conducted a thorough and comprehensive study of public and private record systems and issued some 166 specific recommendations to enhance informational privacy. While acknowledging the soundness of the foregoing principles, the Commission identified three "objectives" of good information practice: (1) to minimize intrusiveness into the personal affairs of citizens; (2) to maximize fairness to individuals in the way personal information is managed, and (3) to legitimize expectations of the confidentiality of personal information.[37] It is probably more accurate to view these as suggested constraints on information practice, rather than objectives, because arguably the main objective of information is to provide a valid basis for decision-making. It does seem sensible that personal information should be collected and used in conformity with these constraints.

The Commission's constraints ("objectives") and the HEW principles are compatible and relate to the five components of information privacy:

- Principle #1 relates to justification—assuring that information is necessary to a legitimate purpose. The effect of this principle is to limit the amount of personal information collected, and privacy threats are diminished when the collection of personal information is restricted. The principle also responds to the avoidance of intrusiveness.

- Principle #2 is also a facet of justification. Decisions can be no better than the information upon which they are based. Stale or irrelevant information may be useless, and incorrect or incomplete data can be dangerous. This principle also promotes fairness by encouraging that decisions be based upon sound data.

- Principle #3 pertains to classification in that it addresses access by the data subject. The principle also promotes fairness since the data subject can learn what information is being used to make decisions that affect him. It also aids in justification regarding the accuracy and completeness of information because the data subject should be able to validate information pertaining to him.

- Principle #4 relates to classification by limiting use of and access to information and establishes expectations of confidentiality. It also promotes fairness by avoiding surprise, especially when data has been gathered from the subject or other source who disclosed it because of the specific purpose for which it originally requested.

- Principle #5 is clearly related to protection.

A difficulty in applying these information principles results from the shifting perspective of those dealing with information. The recordkeeper, the data subject and those who seek access to information about others each have differing viewpoints regarding justification and classification. It seems to be basic human nature that when one asks a question he wants to know everything that may be related to the inquiry, while one answering a question about himself prefers to supply as little personal information as possible. Each of the participants in the process of gathering and using information prefers to be the judge as to what is necessary to the purpose.

Because information is not an end in itself, the fashioning of principles or procedures for the management of information must necessarily take into account the specific objectives of a record system and the nature of the decisions which must be made. The variables regarding individuals, and information system objectives make it difficult to fashion a generally applicable information policy, which is why the Privacy Protection Study Commission found it necessary to make system-by-system recommendations. But, if there are no principles, then there can be no privacy. If principles are sufficiently clear, it will be much easier for the data subject, the recordkeeper and third parties to agree upon reasonable confidentiality expectations. Current policy formulation is insufficient to provide adequate guidance.

Federal Laws

Outside the reshaping of the common law resulting from application of Constitutional constraints, Congress has acted to regulate information by specific legislation. It must be remembered also that Executive Department regulations which have the force of law, may supplement statutes or implement enabling legislation. The capsule summaries that follow are sketchy, but they do set out the thrust of significant laws primarily concerned with the protection of personal information.

Fair Credit Reporting Act (1970).[38] This was the first federal legislation to regulate personal information maintained by the private sector. The FCRA requires that credit investigation and reporting organizations make their records available to the data subject, provide procedures for correcting information, and permit disclosure only to authorized customers.

Crime Control Act of 1973.[39] This legislation requires that state criminal justice information systems developed with federal funds be protected by measures to ensure the "privacy and security" of information. The Law Enforcement Assistance Administration was authorized to promulgate implementing regulations and did so in 1975. The regulations impose some restrictions on the dissemination of criminal history record information, though each state is expected to develop programs to manage and protect its criminal justice information.

Privacy Act of 1974.[40] This was the first comprehensive legislation to protect the confidentiality of personal information stored by federal agencies. The law provides access by data subjects, requires procedures for the correction or amendment of challenged information, and limits disclosure to third parties.

Family Education Rights and Privacy Act of 1974.[41] This Act, popularly referred to as the Buckley Amendment, requires schools and colleges to grant students (or their parents) access to student records, provide challenge and correction procedures, and sharply limit disclosure to third parties.

Tax Reform Act of 1976.[42] This law includes protection for the confidentiality of individual tax returns, limiting third party disclosure primarily to federal and state tax authorities.

Right to Financial Privacy Act of 1978.[43] This legislation provides bank customers with some privacy regarding their records held by banks and related institutions. This law was in response to the *Miller* case, wherein the Supreme Court held that account records maintained by a bank are not the client's papers, but rather are business records of the bank. Consequently, the records were not protected by the Fourth Amendment and the customer was not allowed even to challenge third-party access to such records. The Court said further that customers do not have an expectation of privacy regarding bank records. The RFPA creates an expectation of privacy by providing procedures whereby federal agents can gain access, though the law does not cover state or private sector third-party inquiries to banks.

Privacy Protection Act of 1980.[44] This was another Congressional response to a court decision, this time the *Stanford* case, wherein a search warrant was held to be a proper means for law enforcement agents to gain access to the files of a newspaper publisher. This 1980 law limits the procedures by which law enforcement authorities can see a newspaper's records or files.

Electronic Fund Transfer Act of 1980.[45] Pursuant to this law, any institution providing electronic fund transfers or other bank services must notify their customers about third-party access to customer accounts. EFTA does not provide specific privacy protections, however.

The 96th Congress had before it a variety of measures introduced by the Carter Administration that would have regulated medical, insurance and employment information. None of those proposals was enacted, and they have been reintroduced in the 97th Congress but have received little attention.

Note on the Freedom of Information Act of 1966.[46] The purpose of this Act is to make federal records available for public inspection and copying, on the theory that the government's business is everyone's business. There are a series of specific exemptions from the law's disclosure requirements, one of which is for disclosures that would be a clearly unwarranted invasion of privacy.[47] This exemption is designed to deal with cases in which a government record may pertain to an individual other than the one making the inquiry. It is frequently said that FOIA and privacy are in basic conflict, since the former seeks to open records to everyone, while the latter tends to close records except to the data subject. Though citizens desire free access to information about the way their government is doing business, arguably some government records deserve to be kept confidential in deference to the interests of the individual identified therein. Balancing the public "right to know" against an individual's desire for privacy is the tricky task facing federal agencies and courts when there is disagreement regarding the propriety of disclosure. Though, of course, there is a necessary relationship between information privacy policy and access to "public" records, discussion of the extensive FOIA litigation is beyond the scope of this paper.[48]

State Laws

State legislatures also have supplemented common law protection by providing a variety of specific information confidentiality guarantees.[49] Only a handful of states have enacted any one of the various privacy protections discussed below. Most states do have public records laws, their own brand of FOIA, and the same conflicts are encountered here as in the federal arena.

Criminal justice, medical and tax records receive attention by many states.[50] Almost every state has developed a plan consistent with the LEAA regulations for criminal histories, though they usually provide minimum confidentiality by restricting disclosure only of simple arrest records when there has been no disposition within a year following arrest.[51] Conviction records are usually not restricted, and it is common for data subjects to have rights to inspect and challenge recorded criminal history information. A majority of states provide confidentiality to medical and tax records, respecting the doctor/patient relationship and the financial privacy of the taxpayer.

Less than 20 states protect the confidentiality of bank records in parallel to the federal law, and a similar number have provisions to supplement FCRA protection.[52] Likewise, a handful of states protect the confidentiality of school records,[53] though the pervasiveness of the Buckley Amendment probably reduces the need for such legislation at the state level.

About 20 states have some sort of general privacy law, either in constitution or statute,[54] but on the whole such measures are narrow and relatively insignificant. Information privacy thus far has been a popular subject for state inquiry, though there is not much legislation to show for it.

The National Conference of Commissioners of Uniform State Laws, in 1980, approved the draft of a Uniform Information Practices Code.[55] That proposal includes both FOIA and privacy provisions, each modeled largely after the federal acts. The major benefits of the draft are that it makes FOIA and privacy more compatible in implementation, it avoids some of the problems experienced at the federal level,

and it provides a broad and comprehensive basis for managing information held by state and local government. The UFIPC draft does not seek to regulate information in the private sector, however.

Whatever may be the bounds of privacy defined by various federal and state case precedents, statutes or regulations, the notion does not have an intellectual foundation; what doctrine there is appears the result of emotion, value perception and whose ox is gored rather than because of any rational limits on disclosure of personal information based on reasonable and enforceable expectation. Even the generally accepted "principles" of fair information practice are subject to claims of exception and exclusion whenever applied to any particular information system. "Those rules are good for him but not for me . . ." is a frequent judgment rendered by an information system manager. Federal and state executives, legislatures and courts promulgate or declare more or less privacy, but they have produced a patchwork guilt and not a pattern fabric woven from the fiber of consistent and uniform interests.

Though the pursuit of a rational framework for informational privacy policy is itself a sufficient challenge and contains enough issues to command the attention of even the most astute analysts and theorists, there are specific questions of implementation regarding any policy that may be devised. It does appear, to this writer, at least, that society is not yet willing to accept an "open information" concept whereby there are no constraints on dissemination of accurate and sensitive personal information. Accordingly, even though the current concepts of informational privacy are nebulous and variant, some perplexing questions must be resolved to adequately monitor and protect whatever there is that already exists:

- Can and should information policy regulate the information practices of private individuals? The various principles which have been discussed were fashioned for government or regulated business, but not for that individual who may have a personal computer at home in his bedroom or den. The age of the microcomputer makes available to the general public relatively powerful information processing resources at small cost. Virtually anyone who can operate a typewriter can manage a personal computer, and for as little as $500. National data banks, accessible by personal computers, makes the question all the more pressing; the possibility of "data havens" maintained at home by an employee who would not be permitted to keep or use that information at his office presents additional problems for monitoring and regulation.

- What should be the criterion for triggering a privacy claim—tangible injury to the individual, or simply the outrage and emotional distress resulting when private information is wrongfully disclosed? Should privacy be protected in the Warren/Brandeis notion of "inviolate personality" or only in a property context when there has been commercial or pecuniary harm?

- Is privacy an aspect only of natural individuals (as is the current law) or do corporations have "privacy" too? Privacy in the personality sense is difficult to envision for corporations, though privacy as property is relevant to the protection of a business entity.

- If there is to be regulation, when is federal/state/self regulation appropriate or desirable? The private sector provided virtually no informational privacy until the federal government threatened, although the Privacy Protection Study Commission has urged that in most cases the private sector be left to its own measures of responsibility. There are some notable examples of corporate self-regulation, such as IBM and Aetna Insurance, but these are the exceptions and not the rule.

- What sort of regulatory agency, if any, should be established to monitor and protect the information interests of individuals and society? When the Privacy Act of 1974 was enacted, pressure from the White House discouraged the creation of a separate agency or bureaucracy to oversee implementation of the Act. Information is power, and who will watch the watchers? On the other hand, Congress was uncomfortable with a program that would depend upon voluntary agency compliance enforced only by private civil actions, so the Office of Management and Budget was given minimal oversight responsibility with little regulatory authority. (The UFIPC includes an optional information policy agency with not much power or authority.)

- How can press responsibility be assured? As in the time of Warren and Brandeis, the press is frequently accused and apparently guilty of excesses in the publication of personal information. Considering that anyone who can run a Xerox can disseminate news, it is not realistic to consider the press only in terms of the New York Times or the Washington Post. What about the National Enquirer? The electronic media pose the same problems, and size and general respectability of major networks is no guarantee. What about 20/20 or 60 Minutes?

- Consider the single identification number, a proposal with the unfortunate acronym of SIN. Everyone would have one identifying number, carefully assigned and always used; there are negative and positive factors. On the down side, such a number allows the easy linkage of information from any number of files and sources, and Orwell's Big Brother looms in the distance (1984 is just around the corner!). On the up side, however, is the convenience and accuracy of such a number; it can virtually eliminate information mixups and make it possible to quickly

sort and assign data. Are the threats of SIN real, or can technology render it a gentle giant that facilitates fair information practice?

- Should the needs of criminal investigation and law enforcement require a general exclusion from information confidentiality? Congress has considered several comprehensive criminal justice privacy bills during the past decade, but has not agreed on any proposal save the extremely general mandates of the 1973 Crime Control amendments, referred to above. Specific confidentiality enactments usually have broad exceptions for law enforcement purposes, as in the Privacy Act of 1974, and seem to contemplate a special law to deal with the pecularities of criminal justice. Because it is difficult to predict when an otherwise apparently routine or benign bit of personal information may assume critical importance in a criminal investigation, special exceptions to confidentiality may be appropriate.

It is not pretended that this list exhausts the issues attendant upon a rational information policy, but they are some of the more immediate and important. An information policy could be rational without resolution of those questions, but it would be difficult to regard the policy as comprehensive or adequate if many of these gaps remain.

Footnotes

1. A. MILLER, THE ASSAULT ON PRIVACY (1971); A. WESTIN & M. BAKER, DATABANKS IN A FREE SOCIETY (1972); J. SODEN. PRIVACY: RIGHT OR PRIVILEGE? (1977); J. RAINES. ATTACK ON PRIVACY (1974); U.S. DEPARTMENT OF HEALTH. EDUCATION AND WELFARE. RECORDS, COMPUTERS & THE RIGHTS OF CITIZENS (1973); MILLER. *The Dossier Society*, 1971 U. ILL. L.F. 154 (1971); and ERVIN. *Privacy and Government Investigations*, 1971 U. ILL. L.F. 137 (1971).
2. Griswold v. Connecticut, 381 U.S. 479 (1965).
3. Roe v. Wade, 410 U.S. 113 (1973).
4. Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975); Katz v. U.S., 389 U.S. 347 (1967).
5. California Bankers Association v. Schultz, 416 U.S. 21 (1974); Bisceglia v. United States, 420 U.S. 141 (1975); and United States v. Miller, 425 U.S. 435 (1976).
6. PERSONAL PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977).
7. *See* F. Weingarten, Information Technology & Privacy Trends (1981) (a paper written in connection with this symposium).
8. SENTRY INSURANCE, THE DIMENSIONS OF PRIVACY (1979).
9. *Id.*
10. *Id.*
11. Warren and Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1980).
12. *Id.*
13. COOLEY. TORTS (2nd Ed. 1888).
14. Warren and Brandeis, *supra* note 11, at 214-218.
15. *Id.*
16. PROSSER. LAW OF TORTS (4th Ed. 1971).
17. Restatement (Second) of Torts, §§652A-652I.
18. Kimmerle v. New York Evening Journal, 262 N.Y. 99, 186 N.E. 217 (1933); Belli v. Orlando Daily Newspapers, Inc., 389 F.2d 579 (5th Cir. 1967).
19. Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974).
20. Hulton & Co. v. Jones [1909] 2 K.B. 44; a [1910] A.C. 20.
21. Corrigan v. Bobbs-Merrill Co., 228 N.Y. 58, 126 N.E. 260 (1920).
22. New York Times v. Sullivan, 376 U.S. 254 (1964).
23. Curtis Publishing Company v. Butts, 388 U.S. 130 (1967).
24. Gertz, *supra* note 19.
25. Jacron Sales, Inc. v. Sindorf, 350 A.2d 688 (Md. 1976) (Gertz does not apply only to news media defendants.) Harley-Davidson v. Markley, 568 P.2d 1359 (1977); and Calero v. Del Chemical, 228 N.W.2d 737 (1977) (Gertz applies only to news media defendants. Note that the Oregon Court applied a standard of strict liability.)
26. Cantrell v. Forest City Publishing Co., 419 U.S. 245 (1974).
27. Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).
28. *Id.* at 494-495.
29. Melvin v. Reed, 112 Cal. App. 285, 297 P.91 (1973) *But see* Sidis v. F-H Publishing Corp. 113 F.2d 806 (2nd Cir. 1940).
30. *See* notes 2-5 *supra*.
31. Rights involving "personal autonomy" are sometimes referred to as the "volitional" branch of privacy law. An example of this type of privacy is expressed in Roe v. Wade, *supra* note 3, which involves the right to make personal decisions, such as the right to decide whether to bear children.
32. Paul v. Davis, 424 U.S. 693 (1976).
33. *Id.*
34. G.P.O. #1700-0016.
35. *Id.*
36. *See* note 6 *supra*.
37. *Id.*
38. 15 U.S.C. §1681.
39. 42 U.S.C. §3701..
40. 5 U.S.C. §552a.
41. 20 U.S.C. §123g.
42. 26 U.S.C. §1.
43. 12 U.S.C. §3401.
44. 42 U.S.C. §2000aa-§2000.
45. 15 U.S.C. §1693.
46. 5 U.S.C. §552.
47. Lawyers' Committee for Civil Rights Under Law, *Law and Disorder III: State and Federal Performance Under Title I of the Omnibus Crime Control and Safe Streets Act of 1968* in COMPUTERIZED CRIMINAL INFORMATION AND INTELLIGENCE SYSTEMS. (S. Carey, 1973).

48. *See, e.g.*, R. VAUGHN, A GUIDE TO PRACTICES AND PROCEDURES UNDER THE FEDERAL FREEDOM OF INFORMATION ACT (1981).

49. R. Smith, *Compilation of State and Federal Privacy Laws*, PRIVACY JOURNAL, AN INDEPENDENT MONTHLY ON PRIVACY IN A COMPUTER AGE (1981).

50. *Id.*

51. For analysis of State Criminal Justice privacy legislation, see COOPER & TRUBOW, TRENDS IN PRIVACY LEGISLATION (Search Group, Inc., Sacramento, California).

52. *Id.*

53. *Id.*

54. *Id.*

55. THE NATIONAL CONFERENCE OF COMMISSIONERS OF UNIFORM STATE LAWS, UNIFORM INFORMATION PRACTICES CODE (1980).

Morality and Privacy

by Alfred R. Louch*

Is privacy a moral concept? Perhaps the question is premature. We should ask first whether it is one concept or applies by a series of puns across a wide range of doubtfully related instances.

Think of the variety of cases where it is said to have been invaded: the peeping tom, the wire-tapper, the policeman's too energetic pursuit of incriminating evidence through rectal and vaginal searches, the extraction of blood, the recording of personal financial transactions. Think also of the various places, positions and relationships in which privacy is supposed to reside: the bedroom and bathroom, or any part of one's house, the telephone booth, the glove compartment or trunk, the concealment afforded by bushes on otherwise public ground, the bond and what is entailed by it between spouses or lovers, families or friends, professionals and clients.

Some of these cases focus on the alleged intrinsic wickedness of surveillance, some on the bad manners (at least) of those who disturb and annoy their neighbors. Others call to mind the need for seclusion to pursue certain legitimate, and indeed virtuous, projects. It would be tempting to say that all these cases share a common conception of the fact or condition of privacy: being unobserved by anyone who has not been explicitly invited to share one's company or activities. But, as lawyers and law-watchers have come to use the term, even that definition must be strengthened to justify not just the right to do certain things unobserved, but the right to do them at all.

The key here to the semantic confusion is the verb "to justify." Like other cases of contested meaning in the law (including the word "law" itself) the extension of the concept of privacy is entangled in the issue of its propriety. We aren't willing to say this or that area is private until we are assured that it ought to be. So we all know what privacy is—we know it when we're enjoying or suffering it, or looking for it, but we don't know whether Katz in his public telephone booth, or Griswold in his consulting room is in it in some justifiable sense.

I propose, therefore, to begin at the other end, and talk first about the justification of privacy, and allow its scope to emerge by inadvertence. But here I have two options, to tease out my, and I hope your, intuitions on privacy intrusion, or to formulate abstract moral theories, with a view toward testing their possible implications for the justification of privacy, and the charting of its domain. Right off, one might suppose there to be a match between one's rudimentary descriptions of privacy and the structure of the two substantive ethical theories still in circulation: utilitarian and Kantian. Whatever else, privacy is spoken of as something prized. One wants to be left alone, one craves solitude, and to discover that one has been spied on, or to hear broadcasted the details of one's personal life is a source of injury. So these wants and injuries go into the utilitarian balance. But, alas, so do other values that, as it happens, conflict with these acknowledged desires. Surveillance and data collection turn out to be necessary, or so it is believed, if one is to have security against assault, theft or fraud. A limitation on one's personal space is a condition of civilized life. So one must rank the competing values, not a problem to which utilitarians have found the solution. Their calculations depend on the commensurability of the values measured. But privacy's competitors—security, the right or the need to know—do not find a place above or below privacy on a single scale of desires. So we are reduced to consulting our intuitions in particular cases.

The Kantian view is at first more promising. It rests on a principle of respect for persons. I conform my conduct to this principle only if I treat others as ends, not as means. If I lie to others, I treat them as means; I manipulate them for my own ends. So, if the state (and likewise, the individual) engages in surreptitious surveillance, if it frustrates the life-plans of the heterodox by laws prohibiting contraception, abortion or drug addiction, if it collects data as a means of extending its control over citizens, it may be said to be violating the Kantian condition of morality. On this view, the concept of privacy is hard to distinguish from the concept of morality in general. Privacy is, as it were, the way of being treated morally. To respect persons is to respect their privacy. My claims to privacy is my request that you treat me with respect. This point of view, in its grand sweep, makes all but irresistable the ideal of an anarchic human condition, in which noble savages respect each other without the coercive goad of the state. Philosophers as different as Robert Paul Wolff and Robert Nozick find themselves in or near that state, as for them respect for persons means that no action against the will of another is morally permissable at all.[1] In consequence it is difficult to imagine how one can go to the doctor and preserve one's status as a moral being.

Kant was far from endorsing such a consequence of this theory. He assumed a state capable of enforcing moral duties. The instruments of enforcement will, by definition, violate the autonomy of individuals. So, he and all proper Kantians after him, must draw a line between permissable and impermissable intrusions on the person. The areas of impermissable intrusion may be called the area of privacy, but equally, the area of autonomy. Privateers, if I may call them so, will be disappointed at such a consequence. They want a particular area of immunity identified as private and justified accordingly. The mere facts of intrusion or the reduction of autonomy will not suffice, since they will allow cases in which observation or coercion serve legitimate and overriding social purposes. They may say that no sufficiently important aim is served by

*Alfred R. Louch is Professor of Philosophy at Claremont Graduate School, Claremont, California.

prohibiting contraception, that, setting aside the personhood of the fetus, no other legitimate aims favor the criminalization of abortion, but that, on the other hand, patrolmen may take blood samples from unconscious or protesting but palpably drunk persons, in the interest of highway safety, or that the police may bug a public telephone from which a bookie conducts his business. These judgments take into account the importance of preserving the social order, an aim that may be of greater significance to the individual than personal autonomy. So the area of privacy will have to be charted in the light of acknowledged utilities as well as out of respect for persons. Some of these utilities will be responsive to other needs and interests of individuals—for security, equal treatment, and the availability of goods. Others will relate indirectly to those aims, by endeavoring to secure the institutions necessary to protect them. With order, autonomy in Kant's sense is limited; without it, autonomy may be impossible altogether.

This means that we cannot expect moral theories to tell us what we want to know. They serve rather to remind us that in arriving at social decisions we acknowledge these formal constraints; we want at least to remember that we ought to respect persons but not so as to imperil the future, we ought to work toward maximum benefits, but without totally submerging individual dignity. And we shall be especially mindful of the sobering fact that by trying to respect persons we may be implicated in policies that in some way abrogate or invade autonomy or privacy. (The significance of this remark will appear at the end.) I am persuaded that this perspective on moral theory clouds the distinction between principle and policy that Dworkin has used to such effect in *Taking Rights Seriously*[2] and subsequent pieces. More to the point here, it suggests that the only available procedure in testing the moral force of claims to privacy is to consult our moral intuitions, informed to be sure by Kant and Mill, but not deduced from the claims to be found in their moral theories. I propose now to appraise the various types of privacy sketched earlier in just this way.

I begin with confidentiality because the primitive force in the promise to keep a secret is so obvious, and the strains on principle at the same time so palpable. At issue are the fundamental ideas of trust and betrayal, close to the heart of our moral intuitions and to Kantian ethics. Nonetheless, these forceful intuitions do not exclude counter-cases where, for example, keeping a promise endangers a life. In professional cases of confidentiality, it is argued that the useful function of the relationship with priest, therapist, doctor, attorney or newspaperman will be frustrated by divulgence. Setting aside the confessional which in our way of thinking has a different source of protection in the wall between church and state, this argument depends on the assumption that certain forms of counselling or investigation serve an important purpose in society. Counselors hear the uninhibited anxieties and aggressions of their clients, and so assist in venting them and possibly contributing to an understanding of them as well. Newspapermen are able to expose graft and corruption in high and powerful places only by using informants who would say nothing without the assurance of confidentiality. We recognize the moral obligation but may find in conflicting needs and interests reasons to divulge information as to a future crime, or to aid in the defense of a criminal suspect. Dworkin's easy answer to Farber,[3] that the use of informants is a matter of policy, the most efficient way of collecting information, is in fact not easy at all, unless one is quite sure the obligatory functions of the press are possible without the network of informants. This is a factual question to which I do not have the answer, but it is the answer that must be given before we weigh the rights of newsmen against those of criminal suspects. Morality turns on the nature of facts in most complex cases, even if the facts are not known. They may often be construed as moral problems because the facts are not known.

The therapist claims not to know when patients intend and when they only express violence. Their clients, they say, constantly talk aggressively, and were they obliged to warn in every such case, their words would have the effect of the boy who cried wolf, or, if believed, move the informed to counter-violence. Again, the facts are not clear, but their weight would contribute to the overall judgment of the legitimacy of breaking a confidence.

What is imparted in confidence has the character of a secret. Could we discover and chart the private by recounting secrets? What is divulged in confidential meetings will often be information about a person which otherwise would not be divulged at all. The special relationship encourages a sense of intimacy that matches, possibly goes beyond, that between husband and wife, parent and child, friend and friend. Thoughts, feelings, fantasies are revealed that, from shame to guilt, or other causes, patients cannot confront themselves. One may wonder why people are compelled to blab their secrets, but I assume we need not take the court's point of view in *Lovisi*[4] that revelations to someone else deprive the activity divulged information of its private status. We want to say of these confidentially communicated matters something which may be hard to say in law, that what they reveal to the therapist or priest are facts and feelings that constitute them as persons. It is their identities they choose to share for various extraordinary reasons. We come to one source of the private here, not because of the professional relation to the confidant, nor because of a promise given, but because what is said bares the soul. Love, jealousy, despair, grief—none are emotions that thrive in company. If others are present they must be there by invitation, as professionals or intimates. The TV cameraman and interviewer callously probing the bereaved's feelings about their lost loved ones are unwanted and unconscionable intruders.

Now this train of thought began with confidentiality as a special case of legitimate barriers to disclosure. But it ends with the conception of the personal,

or the intimate, a way of being or doing that cannot flourish in a fish bowl. But this idea, even if it can be made clear, does not cover the entire range of cases in which privacy has been advanced to block covert or coerced information gathering. The bookie taking and placing bets on his own or a public telephone, the war protester attending a political rally, the average person cashing and depositing checks are not in any of these activities revealing their emotional states or most intimate thoughts. They are doing business or making public statements and in the main with strangers. In all these cases there may be a good reason to shield the individual. We fear the exercise of police power and so wish to limit the extent and methods of surveillance. One, perhaps the only, feasible way of ensuring such limits, is to insist that searches be based on the reasonable suspicion that evidence will support specific allegations. A more extensive use of that power alters the relation between the state and the individual. Surveillance cannot be extended very far without subverting the moral ideal of a populace governed in the main by internalized conceptions of right and wrong, good and bad. Such a regime replaces moral motivation with fear and coercion. (Notice again the Kantian conception of the moral agent at work here.) I think it is at least plausible to argue, against the prevailing tendency, that unrestricted bugging, by which I mean the monitoring of all telephone calls over a period of a day or a week, moves too far in the direction of generalized search. The same could be said for FBI surveillance and picture taking of political rallies, or for the collection of all data on financial transactions. But one need not invoke a right to privacy to draw this conclusion. And it would be odd to do so, if our notion of intimacy is a guide to the use of the concept. Attending a political rally, for example, is public and is meant to be. We deplore its surveillance, not because it brings to light personal secrets, but because surveillance is the first stage in a plan to punish or suppress political convictions. It is the purpose of collecting and storing information that defines it as an invasion of personal rights.

I suggest we turn back to the vague conception of privacy emerging, or should I say emanating, from the account of confidentiality. What has emerged, or emanated, is the sense that a meaningful life depends on the capacity to enter into emotional relationships that exclude outsiders. And we may as well add at once that it depends too on the opportunity to derive the strength and self-confidence for the stresses of public life through retreat into solitude. But one is tempted to substitute for this compelling but vague idea some objective counterpart that could serve better as a legal criterion of the private zone. This is the temptation to resort to visible things and places: the body, the home, perhaps the office, the automobile, or its trunk, the locker, the bank vault. There at least we know *where* we are: the trouble is we don't always know with what right we are there. What I have in mind is best illustrated by the claim to the immunity of the body. Two models are particularly tempting here. The first is the privacy accorded to bodily functions—specifically sexual and eliminative functions. This cannot mean, however, that bodily functions as such are private. We do not take the same view, though some cultures may, of eating; we take a less private view of urinating than defecating, and so on. So it is not the body that is privileged, but the act. One would be hard put to explain why we taboo some acts and not others. But if we did not invest that kind of significance in some acts, our moral concept of respect for some persons might well be empty. It must be filtered through sensitivities of this sort to have any content at all. (Just as the concept of malice or crime needs the concept of harm or taint to find application.) The body itself, or parts of it, may be said to be tabooed. But again, the taboo, at least in our culture, does not turn on the conception of the body as personal, but because it, or parts of it (the private parts), signify acts whose public performance would be offensive, a breach in morality or manners.

The second model depends on the fact that intrusion on the body entails coercion. The police, believing that a suspect has swallowed the evidence, chokes him or forcibly administers an emetic.[5] Suspecting that a prostitute has secreted a razor in her vagina (private parts) they pry into body cavities. They extract a blood sample from an unconscious or a protesting automobile driver suspected of drunkenness.[6] Are these inadmissible invasions of the body's sanctuary? I think not. What offends us all in the *Rochin* case[7] is not the fact that the evidence was in his body, but that it required unconscionable and brutal procedures to get it out. Imagine that evidence could have been supplied by X-ray. The mere fact that the article is inside the body is not the limitation on such a search. Similarly, blood tests or body cavity searches fail to support the idea of the body as an inviolable place. The location of evidence in these cases, as in *Rochin*, improves the individual's chance of resisting disclosure or seizure. The body is, after all, the object most nearly under the control of the will. So body searches are more apt to occasion coercive methods of recovery. Blood under the fingernails, fingerprints, particles in the hair can be occasions for more direct confrontation of police and suspect than the body buried in the basement or the woods. We confuse that kind of confrontation and its implications for coercive and brutal search with the claim to bodily sanctity.

Much that is said of the body applies with diminishing impact to other enclosed spaces—the house, the car trunk or glove compartment, perhaps too the thicket in the woods.[8] They can be viewed as barricades that one can man, and so invite confrontation and its coercive consequences that threaten abuses of police power. Some of them can also be viewed as the settings necessary to perform bodily functions in a way consonant with public standards of decorum. All of them can serve as ways of shielding any activity from which we choose to exclude the public. Enclosed, shielded spaces are imposed on us as a duty—hence the very strong sense of a right to seclusion within them. They are also respected more broadly as the

means to nourish and enrich the interior life—hence the exacting requirements for police intrusion.

Do these observations point to a spatial—a topological—conception and a definition of privacy? If so, do they point toward ownership or title as a means of defining the zone? In spite of Brandeis,[9] earlier courts looked at it this way and failed to find it. I would agree. The physical shield may, after all, be a publicly provided sanctuary. It is not implausible to suppose that public telephones, at least of the old-fashioned kind no longer to be found in modern airports, are sanctuaries of just this sort. Private property is one way of making it possible to be private, but it is not the moral justification for privacy. In this respect it is like the body, which also, as a detached self-activating organism, affords another opportunity to be private. Our discussion would be moot if our minds were telepathically open to one another; and so it would be if we lacked opaque walls and blinds behind which to live and act out of the public gaze. If we believe that private places are necessary to our flourishing as moral persons, we may find artificial aids—walls, curtains, hedges—as necessary to this aim as our clothes or skins, or separate nervous systems.

I harp on this theme of bodily privacy to block at least one inference commonly drawn from it. This is the move from the metaphysics of the body (if I may put it so vaguely) to claims of property rights in it. It is, we say, my body, after all . . . presumably in response to being hectored for one's smoking, overeating, or dissipation. A particular instance of that line of thought has played a mischievous role in discussions of abortion. It has been urged that because the fetus is in the woman's body, and dependent upon it, the decision to abort is entirely hers, whether the fetus is a person or not.[10] This suggests a right of disposal which has nothing to do with privacy, and besides, may encounter rough weather conceived as a property right. There is nothing in the concept of ownership that overrides any possible public interest in the thing owned. If one abuses one's body, it is not implausible to say that one's care of it is not by any means unconnected with one's responsibilities to those who may have a legitimate interest in its healthful condition. So too in the abortion case. The whereabouts of the fetus do not decisively block the public interest. Whether other considerations work against public interest in the fetus is another matter. But the idea that the fetus *is* the mother's flows from a conception of motherhood as a responsibility and a major aim of her life. On that view it would be incoherent to appeal to the discomforts of pregnancy, and the loss of a preferred life-style as grounds for abortion.[11] For that way of talking alienates mother and fetus, opening the door to the public interest as much as it closes it. The property interest does not go through the body, but through a possibly atrophying sense of the intimacy of a relationship. But the way in which the fetus is the mother's entails a kind of personality to the fetus that, in the interest of liberalizing abortion laws, the courts and feminists have been at some pains to deny.

So the body and, along with it, the home are thus means of protecting something else, not the thing to be protected. If we then ask what it is we mean to protect as private, the answer that may satisfy our moral intuitions may trouble our legal scruples. We extoll intimacy, the kind of life than can only flourish given separate nervous systems, clothing, walls and hedges. We believe something essential to the quality of life is lost if we can't let down our guard, alone or among chosen intimates. That answer accords to the individual a central place in our scheme of values and duties. Self-identity and self-esteem depend, we believe, on an interior life as well as on public roles and achievements. There must be time apart as well as time together, tranquility as well as activity. Within this conception certain actions and relationships hold a prominent, if culturally contingent place, symbolized in physical terms by bedroom and bathroom, and the clothing of private parts. I say culturally contingent because we know that the shape of the private world alters under the pressure of relative senses of decorum, of prudery and modesty. Our standards of decorum are not only *ours*, they are in flux; that is why the concept of the private is so hard to specify. So one turns to half-baked theories of individuality and seeks at least partial sketches to the private realm by claiming that certain actions and relationships are essential to it. The sexual life is our leading candidate. It is both customarily private and, as Orwell noted in *1984*, the last bulwark of individuality against an omnipresent collectivity. This is the moral intuition that supports *Griswold* and *Eisenstract*. Prohibitions of contraceptives touch a couple in their most intimate moments.

This intuition, however, does not carry us very far. It affirms sexual privacy with such particularity that it affords little basis for analogy. It does, however, give rise to three concluding observations:

1. *Griswold* privacy needs to be looked at in the context of a mental health ethic, to which unimpeded sexuality is the core. Any obstacle to that end threatens the wholesome and valued relationships of married partners or lovers. This is why Douglas is able to carry forward his line of thought to *Doe v. Bolton*, where pregnancy and the unwanted child are seen as frustrating the life-style of the mother. Whether it is a good thing to sever act and consequence in this way is a deeper matter, but this is what a mental health ethic does. It strongly implies that unhappiness is always a sign of a redeemable mental or moral lapse.

2. The vague, disjointed area of privacy running from sexual intimacy at one end to simple tranquility—the right to be left alone—at the other is a bourgeois ideal. It depends on detached houses, surrounded by fence and hedge, separated from the neighbors. This is the natural setting for moral theories that rest on an individualist basis. It is not a condition, however, that could be said to be shared, even to a minimum degree, by the urban poor, even in societies like ours that affirm the virtues of privacy. It is also quite absent from the life of the Kalahari

Bushman or the Brazilian Indian,[12] for whom the concept of privacy as we use it is unintelligible. If the respect for privacy is a cultural and historical phenomena, the question naturally arises as to its future prospects. Is it an ideal that is possibly out of phase with the social realities of our time? It demands space where we lack space, individuality where we desperately require cooperation and sociability. Perhaps we have tried to articulate the ideal in law at the moment of its passing. If so, it is understandable that we should find the concept perplexing. But it would also reflect on those abstract moral theories in which the concept of privacy finds a comfortable and an exalted place. The value of privacy or the duty to respect it are intelligible only in the light of a prevailing conception of a life worth living and within the constraints of a life that our relative affluence makes possible.

3. Our world has changed in another way that bears more directly on the theme of information privacy. Information technology, as the contributions to this conference by our electronic experts makes clear, can potentially and radically alter our modes of interacting with others at home and in the marketplace. If I cash a check, in the frame of mind to which I have been habituated from my youth, I have no thought for this act as other than a momentary though useful transaction. If I am conscious that cashing the check will be somehow lodged forever as an available item of information about me, I must come to think of it differently. And this difference in attitude has nothing to do with embarrassment or some deeper distress at the revelation of a deeply personal aspect of my being. The shock to me is not that this transaction is known by my wife, employer or the FBI, but that the retrieval of this trivial moment in my day's business implies that my life as a whole is on public view. This shock is fundamental. It goes beyond the question of legitimate uses of information within a particular form of political order. I find, in contemplating such a potential reality, that my idea of myself as an individual has undergone radical transformation, as it would were I to discover that my belief in the opacity of walls, clothes or skin had all along been mistaken.

John Wyndham invites us to enter such a changed personal world in his science fiction tale, *The Midwich Cuckoos*. The strange children in this story, who are incubated in terrestrial mothers through impregnation by an other worldly parent, have telepathic powers. Each of them thinks, knows and feels what all the others think and feel. Are they individuals, in our sense? The separateness that allows us the luxury of our private thoughts is not available to them; nor would it be to us if each detail of our public lives were preserved forever in a retrievable form. This is not an assault on our civil liberties, but on the concept of ourselves as discrete persons, on which all civil liberties and legal institutions generally depend.

This is what makes the issue of information privacy intractible. The potential of information retrieval systems reaches to every conceivable act; but our conception of ourselves as individuals is still nourished by our capacity for internal soliloquy, private thought. That capacity seeks confirmation in the guarantees of an arena of private, unreported action. Information systems eliminate those guarantees. Of course, we can imagine someone like the hero of Jack London's *The Star Rover*, who, though in solitary confinement, manages by sheer will to create and sustain a fantasized individual life. But in prizing individuality, we surely mean more, or less, than this. We do not suppose that we are required to affirm our individuality heroically, but acknowledge that independence and autonomy are frail and easily extinguished qualities of mind and life. They require protection and insulation. A totally open society strips us of these guarantees.

On the other hand appropriate guarantees appear to require a degree of regulation that would portend for many the opposite evils of a closed society. Control of information appears to be possible only in the design of the hardware, and this entails currently unorthodox measures for the regulation of private industry. Perhaps our guide here should be such ventures as we have made into the control of industry-created pollutants. In this case, as in privacy violation, the striking fact is that individuals who stand to be harmed, are willing participants in the processes that bring the threatening condition about. Most of us want the technology; it makes life easier for us. Similarly, most of us consume pollution-related products avidly and sometimes unavoidably. So we cannot quite construe the problems we have in this area as a conflict between business practices and individual rights. A fish bowl society threatens us in basic ways: its control will be contrary to our political and legal traditions. But perhaps we have moved a stage forward when we recognize how intractible the problem is.

Footnotes

I owe much of what I say here, and how I say it, to twelve college teachers who gathered together in the Summer of 1981, under the auspices of the National Endowment for the Humanities, to discuss the concept of privacy.

1. R. WOLFF, IN DEFENSE OF ANARCHISM (1970); R. NOZICK, ANARCHY, STATE AND UTOPIA (1974).
2. Cambridge, Mass: Harvard University Press (1977).
3. R. DWORKIN, *The Rights of Marvin Farber*, NEW YORK REVIEW OF BOOKS (Oct. 26, 1978).
4. Lovisi v. Slayton, 363 F.Supp. 620 (D.C. Va. 1973).
5. Rochin v. California. 342 U.S. 165 (1957).
6. Breithaupt v. Abram, 352 U.S. 432 (1957); Schmerber v. California, 384 U.S. 757 (1966).
7. I ignore here ways in which it may offend the Fourth Amendment.
8. *But see* Chimel v. California, 395 U.S. 752 (1969).
9. Olmstead v. United States, 277 U.S. 438 (1928).
10. J. THOMSON, *A Defense of Abortion*, 1 PHILOSOPHY AND PUBLIC AFFAIRS 47 (1971).
11. Doe v. Bolton, 410 U.S. 179, 214-15 (1973).
12. *Compare* J. ROBERTS and T. GREGOR, *Privacy: A Cultural View*, in PRIVACY: NOMOS XIII (Pennock and Chapman Eds. 1971).

Information Technology and Privacy Trends in Products and Services

by Fred W. Weingarten*

Introduction

Privacy is far from a new problem. As an issue in this country, it dates back to colonial days and earlier. Furthermore, since the privacy issue concerns, in part, the collection and distribution of information, it has always been affected by developments in information technology—the printing press and the camera, to name just two.

Thus, we will state two hypotheses: (a) The information revolution we are entering may have a profound effect on our notions and rules regarding privacy. (b) The resulting problems will have deep historical and political roots that will inform our response as a society. This meeting is an attempt to understand future challenges to privacy—the nature of the conflicts that will shape the ultimate choices we make and the possible responses available to us.

In order to begin this process, it is necessary to survey the information technology that will surround us in the next decade or two. This task is the purpose of this paper. It is a job with severe constraints and, before proceeding, the limitations of such an analysis must be underscored.

A Warning

Scrooge asked the Ghost of Christmas Future if the shadows he was shown were of those events that would occur or that could occur. The distinction is important. Technologists can tell us about the potential, not about the choices we will make in using that potential. Therefore, if this paper says that a device or an application is technologically possible, such a statement does not necessarily constitute a prediction that it will occur.

This caveat is especially important to keep in mind with regard to sections of the paper on data collection. We have a fairly good notion of certain trends in information technology. We also know to some extent what hardware and software computer science is preparing for us in the laboratory and what manufacturers are dreaming about in their board rooms. However, we know less about the future desires of the marketplace and the nature of the laws and regulations that will govern how information is used.

We need also to keep in mind a more general warning made by the sociologist Daniel Bell in several of his writings. It is not necessarily technology that impacts society for good or bad, but its uses, which are, in turn, shaped by the values of the society and by the historical context in which the technology is used. For instance, many issues regarding individual rights surround the use of criminal justice systems, but the nature of their use, when computerized, is shaped by centuries of law enforcement traditions and attitudes.

The National Criminal Information System (NCIC), run by the FBI, is far different from a comparable system that would be designed to operate in the Soviet Union, or even in another democracy such as Britain. The societal impact of the NCIC system, then, is dependent not merely on the nature of modern computer and communications hardware, but on the design choices made during its implementation and its uses by the criminal justice community.

This warning preface is intended to encourage a critical perspective on the part of the reader in reacting to what may appear to be a rather chilling picture of the future, a picture in which the capacity of the technology to collect, store, analyze, and distribute the most personal information about ourselves appears to be nearly limitless. We are not trapped helplessly in front of an unstoppable technological steam-roller, however, much will be required to live with the results of our decisions regarding its use.

The Approach

Since this description of technology is intended to support the discussions of this workshop on privacy, four guiding principals have shaped the analysis to that end:

1. The paper focuses on the products and services that are likely to be available.

Most technological forecasts in the area of information technology dwell on the remarkable trends in the basic technology itself—how the new pieces of silicon created by the microelectronics industry compress enormous capability into microscopic space at bargain prices.

These trends are indeed noteworthy, but, with a few exceptions, they do not directly relate to privacy. Of greater importance are the ways in which these tiny chips are incorporated into the environment surrounding us. As an extreme example: if the automobile industry was to absorb the total production of microcomputer chips over the next decade, our task would be made easy. Although the automobile industry will, in fact, use a lot of chips over the next few years, a large number will be left over for other purposes, some of which this paper will explore.

2. The forecast is be "surprise-free"—it assumes that most of the information technology that will be commercially available over the next decade exists now, at least in the laboratory.

*Dr. Fred Weingarten was President of Information Policy, Inc., Washington, D.C. and is now Program Manager, Communication and Information Technology, Office of Technology Assessment, U.S. Congress.

This type of forecast is most common, and it is justified for two reasons: (a) It keeps the policy analysis, which is at best a slippery exercise in uncertainty, at least fixed at its starting point. (b) The length of time required to find an application for a new basic research discovery and to market it widely usually exceeds the period of analysis.

3. The forecast emphasizes those characteristics of the new products and services that seem to have privacy implications.

In particular, we will be concerned with potential users of the technology, the environment in which it is used, and its characteristics in terms of the collection, storage, transmission, or manipulation of personal data. (No judgment is implied about the sensitivity, utility, or potential for harm from misuse of any particular type of personal data.)

One interesting characteristic we will examine that is often ignored is the potential of a computer application to create a new market for personal data. We often hear computer users say, "Sure, that capability to invade privacy exists, but there is no incentive to collect such data." However, some new computer applications—for example, systems to predict jury voting behavior—may, in fact, create markets for personal data that would provide such an incentive.

4. The paper assumes no legislative or market barriers to the development and production of applications and services.

Although certain applications could be considered damaging and be outlawed, or particular types of information services could be delayed by antitrust rulings in the courts and so on, this paper assumes a permissive atmosphere. More importantly, although many industry experts are making grand predictions about the growth of the information service industry, the possibility remains that consumer resistance or indifference could stifle the growth of the market. For example, twenty years ago the nuclear power industry would not have predicted the combination of popular resistance and regulatory restrictions that has hampered its growth.

General Trends

A number of general trends in information technology affect our view of services and products available in any specific environment. Many of these trends result from the marked drop in price and the availability of microelectronics hardware.

1. Products that contain computers will be more prominent than computers themselves.

This trend, resulting from the low cost of computer hardware, means that, rather than selling general computer systems, manufacturers will sell complete packages designed to do specific tasks—for example, word processors or sophisticated sales terminals for retail stores. These systems do not require that the purchaser be an expert in computer systems. With the low price of computers, computer manufacturers make money in only two ways: (a) selling hardware already equipped with expensive software and (b) increasing their volume of sales. To sell more products to a population not completely composed of computer experts, companies must sell systems that don't require sophistication. This observation leads to the next.

2. Computer products will be mass produced.

A large variety of computer-based products will be used by people in many walks of life. This point is important to note since some effects of smaller computer-based applications on privacy may depend upon widespread use.

3. Computers, communications, and other information technology are becoming integrated.

The so-called merging of computers and communications is often interpreted in the press to mean that computers and communications can no longer be distinguished. This conception is attributable to the development of more complicated information services that use both computers and data communications. If companies like IBM and AT&T were content to make computers and carry signals over wires respectively, there would be no problem. However, both companies choose to sell the new information services, which represent the real profits in the industry. The integration of computers and communications will magnify the privacy problems in the 1980s and thereafter.

4. The nature of information storage is changing.

In the last few years, the cost of storing information electronically has become competitive with the cost of using paper. Before, the chief motivation for putting data in electronic form was that it would be processed on a computer or transmitted.

Now, the change in economic incentives will greatly increase the nature of information regularly stored in electronic form. Furthermore, it will reduce the incentive for system operators to purge old information from their data bases.

5. The market for information is growing.

We are becoming a knowledge-based society, one that depends on the creation and use of information. Economists point out that information is becoming an important commodity of trade. Many important public policy impacts arise from this trend alone. Particularly, many privacy problems will grow more severe, depending upon the growth of a market for personal data.

6. The number of very large integrated data systems will increase.

Although much attention has been paid to the explosive growth of small computers due to the microelectronics revolution, an equally significant trend is the development of systems capable of storing and retrieving information in very large data bases containing billions or even trillions of elements of information. Perhaps one reason this trend has

received less attention is that big data systems are not new, especially with respect to the privacy issue. The fair information practice concepts were meant to apply to such large, centrally controlled data bases to which the information has been knowingly contributed by the data subject.

It does little good to think about general trends unless they can be discussed in terms of our environment. This paper will examine the environments in which humans live their lives, beginning with the most intimate environment, the individual person and following with the home, the workplace, and other social environments—finance, education, the marketplace, and the government.

Information Technology and The Person

The first and most important locus of new information technology we will examine is the last fortress of privacy, the individual. Three important trends are changing the nature of information collection at this important boundary:

1. Micro-miniaturization of electronics increases the portability of information technology.
2. Improvement of sensory instruments allows for sophisticated, unobtrusive monitoring of bodily functions.
3. New telecommunications technology will facilitate direct links with individuals no matter where they are.

Portable Information Tools

A number of information devices can be designed to be carried in a person's pocket for everyday use. They will resemble the current pocket calculators that have become so popular. The principal differences will be that their function will depend at least partly on the storage of information, and they will be capable of linkage with other systems.

- The hand-held computer

The hand-held calculator will be looked at as a very short-lived phenomenon, although some version of the device will continue to be around for a while to perform very simple calculations. The first hand-held computers are already on the market. They are fairly limited, both in programming language (Basic) and in memory size (a few thousand characters), and they cost a few hundred dollars. Their price is expensive for a calculator, but cheap for a computer. If the trend established by the calculator offers any clue (and it should), we can assume that performance will improve rapidly, and the price will drop just as quickly. These machines will be used for numerous purposes in an individual's daily life—storing telephone and address lists, a calendar of appointments, and financial records and inventories of personal property. These applications are already popular with owners of home computers and would probably be even more so on portable hardware.

The popularity will increase as systems are developed that require less computer sophistication on the part of the user. As the price of hardware continues to drop, dedicating a unit to a specific task accomplished through a specific language becomes more feasible. For example, a checking account management system the size of a checkbook might be permanently programmed to perform specific tasks, which features a keyboard that has commands such as "post," and "deposit." A pocket "Day-timer" might be similarly marketed, or a pocket address book. Particularly promising is a pocket investment computer designed to track an individual's portfolio or list of stocks he or she is watching. Periodic plugging into the Dow Jones service would update the data base and a stockholder might even use it to initiate transactions.

The key to all these devices is that they will store information of various kinds and will probably be designed to communicate with a larger system at times to dump recent transactions or update their own small data base.

- The "Intelligent" or "Smart" Card

The intelligent card has not yet reached our shores from France where most of the developmental effort seems to have expanded. Some U.S. corporations are reportedly studying it.

Simply put, the intelligent card is a microprocessor within a credit card. From a technological point of view, the intelligent card is similar to a hand-held computer. However, from a functional point of view, it is designed to be part of a much larger system and to perform very specific functions within that larger system. Thus, the card neither has a keyboard nor any mechanism for the person who carries it to interact with.

In its simplest incarnation, the intelligent card will be a more sophisticated automated banking card. It will allow for more elaborate identification and authentication processes that will be more difficult to forge. It will allow more sophisticated operations for point-of-sales transactions.

Development of the card is a step toward the ultimate goal of creating a true "cashless" system. If the equivalent of a cash advance could be written into the card's memory by the bank, then a merchant could accept the card as direct payment without needing to communicate on-line to a bank. Advances could be made electronically by an automatic teller without dispensing cash. The bearer would, in turn, have the equivalent of cash in his or her hands without the danger of theft or loss.

Several problems remain to be solved, however, not with the technology of the card, but with the overall system in which its use would be imbedded. Problems such as security, protection from forgery and fraud, must be studied very carefully, not to mention the numerous legal and regulatory problems that would have to be resolved. Privacy would, of course, be a probable consumer concern, in addition to a general uneasiness at not having the green and silver stuff in hand or pocket.

Even aside from its use as a cash-card however, numerous applications have already been proposed for this technology. Among them are the following:

- A gasoline credit and/or rationing card.
- An unforgeable national ID card.
- A device for home terminal stock and bond trading.
- A portable medical record file.
- A medical insurance identification and record.
- A credit or debit card.

It will probably be a few years before a major application of the intelligent card appears in the United States, while some experiments are projected to start in France by early 1982. U.S. firms reportedly looking at it include a few banks, the American Express Co., and Blue Cross/Blue Shield.

Medical Sensors

Medical science is on the verge of acquiring a number of new devices based on microprocessors. The instruments also make use of new sensor technology developed for the military and NASA. These instruments can be implanted in the body and be programmed to measure bodily functions and provide electrical or drug stimuli.

There is no reason to believe that the industry currently is working on devices that could control the brain or even provide simple location or identification capabilities. However, such technology will certainly become technologically feasible over the next decade, and it is not hard to imagine certain legitimate applications that would result in such a capability being developed. The possibilities for misuse, no matter how unlikely, are nearly Orwellian in their implications.

There are three reasons why new medical technology may have privacy implications:

1. More types of measurements are possible.

Scientists are now able to monitor with microprobes the biological functions even within the nucleus of a single cell. This ability coupled with an increased understanding of biological and neurological processes ensures that future instruments will be able to collect a great deal of information about the physiological and psychological state of a subject.

2. The presence of instruments may be unknown to the individual.

3. The instruments could be monitored externally.

Very small transmitters could be added to the devices to allow the readings to be monitored from a remote location. Such a device, in its simplest form, could serve as a locator or identifier.

Information Technology in the Home

This section will examine the five specific characteristics of new information technology in the home:

1. Many common consumer devices will contain computer chips.
2. Many homes will have personal computers.
3. A variety of new entertainment media will be available.
4. Communications lines into and out of the home will increase in capacity.
5. Homes will be linked to various outside information services.

Consumer Devices

Many appliances already contain microprocessor chips; sewing machines, microwave ovens, television sets, children's and adults' games, and thermostats are but a few of the applications already on the market. This trend will continue, limited only by the production capacity of the chip makers.

Today, appliances use computers in fairly simple ways to duplicate or slightly improve control functions or to clarify a display of the appliance's performance. Future versions will make more imaginative use of computer technology. One of the important features will be the ability to tailor the appliance to the user's needs. Microwave ovens, for example, will remember the favorite recipes of the owner and adapt a cooking sequence to match. Telephones now "remember" the most frequently called numbers to simplify customer dialing. In both of these examples, one of the functions of the processor is to remember something about the habits of the user and incorporate that knowledge into its performance.

Personal Computers

Estimates of the robustness of the growth of personal computers vary. In fact, the sales curve of any new product exhibits an "s" shape, tapering off at the saturation point. Experts differ on the location of the point with regard to personal computers. Conservatives argue that the personal computer, like the ham radio, will be the domain of the home hobbyist, not of the mass consumer. At the same time, sales have been higher than predicted, stimulated by the Tandy Corporation's (Radio Shack) entry into the market.

In 1977, the Tandy Corporation, a firm that specializes in consumer electronics, marketed a home computer, the TRS 80, a phenomenon that future social scientists may look upon as a watershed. For a few years before 1977, the personal computer market was characterized by very small manufacturing firms, unreliable distribution, small stores, and little service support. Then Tandy went for the mass computer market and paved the way for other firms such as Apple. Now computers are being purchased by small business owners, professionals, school teachers, and other people who use the computer as a tool. In these homes, computers help with budgets, store information of all sorts, control household appliances, and educate children (or parents). In the next decade, this trend could well keep the sales curve climbing sharply.

The practical uses of computers that motivate the market are also significant from a privacy point of view. The most popular applications appearing on the market now involve automating checking accounts, tax preparation, inventories of personal property, telephone and address lists, and time scheduling—all applications that involve computerization of personal data. Furthermore, the personal home computer is a vital link to other information services originating outside the home and delivered over various types of communication channels.

Entertainment Media

If market estimates are correct in their predictions of widespread use of new video entertainment services supposedly on the way, this society will soon perish, for we will have no time left in the day for sleep, nourishment, work, or any other normal social function. A list of some new video technologies here or on the way follows:

- Video cassette recorders

The first of the new video technologies is nearly ten years old, but has grown into a major consumer product, at least among the affluent markets. Its principal lures appear to be "time displacement," that is, the ability to watch programs at a time of one's own choosing and X-rated films.

- Intelligent video discs

The technology used for some of the video disc devices allows a microcomputer to be connected to the unit. Computer data and programs can be stored on the disc, as well as text, stereo sound, and high resolution still pictures. A video disc so equipped becomes a device markedly different from the "record player with pictures" originally conceived by the industry. The data storage potential of the disc is illustrated in an estimate by Xerox that, within five years, only 100 video discs could contain the entire holdings of the Library of Congress.

- Low power broadcasting

Low power broadcasting is a new television capability just opened by the FCC for licensing. It merely allows television stations to broadcast programs on standard television channels at a power level low enough not to cause interference beyond a range of only a few miles. The advantages are twofold: it allows many more channels to be opened for use in an area, and the broadcast facilities are relatively cheap—only a few tens of thousands of dollars can get a channel on the air. These two advantages will, in theory, open up the airways to more groups with specialized interests and markets.

- Cable and two-way cable

Like video cassette, the cable has been around for some time, but the boom has only now started. Cable use has grown from a mere five million homes in 1970 to 30 million homes in 1980 to a projected 45 million homes in 1985. The attraction of cable is no longer better signal quality for the normal broadcast channels, but a rich variety of offerings from normal broadcast to specialized cable services that operate nationwide over satellites. Most new installations are also installing two-way capacity despite the enforced retreat of the FCC from regulating the industry.

- Direct broadcast satellite

COMSAT has proposed to the FCC establishing a direct broadcast satellite service that would provide three channels of programming across the country. The programs would be broadcast directly from a set of communication satellites to receivers' homes. The technology remains somewhat expensive, but the cost is dropping rapidly. As with many other video technologies, the final price levels for the hardware will depend upon the size of the consumer market that develops. Over the next decade, a number of such direct broadcast services could evolve, although the price of building a satellite system and limitations on frequency and satellite parking orbits would serve to keep the number low.

It is pure guesswork at this time to predict which of these technologies will win the competition for the attention of the consumer. Nor is it possible to see with confidence what their long-term uses will be or the changes in social behavior patterns they will create. Surely, in many ways they are new media, as different from network broadcast television as that technology is from the radio. However, the following trends already seem likely and may be relevant to privacy problems:

— The substitution of electron storage for print

While printed paper will not disappear for a long time as a means of communication, current trends suggest that there will be a steady replacement of print by electronic communication. Publishers and newspapers are buying communication companies as fast as they can. At least one magazine is published on videotape, and experiments are underway with an electronic newspaper.

— Pay-for-service

The days when most video entertainment was provided "free" by network broadcasters are probably drawing to a close. The new technology, as well as the changing economics in the information marketplace, will promote a move toward the consumer paying for each of the programs used. This trend will, of course, raise questions of "access," but they will also result in detailed records of viewing habits retained for billing purposes; these records are possibly equal in sensitivity to library records.

— "Narrowcasting"

Also on the wane will be the orientation toward mass entertainment. The new video technology will lead to what is referred to in the industry as "narrowcasting," that is, aiming particular productions at specific audiences and specializing in particular types of programs. This trend, analogous to that already experienced by the magazine industry, is starting to

appear in cable. Special cable networks exist for exclusive coverage in areas such as sports, news, and religion. This trend is facilitated by the increased number of channels available and by satellite transmission to many cable outlets which allows even a specialized market to aggregate over a large population.

Communication Channels

New communication technologies are changing the amount of information that can flow to and from and within the home. The principal limit on the speed with which these changes take place will be the rate at which facilities can be built, for the entire copper wire-based communications network of this country is being transformed. The home will see the following changes:

- Fiber optic telephone lines

Fiber optic transmission consists of pulses of light sent through thin glass fibers. The capacity of fiber optic transmission lines is much greater than that of copper wire or cables of comparable size. The steady improvement of the technology, coupled with the increased cost and scarcity of copper, indicates that fiber transmission lines will steadily replace copper ones. Replacement, however, will be slow because of large amounts of capital tied up in the existing system. AT&T's annual capital budget is an enormous $14 billion, but the total value of the current system is an even more awe-inspiring $111 billion book value. (Both figures are 1978 dollars.) Telephone companies will probably begin this effort in the intermediate-length trunk lines connecting cities and within large cities such as Chicago and New York. New developments, towns, and very large buildings are receiving fiber transmission lines early. Replacement of lines in older neighborhoods will probably take much more time.

This conservative estimate could be changed by regulatory and tax changes directed toward encouraging faster installation or by increased competition from other new channels of communication for the home such as cable or broadcast.

- Cable

After a period of dormancy following grand predictions of growth in the late 1960s and early 1970s, cable is now growing rapidly. Cities are granting franchises, and large corporations that have the necessary large amounts of available investment capital have now entered the business.

By the end of the decade, a significant number of homes will be tied to the end of a cable and most of those links will be "two-way;" that is, they will allow the home to transmit information as well as to receive it. However, because of the demands of a television signal, the transmission capacity into the home will be significantly greater.

- Direct satellite broadcast

Depending on the success of experiments such as the COMSAT proposal mentioned in the previous section, many homes may have small antennae on their roofs for the direct reception of satellite transmissions. A two-way satellite system is a more remote possibility, but expensive, and although technologically feasible, such a facility would not merit implementation.

In-home Information Services

The new home communication lines mentioned above are intended to carry services to generate the income to pay back the large investments made in them. In many cases, entertainment services will be the principal offerings, but, once the lines are in place, many other services become economical. In fact, in some cases, non-entertainment services that were once regarded as supplementary are now being viewed as major sales attractions.

Among the wide variety of possible services on the drawing board or offered experimentally are the following:

- Teletext/Viewdata

A number of technologies exist to bring information services directly into the home through the television set. Both broadcast and cable services are being designed.

The teletext services are the oldest technology and have been widely developed in Europe and Japan. The format is essentially passive, like a magazine. All information in the magazine is broadcast over and over, and the viewer has an electronic switch with which he or she chooses pages. Two-way viewdata systems allow the user to request specific information from a very large data base. The information is then transmitted to that specific person's receiver for display.

The specific formats for these systems are now a matter of great debate among U.S. firms. The key point for the future decade, however, is that the individual will have nearly instant access to a wide variety of timely and valuable information.

- Home banking

Today many banks and savings institutions already offer a pay-by-phone service to their customers. However, more elaborate services are imminent. Owners of personal computers already have available a more sophisticated service being offered experimentally by a few banks. Such services in the future will link a home computer system with a person's bank record as to allow access to budgeting, tax accounting, payment authorization, loans; virtually the entire range of services banks now offer their larger corporate customers.

Subscribers to cable-based videotext systems will also have access to sophisticated banking services. An experiment along those lines has already been mounted by Bank One in Columbus, Ohio.

The principal technological limitation to home banking services will be the inability to handle cash transactions for deposit and for withdrawal. Perhaps the greatest pressure for replacement of cash by the "intelligent card" (see p. 17) will be that such a card will allow complete in-home banking including the

direct withdrawal of money in electronic form. Such a service, should it come to pass, will appear only toward the end of the decade, for several technological and regulatory problems remain to be solved.

- Home security

Cable systems with two-way capability are offering burglar and fire alarm and medical alert services to their customers and have found the market to be quite strong. Over the decade such services will likely become commonplace additions to the in-home cable, and they may become increasingly sophisticated. The implication, however, is that substantial monitoring of the household environment is taking place from the outside and the results stored in data bases. Since it will be done in the name of security, the privacy implications of such data collection may be ignored by the customer.

The security concept could be extended to include other services that monitor the home environment, for example, utility meter readings done by cable. Such facilities, however, could be used to accomplish other types of surveillance that may not be voluntary on the part of the occupant. As a single example, suppose another wave of energy conservation regulation sweeps the government. Using information technology, government agencies could easily monitor homes to ensure compliance.

- In-home shopping

A service known as Com-U-Star, which now exists on personal computer networks, provides a nationwide shopping service to participants. Two-way cable companies are beginning to develop such services, although they are experimental at this time. It seems probable that a significant amount of purchasing will take place from the home over cable, telephone, or personal computer data network. The rate at which it grows will depend on the degree to which the savings in time and cost to the consumer will outstrip his or her desire to look the salesperson in the eye and squeeze the merchandise.

- Electronic mail

Some primitive electronic mail services already exist for users of personal computers. Eventually, the transmission of text material from point-to-point electronically will be commonplace.

Some experts, including the U.S. Postal Service, claim that this transmission will be achieved by means of intermediate processors that convert the text to electronic form in some central office and transmit the text, which is then converted back again to paper in the home.

Indeed, were electronic mail to evolve from the traditional services, such a development might occur. However, electronic mail may also develop as an added service of cable or personal computer data networks, sophisticated services that already exist. A mail network will grow because of increasing numbers of people tied into existing networks, not necessarily because of technical advances.

Furthermore, many of the tasks we now perform by mail will have electronic substitutions. As stated above, the next decade will see the growth of the electronic magazine and newspaper, advertising and in-home purchasing over cable, and home banking. As a test, look at the next batch of mail that comes to your home and try to imagine how much of it could be replaced by home information services, whether called "electronic mail" or not.

- The digital telephone

For mostly technical reasons, the telephone company has been gradually converting its network to digital transmission. One result of this conversion is that the signal conveying the voice will be in a computer-readable and storeable form. Signal information about the source and destination of the call is also digital.

These changes allow the telephone companies to computerize their network switching operations, and they also allow a number of new services, including the following:

— Forwarding of calls to another number

— Display of the calling number on the telephone of the receiver

— Storing a voice message in the system for later transmission

Although the potential for future information technology and services in the home may seem somewhat overwhelming, some general statements can be made about the privacy implications of all these systems:

1. George Orwell's concept of massive television surveillance in the home is not likely to be technologically feasible for some time, due to limited communication capacity from the home and the difficulty of processing such a mass of surveillance information.

2. The available technology would support, at some expense, the ability to keep close watch over specific residences.

3. Substantially more personal information would be available in electronic form for surreptitious bugging than can currently be gained from a wiretap or eaves-dropping device.

Information Technology in the Workplace

In this section, we will describe those technological trends that will affect the workplace and that may have privacy implications. If the discussion seems to dwell on the service and information sectors of the economy, white-collar work, there are good reasons.

First, the number of people engaged in the manufacturing and agricultural sectors of our economy is small and still shrinking. Second, the service sector, because it has felt the heaviest pressure to improve productivity, is automating rapidly. Office automation has become the fad of the early eighties.

Whether white or blue collar, automation of the workplace will have some general effects on the people who are asked to operate them:

1. Any automated machine is potentially capable of collecting and storing information about the performance of the person operating it.

2. Automation will change job definitions and patterns of work. These changes will also be reflected in changing patterns of authority.

3. Whenever a job is capitalized by the addition of expensive machinery, the attention of management shifts to the productivity of the machines rather than the people operating them. This shift in concern can lead to a greater desire by management to measure and monitor employee performance. The performance of a secretary with a typewriter is measured as a combination of many skills. The installation of expensive word processors, however, can drive management into an obsession with keeping the machinery going at the fastest rate possible.

Factory Automation

Spurred by advances in computer technology, specifically robotics and computer aided design, along with increased competition from the Europeans and Japanese, manufacturers will undoubtedly move very quickly to automate over the coming decade. The principal changes will be the movement of automation into manufacturing assembly, putting small devices like pumps, electric motors, or computers together. The automated factory of the future will integrate its functions. That is, the automation will not consist of merely bringing in another machine, but of reorganizing the entire work of the factory around computer control.

As stated above, these changes will affect workers, and unions are starting to warn their locals to watch for the use of such computerized equipment for surveillance or other types of coercive activity. However, the two most significant problems that worry unions are (a) protecting jobs and (b) accommodating the changes in skills that will be required of the workers.

Office Technology

A number of basic changes are taking place in the office. Among them are the following:

- Disappearance of paper

The costs of electronic information processing are dropping, and the costs of material and labor for handling physical forms of information are climbing. Some analysts say that the electronic form is now cheaper than paper.

In a typical word processing system, 1000 characters can be stored for only a penny or two, and storage prices continue to drop rapidly as the technology improves and as mass production economies are realized. Many cost projections dwell on the effects of technological advances. However, the effect of the rapidly growing market for computer supplies is also marked; this increased demand results in more efficient production and distribution and, consequently, lower prices.

While politicians soberly discuss the possibility of electronic mail, corporations are already using it. New data communication services are being developed by old and new companies to serve this new application.

Satellite Business Systems, a new company, has just connected its first customers. AT&T and Xerox will soon follow. Their facilities are designed to provide high capacity data communication services that will support inter-computer networking, electronic mail, fascimile transmission, and conferencing. Over the next decade businesses will link together through these data channels and most information exchanged will be transmitted electronically.

The teleconferencing technology has been awaiting a drop in data communication costs and for facilities to become more accessible. Whether through audio, video, or computer conferencing, organizations will probably turn to these media as a substitute for travel and as a means of building tighter and more timely administrative links between offices. While the literature has focused on teleconferencing between distant locations, the technology may well turn out to be an economic facility for use within a single building.

- Automation of clerical functions

Closely linked to the trend above is the automation of information handling. Probably the most visible current trend is the advent of the automated office, word processing being the leading development.

Word processing represents the substitution of electronic computer-based devices for the typewriter, and we all know the benefits that have been attributed to it. Over the next decade, word processors will be integrated into the larger information flow of the organization. They will be tied to the electronic mail system and an electronic filing and information retrieval system. Managerial and professional staff will have terminals on their desks. The manager can enter a draft into the system; then sophisticated interfaces could put the draft into correct format (e.g., memo or letter) and correct spelling and grammar. Voice input has been projected for the mid-to-late 1980s although several problems remain to be solved.

The technology clearly has the potential to change the nature of the secretarial job, possibly even eliminate it. However, another trend is also becoming clear, at least in the early stages of office automation, a trend that may well run counter to the expected disappearance of the secretary. Because a word processor is more complicated to use than a typewriter, this technology may well professionalize the job of secretary.

It is usually assumed that automation is applied to a job as previously defined. In this view, an automated typewriter should take less skill to use than a manual one. Why is the opposite true?

Because, the new technology provides more flexibility by allowing the user to do more work and to manipulate many more possible functions. Like a librarian, the secretary will manage the flow of information into, out of, and within the office, using all the information technology discussed above.

Many other service jobs are being affected by automation. For example, cash registers have by-and-large been replaced by computerized systems. Bank tellers work with terminal or telephone access to a computer data bank containing account information. The same holds for airline ticket agents, car rental agents, hotel clerks, and so on. Grocery stores are currently installing automated checkout systems.

A common characteristic of all these devices is that, in addition to providing the information services necessary to do a job, they also collect information on the employee. Even if that information is not used at present, it is available, and employers are starting to collect it. Word processor operators in large shops may find that elaborate statistics are being maintained on their performance, typing speed, time at the terminal, error rates, and so on. Measurements of the activity of store clerks, bank tellers, and others can help employers check for fraud or employee theft.

- Changing patterns of information flow

Because of the changes discussed above, the pattern of information flow within an organization will likely change, thereby affecting the way decisions are made and authority exercised. The process by which new ideas are born, discussed, tested, and modified within an organization before they are presented to upper management occurs in an environment with some limited form of privacy. If the effect of automation is to increase the transparency of information flow within the organization, creativity could be stunted, or alternate informal channels could develop. Therefore, for their own self-interest, organizations may need to concern themselves with the "privacy" of internal employee communication.

The computerization of information within an organization will also expose it to more attempts, legal and illegal, to gain access to that data from the outside. A well-organized corporate information system, which stores all memos, correspondence, reports, and forms electronically and indexes them for retrieval by management, would certainly be a useful target for "fishing" by regulatory agencies, adversaries in lawsuits, or competitors.

- Automated security systems

Employers have legitimate concern about the honesty of their employees. In some businesses, employee theft and fraud are a major expense. The productivity of their employees is also of legitimate concern. Information technology offers new opportunities for imposing tighter controls.

Companies now offer microcomputer-based locks that are activated by a machine-readable employee card. These locks can be used to control physical access to locations or to devices such as gas pumps or computer terminals. They can also be used to control the access or just to monitor it, for access information—since they are computer-based—can be stored or transmitted to some central location to keep close tabs on the movements and activities of employees. Later in the decade more sophisticated surveillance technology may develop, particularly automatic picture or voice recognition.

The capability to use other information technology in an automated office for such surveillance will also develop. Already, companies are using pen registers in digital telephone systems to monitor employee use of the telephone.

Finally, the next decade may see substantial refinement in the technology of computer-based devices for lie-detecting or other psychological measurements. The voice stress analyzer now on the market is reportedly used by some companies. Many other companies still use conventional lie detectors, which are troublesome enough, but at least require some cooperation and knowledge of the employee.

- Automation of professional services

Professionals such as lawyers and doctors also deal with information. In the coming decades, information systems will support their work in a number of ways:

- Data bank services. A number of such services are already on the market, such as Lexis, Medline, and so on. Pergammon is developing a patent search library for a video disc/computer system.
- Office management systems. These systems may be based on small office computers or they may be linked through terminals to a central service bureau. They may maintain client records as well as financial information.
- Assistance with work. Researchers have been working on diagnostic aids to doctors and some are soon to be commercially available. Lawyers have for some time been using computers to store and index evidence. Over the next decade, systems using artificial intelligence techniques may even play the role of a research assistant. As the size of complexity of the data bases increases, the professional will need sophisticated aids to help him or her make use of the information.
- Educational services. Many professionals find it difficult to stay current with rapidly changing fields. It seems likely that technology based professional refreshment packages will be marketed in the near future.

Of course, the applications that have privacy implications will be those involving the maintenance of client records. These will be uses such as billing, medical treatment, or manipulation of legal evidence.

- Geographical dispersion of work centers

Some experts predict that work will be dispersed geographically. Some press attention has been given to the electronic office and the idea that office automation combined with high-speed data communication

make it unnecessary to locate all employees in a concentrated center. Regional offices or even work in the home will be feasible.

Decentralization is also planned for manufacturing. The Norwegians reportedly are considering using robotics technology to develop a system of small, geographically dispersed manufacturing centers. They feel that automation will eliminate economies of scale in manufacturing that favored large factory complexes.

All these trends are technologically feasible. Whether they are implemented on a large-scale basis in this country will depend on many social and psychological factors that are not so easy to predict. A trend such as concern about energy or national security could motivate a boom or a decline.

Information Technology and Society

Individuals encounter information technology in a number of social environments. This section will discuss four of them—finance, education, the marketplace, and government.

Finance

Electronic Fund Transfer (EFT) has been in the news for some time. There is no common definition of what EFT consists of. It is not a single, unified application, but a number of advanced computer-based services found in banks across the country. The most familiar examples include the following:

- Automatic teller machines

These machines are already ubiquitous in most cities. They are the storefront machines that allow cash withdrawal and deposit 24 hours a day.

- Pay-by-phone services

Some banks allow their customers to initiate payments by a telephone call. The process is not completely computerized at this time, since a human operator intervenes in most systems.

- Point-of-sale systems

This type of system is essential in the future "cashless society." A consumer will be able to pay for goods at a store by directly initiating immediate payments from the customer's account to that of the store.

- Automated clearing

Clearing is the process of transferring funds from one bank account to another in correspondence to checks that have been drafted. Automated clearing, simply the use of computers for the transaction, is invisible to the consumer, but it may have significant privacy implications because of the collection and storage of personal data and the possible role of the Federal Government in operating a regional or national clearinghouse.

To the list above, the in-home banking services mentioned previously should be added. But the trends in computerized financial services are too complex to be encapsulated in a list. The structure of the industry is changing. Marked changes include national banking, the merging of savings and checking accounts, the provision of traditional banking services by institutions such as insurance firms, stock brokerage houses, and credit card firms.

In such turmoil, only a prophet would dare to try to predict the future. However, it is possible to describe certain privacy-related characteristics of this new world of finance:

- Much more personal information will be collected and stored in computerized form.
- The integration of financial services, banking, investment, insurance, and credit will cause the integration of individual financial information.
- Nationwide financial networks will be created by national interstate banking, a national clearinghouse, or alternate providers of financial services.
- It will handle personal financial information gathered by organizations not having traditional standards of responsibility for protecting privacy as the banking industry does.
- For those who do not wish to participate in a "cashless society," a major issue may be whether alternate payment mechanisms will be available. The economics of payments technology may not support two or more parallel mechanisms.

Education

Education is basically an information activity. It transfers information, and it teaches individuals to use information. It is only natural to expect that information technology would have a significant effect on education. However, past predictions that it would revolutionize education have not come to pass. There are two reasons why the past may not be a guide to the future. First, the cost tradeoff curve between technology and teacher salaries continues to move in favor of technology. Second, people traditionally equate education with the schools. Historians of education will point out that such an equivalence is wrong, that the public school is a fairly recent invention in social history designed to achieve specific goals. It would not be a very major change for the principal locus of education to shift away from the public schoolroom, and, indeed, there is persuasive evidence that such a shift may be occurring. Information technology may be more effective in a different environment.

There are a number of functions that information technology could perform in education:

1. It will serve as a teacher.

Computers will present teaching materials to students interactively. Linked with video technology such as video discs, cassettes, or even broadcasting, computers can present instruction through interactive dialogue or simulation.

2. It will facilitate distribution.

Communications technology frees the restrictions of place and time that education now experiences. The home, the office or factory, the church or community center all become feasible locations in which to study. Even seminars or other forms of classes that require class discussion can be conducted over a nationwide network. The integration of computers and communications will magnify the privacy problems in the 1980s and thereafter.

3. It will provide sophisticated testing and diagnosis.

Computers have already revolutionized testing for ability and achievement. The computer that is actively involved with teaching has even more data with which to draw inferences about a student's learning style, abilities, and the degree of mastery of the subject at hand. This data will be useful to guide the education process and will likely be maintained as part of the student's records. Also included under this label should be the continued growth of large testing organizations such as the Educational Testing Service. Despite the recent controversy over testing, such organizations cannot help but continue to grow as gatekeepers into the regular education system. Indeed, new pressures are on them to become more active in the area of professional certification and re-certificaton. The services they provide are certainly dependent on the availability of inexpensive, large-scale computing and data storage.

Even if education is not fundamentally transformed by technology, instructional applications will become far more important. Instructional programs are already being offered for personal computers, video discs, and on two-way cable systems; and public broadcasting has undertaken a major effort to develop a "university of the air." Industrial education, already a major user of information technology, spends an estimated $50 to $100 billion annually. Commercial schools, such as the Control Data Institute, are springing up; they also offer alternatives to public education.

Information technology will allow for more generation and storage of personal information generally considered sensitive, especially data on academic performance and psychological profiles. This information may be kept by any number of organizations other than schools.

The Marketplace

Much of the technology that will be used in the retail marketplace has been discussed in the sections on the home and finances. It is necessary to point out, however, that all of these systems link together, and the link is the personal data collected in the systems. The following quote from the *LINK News Briefs* of April 1 illustrates this concept:

> (A corporation) will monitor the influence of commercials on cable viewer's buying habits for . . . a firm whose clients consists of major advertisers and agencies. The test will take place on several cable systems, with selected subscribers viewing specific commercials sent down from the headend. Data on these viewers' subsequent purchases will then be recorded at their local supermarkets via optical scanning of the Universal Product Code found on shelf items. (*Cablevision*, March 16, p. 9)

The firm in question probably has obtained the permission of the subjects, but that point is irrelevant to this technology profile. The significant points are the following:

1. Such a study can be done even with the currently limited state of technological implementation.

2. There is an economic motivation for firms to collect the information.

3. The information can be collected through these systems without the conscious cooperation of the data subject, and the subject has no interest in the data collection.

The Government

The government, of course, will also have a large menu of information technology available. There are five significant trends that will affect the privacy problems of federal data systems over the next decade:

1. Big, integrated data bases will be possible.

There is renewed interest within the Executive branch in a central data base to combine information on all recipients of social services. Such systems will become increasingly feasible and economical.

2. Distributed information systems will become common.

It is not necessary to combine all data into a single computer to use it. High-speed data communications, combined with advanced software technology, make it possible to build systems with pieces of the data scattered around the country. The systems may be operated by a single agency, as are regional centers run by IRS, or they may be interconnected data bases of many agencies, federal and non-federal.

3. The technology now or soon to exist will support a nearly unforgeable national identification card combined with instant on-line access to an accompanying data base.

4. The increase in computerized data in all parts of society will increase the opportunity, if not the temptation, for further data collection on the part of government.

5. Powerful polling and direct mail solicitation technology may have profound effects on the nature of politics both at the federal and local level.

Bibliography

Arden, B., ed. 1980. *What Can Be Automated?* Cambridge: MIT Press.

Bell, D., Communications technology—for better or for worse. *Harvard Business Review.* May-June 1979:20-42.

Cornish, E., The coming of an information society. *The Futurist.* April 1981:14-21.

Evans, C., 1979. *The Micromillenium.* New York: Viking Press.

Laudon, K.C., Privacy and federal data banks. *Society.* Jan/Feb 1980:50-56.

Lecht, C.P., 1979. *The Waves of Change.* New York: McGraw-Hill.

LINK 1980. *Emerging Opportunities in the New Electronic Media.* NRR, Vol. 1, No. 1.

Meindl, J.D., 1980. Biomedical implantable microelectronics. *Science* 210:263-267.

U.S. Congress. Office of Technology Assessment. 1981 *Computer-Based National Information Systems: An Overview of Technology and Public Policy Issues.*

32

A Taxonomy for Privacy

by Willis H. Ware*

The invitation to present this paper suggested that it might seek to organize privacy concerns in some overall framework. How can the many dimensions of privacy be all put together? How can the various perspectives on privacy be harmonized? Can a focus be provided to give some guidance to the legal and judicial systems of the country? Behind these questions is the observation that the legal, judicial, and legislative communities—as influenced by moral and ethical views—are dealing with privacy issues one by one as they arise. So to speak, the issues are dealt with disjointly and in the small rather than in the large. There seems to be no cohesion presently across the fabric of privacy.

A suitable framework must not only accommodate the forward march of technology, but it also must embrace such privacy law as has already been created; and it must provide a mechanism for the moral and ethical views of society to play their part. One might try to approach the task by imagining the privacy consequences for each application of new technologies. However, one cannot be sure that a comprehensive catalog would ensue; and anyway it would all be speculation about things that are possible in principle but might never happen. It is altogether too easy to construct scenarios based on technological possibilities, but altogether too difficult to predict whether such events will ever occur. The discussion here will attempt a pragmatic look at the broad sweep of privacy and is oriented toward providing the legal and judicial communities a way to look at privacy litigation, and possibly also a way for the legislative community to think about new law.

It has been suggested that the proper issue to focus on is the mere existence of technology rather than its use. However, even though the purveyors of contemporary technology might contend themselves with marketing just products rather than services, privacy consequences will inevitably arise as the uses of such products spread. Existence of technology will unavoidably breed some uses that are undesirable in some way. Furthermore, the world, its population, and its institutions must collectively struggle to become more efficient, to conserve resources, to exist and grow, and to establish more equitable societies. Thus, although such products as hand calculators, personal computers, various cable services, wired cities, and on-line data bases can—in some scenarios—create privacy consequences in principle, they do not automatically give rise to privacy difficulties in fact and may never, depending on details of the utilization. In many circumstances economic aspects will be the principal driver; although in some, innovative applications by imaginative people can also stimulate problems.

*Dr. Willis Ware is with the Corporate Research Staff of the Rand Corporation, Santa Monica, California.

Any discussion of technology will always point out its rapid progress and the profound effect it is likely to have on society, especially when the technology in point is related in some way to information or data. Without question such advances will have a profound effect; the only thing one can argue about is the time scale over which it will occur. Will it be 25, 10, or only 5 years before things now readily possible in principle will become real? Why though is the certainty of the effect so evident?

First, information—which is a more comprehensive term than data—is the essence of purposeful behavior for every element of society. Information is an essential ingredient behind the behavior of organizations, in the functioning of physical mechanisms, and indeed in the basic biological structure of individuals and other life forms. Along with energy, information is the basis for the physical universe as we know it, for everything we appreciate about it, and for the behavior of society and its institutions.

Second, modern communication technology is the transportation mechanism that moves information from place to place and allows us to deliver it wherever wanted. In addition, modern digital computer technology allows us to manipulate information in very general ways, and it is important to note that digital computer technology is the only thing that mankind has which can process information faster than the human head. Together the two technologies allow us to do pretty much anything we wish with information; and to the extent that we do not yet know how to do some things, it is a matter of not yet intellectually understanding enough about the information processes in them. There is no basic lack of technology in the way for the most part.

Thus, the blend of communication and computer technology—what they jointly make possible—plus the universality of information as an element of nature, explains why technology is so central as an issue of concern to society at large, especially for privacy consequences, and why the impact of the two is so certain. Furthermore, the same facts explain why the world has made an irrevocable commitment to computer and communications technology. The days in which affairs could be conducted by paper and pencil under green eyeshades are forever gone; there is no way for the world to retreat from its commitment. Therefore, we as a society must deal with the consequences, one of which is privacy in one of its forms.

As the dialogue about informational privacy developed, one sometimes heard the view expressed that "I have nothing to hide; anyone is welcome to know anything about me." The opposite view is that "No one has an intrinsic right to know anything about me except for reason." It is to be observed that society generally does not publish vast encyclopedias concerning all there is to know about everyone; one must

therefore conclude that the "let it all hang out" philosophy does not really prevail. On the contrary, society generally controls access to information by many means, although it sometimes grants blanket access to some subset of society; for example, all physicians can access medical records, or the IRS as an organization has all tax information although within IRS access is controlled by job position. One must conclude that a basic axiom of informational or recordkeeping privacy is: "You may not know something about me without a justified (to me), or socially accepted, or legally sanctioned need-to-know."

Looked at that way, one could in principle reduce all of recordkeeping privacy to defining need-to-know for a category of information, plus establishing the authority under which the need-to-know functions. Such an approach is at best a way to deal with privacy when we recognize its presence, but it is not a very broad-gauge one. The "privacy pie" includes not only fair information policy, which is the way contemporary law approaches recordkeeping privacy, but it also includes aspects of social discrimination, aspects of national vulnerability, plus a broad collection of personal dimensions including physical proximity, surveillance of motion, risk of property, and others.

Philosophically, awkward moral and ethical issues arise when one seeks to define privacy, in part because the very word "privacy" connotes such diverse things to individuals. From a social point of view one might try to frame a broad construct for privacy in terms of equity by using the notions of equality of opportunity for individuals or arbitrary imposition of disadvantage on individuals. It would seem, however, that some very special connotation for "opportunity" or "disadvantage" would be necessary to develop such a theme, and consequently it seems an unsatisfactory direction. While it is desirable in the ultimate to have a good definition of privacy to keep its philosophical basis tidy, a more pressing concern is how to identify and define actionable aspects of privacy for the guidance of legislative and judicial affairs.

We—used as a collective pronoun—do not really know what privacy is in a comprehensive way, but any individual certainly believes that he knows it when he sees it. What is needed is a framework for recognizing a privacy infraction and deciding what to do about it when it occurs. So let us consider approaching the matter in reverse. Rather than trying to define "privacy," define instead "invasion of privacy" and develop an overall construct from that point of view.

Consider the notion of "space"—not in the context of extraterrestrial void, but rather in the context of personal surroundings. Intuitively, one knows what is meant by the term because it has been used frequently in contemporary psychological discussions. To illustrate, one's visual space is what is accessible to his eyes; one's aural space, what his ears catch. One's physical space is a cocoon of certain dimensions around a person; and psychological space, while more abstract and harder to define, has something to do with behavorial or perceptual things. Even more abstract is the notion of informational or recordkeeping space, but one's imagination can see a volume that includes all the records that concern one's life.

If one envisions a "space"—whatever kind it is—as a physical volume, then one can also envision an intrusion or entry into such a space. If there are negative or undesirable consequences of such an intrusion, they can be cataloged and separated into annoyances, those that constitute harm, and those that should be overlooked or ignored. The total effect of the harmful ones will constitute the definition of what "hurt" or "injury" or "damage" means for the space in question. In turn one can then decide how to legally deal with each space and its intrusions and further discover where legislative actions or judicial insights are needed.

Try some examples to validate the construct. First consider ones that might be called sensory spaces; the most obvious is visual space. It includes what the eyes see, and the most severe intrusion is probably blindfolding. Others include flashing bright lights, the display of objectionable material, or critical written attacks. Consequences of such intrusions include sensory deprivation, mental disorientation especially if the frequency and brightness of a flashing light is just right, annoyance, anger, or damage to reputation. Some of these consequences would be actionable under existing law perhaps even as an aggressive act. Under some circumstances intrusion of morally objectionable material before the eyes might be considered an invasion of privacy, whereas written things before the eyes might come under defamation law, but in this particular instance it would be different for a public official and perhaps not actionable.

Another of the sensory spaces would be the aural space which is the totality of what is heard by the ears. Typical intrusions would include loud stereo playing, casual conversation, excessive noise levels such as in a factory, the general background clamor of a city or factory, shouted remarks or obscenities. The consequences of intrusion of aural privacy would range from none through annoyance to physical damage or pain to psychological disturbances or anger. Some of them would be legally actionable as a public nuisance or as noise pollution; others would not be actionable, whereas some would fall under the purview of the Occupational Safety and Health Administration.

Intrusions into one's physical space would include standing close, sitting on the same bench, physical pressure in a crowd, touching and fondling, or the ultimate intrusion of bodily seizure or confinement. The consequences would range from annoyance to physical discomfort, to psychological malaise, to sexual approach or mortification, or to bodily harm. Some of these would be actionable under the laws of assault, sexual molestation, perhaps public nuisance, unlawful seizure or false imprisonment. Some of the physical intrusions might be spoken of as privacy invasion under some circumstances, e.g., when one individual sits down on another's parkbench; many intrusions will be categorized otherwise. Finally, with

respect to recordkeeping space, intrusions would include such things as misuse of information, improper dissemination of information, or collection of inappropriate facts. Consequences would include embarrassment, denial of credit, or destruction of reputation, among others. Generally, the privacy invasion of recordkeeping space is actionable under various federal and state laws.

While these examples certainly do not exhaust all possible dimensions of privacy in the general issue, the approach does seem to circumvent the ethical and moral hurdle by implicitly involving both in the process. This approach also seems to properly include the role of case law, but let us develop these last two points more fully.

In the suggested construct, namely of defining invasion of privacy rather than privacy itself, the first step would be to conceptualize or identify a space of concern. The second step would be to identify possible intrusions into the space; one should note that such a list could be amended as events occurred or became important to society. The third step would be to identify the consequences of such intrusions; here the moral and ethical views of society can be properly involved. Next, one would determine what "hurt" or "injury" or "damage" is for each of the intrusions or consequences; again, the moral and ethical views of society clearly would be at work. Also, the cumulative effect of case law would establish self-adapting definitions of the three as society changes, or as moral and ethical views evolve. The final step is then the question of legal actionability; clearly the overall judicial process and legislative attention would be folded in.

The validity of such a "backend-to" procedure is encapsulated in the following series of points.

- Rather than conceive a very broad definition of privacy that can umbrella all the many variations on the privacy theme,
- it concentrates on events and relates them to societal views, morals, and ethics as exemplified through the legislative and judicial processes.
- It is a phenomenological approach that concentrates on events rather than causation and thus,
- it tracks and reflects usage of technology rather than *a priori* proscribing acceptable boundaries for it.
- It can accept as part of the overall framework any legal actions that are appropriate to the hurt, e.g., recover damages, penalize the perpetrator, or enjoin the perpetrator.
- Furthermore, it can accommodate expressions of concern by society in behalf of individuals as well as individuals in behalf of themselves, or even society in behalf of its institutions and organizations.

Finally, the proposed construct—or taxonomy for privacy—might be used as an analytical framework for perceiving the privacy consequences of some new use of technology, or for identifying areas where legislative attention is needed. For this purpose one would decide what spaces some new service might intrude, imagine the intrusions and consequent hurts, and design safeguards or laws to protect against them. For example, a new service such as delivering many forms of information over the cable-TV network might invade visual, aural, recordkeeping, psychological and perhaps other spaces. In considering the privacy effect of some new technological application, one would have to stitch together the various dimensions of privacy invasion that the technology might impose, and perhaps each of them would have to be dealt with separately under law, judicial action, or social pressure and norms.

Here then is a possible way to consolidate and relate the many dimensions of privacy. It appears sound in terms of the examples given, but on the other hand, all of them have been in the context of an individual. There may need to be a somewhat different set of spaces and intrusions when considering all of society or organizations. There is no pretense that the task or producing a grand construct for privacy is completely finished. The totality of all intrusions into all spaces could be catalyzed under appropriate branches of law or under various specific categoric laws. From a philosophical point of view, one must ask about the various dimensions of hurt or injury. Should it, for example, include denial of right-of-action where such a right is presumed to be one of personal choice? Should it include negative impact, mortification, or shame? Existing privacy law could profitably be examined together with other pertinent law to see whether significant legislative gaps exists and, if so, whether attention is needed. If nothing more, the point of view offered in this paper is at least a different way to think about privacy.

Belatedly, one notes that in the proper context the famous words of Justice Brandeis still prevail: "Privacy . . . the right to be left alone." Now, however, "alone" must be interpreted to mean "alone in a physical sense," or "alone in a visual sense," or "alone in an aural sense," or "alone in a recordkeeping sense" or "alone in . . . ." It would appear that the words which really launched societal concern about privacy are still quite valid if only interpreted to mean: alone in the broadest sense. Even so, however, fuller amplification of Justice Brandeis' words would be necessary. What does "left alone" mean? Freedom, or perhaps protection, from intrusions other than those personally, socially, or legislatively sanctioned? What does "broadest sense" even mean? Perhaps the notion of a space—which is a concept borrowed from the physical sciences—together with an easily grasped idea of intrusions into a space, can usefully add scope and fullness to an insightful idea expressed many decades ago.