UIC Law Review

Volume 18 | Issue 4 Article 2

Summer 1985

Information Law Overview, 18 J. Marshall L. Rev. 815 (1985)

George B. Trubow

ARTICLES

INFORMATION LAW OVERVIEW

GEORGE B. TRUBOW*

One purpose of this article is to introduce readers to this symposium on information technology and privacy law of The John Marshall Law Review. In the future we plan to give an annual update of law and policy relevant to the topic area. Another purpose of the article is to provide a general background to what is called "information law," examining the new challenges to our legal system which result from the rapid advance of information and communications technology.

The Computer Revolution. When the first electronic digital computer became operational in 1945, there was probably no notion of what was in store for the future.[1] That first machine, dubbed Eniac, a 30 ton hulk of 18,000 vacuum tubes and miles of wire, filled a room 30 by 50 feet and consumed enough energy to support the needs of a small city. In terms of computing capacity, it could manage about the same amount of data as can today's hand-held calculators operating on the power of a nine volt battery.

The second generation of computers was spawned by the transistor, invented in 1948, which replaced the vacuum tube. These tiny electronic gadgets were comparatively inexpensive, small, and very reliable. As a result, computers decreased in size and cost but increased enormously in their capacity for information processing.

The third generation, which began in the 1950's, is identified with the development of integrated circuits on silicon chips. These finger-nail-size wafers house the circuits, switches, and other electronic devices that are the heart of the computer. This new technology permitted yet further reduction in the size and cost of computers while again expanding exponentially the capacity and speed of these amazing devices. The end is not yet in sight, however, as the United States and Japan are locked in competition to gain supremacy in the development of supercomputers, devices

* Professor of Law and Director, Center for Information Technology and Privacy Law, The John Marshall Law School.

1. *See* A. RALSON, ENCYCLOPEDIA OF COMPUTER SCIENCE (1976) (discussing history and development of computer technology).

whose speed, capacity, and competence will literally dwarf the accomplishments of today's remarkable technology.

The result of this computer revolution, in terms of personal information and privacy, is that technology makes it possible to store, manipulate, and retrieve information in quantity and quality never before contemplated. The hunger of government agencies and private enterprises for personal information appears to grow with the capacity of technology to store and disseminate the information. Advances in communications technology permit the query of data banks from remote terminals or other computers and for the comparison or merger of electronically stored personal data in separate data banks. Accordingly, it is increasingly the case that personal information is easily and widely available from credit or bank records, insurance or medical files, and a myriad of other governmental and private sources.

In addition to burgeoning data banks, electronic mail and bulletin board networks currently are counted by the thousands, and multiply in number each week. These devices, many of which are available to the public, permit any who join the network to communicate and share the information. Unauthorized individuals can penetrate even restricted information systems, and the phenomenon of the "computer hacker" has become commonplace.

Accordingly, issues of informational privacy arise with increasing frequency, and the capabilities of the technology present new questions in balancing the utility of sharing personal information against the value of individual privacy. It is the province of "information law" to examine governmental, social, and private interests in relation to the restriction and flow of information. This article will review generally the status of "informational privacy," the current law and regulations respecting privacy and information, and some of the major legal and policy issues that are not yet resolved. It seems likely that if we do not manage technology, then it will manage us.

THE DEVELOPMENT OF PRIVACY IN THE UNITED STATES

The notion of "privacy" as a legal concept did not reach the United States from England because privacy was not recognized in the common law.[2] Rather, Warren and Brandeis introduced the

2. The individual's privacy interest was first recognized as a constitutional right in Griswold v. Connecticut, 381 U.S. 479 (1965). In *Griswold*, the United States Supreme Court struck down a state law making it a crime for married couples to use contraceptives and for the Planned Parenthood League to give advice on such use. *Id.* The Court held that the state had invaded the plaintiff's privacy interest when the long arm of government reached into the marital chamber. *Id.*

idea into American jurisprudence in their famous 1890 law review article.[3] The primary concern of those gentlemen was that private information had become increasingly public. When they remarked, in reference to newspapers and photographs, that "numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the housetops . . ."[4] the electronic digital computer was not even an idea, let alone the incredible information processor that it has become. The frequent publication of private information, even at the turn of the century, was such as to cause the acceptance of the new legal concept of privacy. As those prescient authors noted, "[p]olitical, 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. . . ."[5] The law has grown and changed, though it remains inadequate to deal with the new challenges presented by ever-expanding technology. On the heels of microwave communications, satellites, robotics, and computers is the era of photonics—lasers, optic fibers, and other phenomena of light—which portends further change for information and communications technology. The law itself must expand and reshape itself to deal with these technological innovations.

DEFINITIONS

Before proceeding further, it will be helpful to explain the context in which certain words are used in this introduction.

Privacy is a characteristic of a natural person and, in informational terms, refers to what, how, and why information about an identifiable person is gathered. One's privacy is violated if personal information about him or her is collected or disclosed without lawful justification.

Confidentiality refers to the information itself, and means that only certain persons under specified circumstances are authorized to have access to particular information.

Security refers to information systems; information in a secure system is protected from unauthorized access, alteration, or loss. Security implements confidentiality which in turn protects privacy.

Personal information is any information that identifiably refers to an individual by name, number, or any other identifying characteristic. Information is personal not because of its content but because of its reference. Therefore, information which describes or is about a specific individual is considered personal.

3. Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
4. *Id.* at 195.
5. *Id.* at 193.

Whether information is confidential depends upon the law or policy restricting its collection, use, or storage. The degree to which information is secure depends upon the technology and procedures designed to enforce the confidentiality of that information.

THE CONTOURS OF PRIVACY IN TORT LAW

The word "privacy" has become rather common, though the context of its meaning varies widely. Dean Prosser added his own analysis[6] to Warren and Brandeis' initial exposition, and therefore modern American tort law generally recognizes the following species of privacy:

Intrusion into seclusion. Most instances of this tort have involved the physical entry into an area wherein the individual has a reasonable expectation of seclusion or solitude.[7] Examples of this privacy tort are the Peeping Tom[8] or the installation of a listening device in a bedroom.[9] This privacy tort has less relevance to information law than others, except to the extent that prying into confidential records, such as personal letters[10] or bank records,[11] has

6. Prosser, *Privacy*, 48 CALIF. L. REV. 389 (1960) (Dean Prosser organized privacy case law into four categories—appropriation, intrusion, false light, and embarrassing private facts). "[T]he law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff. . . ." *Id.* at 389. *See* W. PROSSER & W. KEETON, LAW OF TORTS § 117 (5th ed. 1984); RESTATEMENT (SECOND) OF TORTS § 652 (1977).

7. The Restatement (Second) of Torts defines intrusion into seclusion as:

> One, who intentionally intrudes physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

RESTATEMENT (SECOND) OF TORTS § 652B (1977).

8. Sounder v. Pendleton Detectives, Inc., 88 So. 2d 716 (La. App. 1956) (private detectives held liable for spying into plaintiff's windows); Moore v. New York Elevated Railroad Co., 130 N.Y. 523, 29 N.E. 997 (1892). *See* Ford Motor Co. v. Williams, 108 Ga. App. 21 (1963) (right of action accrues against "Peeping Tom" even if no one was present in the home at time of invasion). *See also* Note, *Crimination of Peeping Toms and other Men of Vision*, 5 ARK. L. REV. 388 (1951).

9. Birnbaum v. United States, 588 F.2d 319 (2d Cir.1978). *Contra* Lewis v. Dayton Hudson Corp., 128 Mich. App. 165, 339 N.W.2d 857 (1983) (privacy afforded to customer in fitting room of clothing store does not include freedom from overhead observation by security guard). *But see* People v. Abate, 105 Mich. App. 274, 306 N.W.2d 476 (1981) (two-way mirror over women's restroom at roller skating rink constituted invasion of privacy).

10. Hamberger v. Eastman, 106 N.H. 107, 206 A.2d 239 (1964). *See* Pearson v. Dodd, 410 F.2d 701 (D.C. Cir.) (intruders broke into plaintiff's office and took private information), *cert. denied*, 395 U.S. 94 (1969). *But see* N.O.C., Inc., v. Schaefer, No. L-14658-82 (N.J. Super. Ct. Law Div. May 14, 1984) (held not to be an invasion of privacy for defendant to keep a detailed diary of plaintiff's activities).

been recognized as a violation of this interest.

Appropriation of name or likeness for commercial purposes. This tort involves the commercial use of someone's notoriety or prestige without permission.[12] An unauthorized product endorsement attributed to a well-known person is a typical example of this tort.[13] This "privacy" tort is giving rise to a new interest called the "right of publicity" which has been recognized recently in the common law,[14] and statutorily in California.[15] The interest protected here seems to rest upon a "property" right in one's name or likeness.

Public disclosure of private facts. This incursion, the one that most bothered Warren and Brandeis, entails the publication of personal information that a reasonable person would consider objectionable.[16] The conflict here, of course, is between the individual,

---

11. *See, e.g.*, Zimmerman v. Wilson, 81 F.2d 247 (3d Cir. 1936) (unauthorized prying into private bank account); Burrows v. Superior Court of San Bernardino County, 13 Cal. 3d 238, 529 P.2d 590, 118 Cal. Rptr. 166 (1974) (reasonable expectation of privacy found where evidence resulting from unauthorized disclosure by bank of plaintiff's account was suppressed).

12. RESTATEMENT (SECOND) OF TORTS § 652C (1977). This was the first type of invasion of privacy recognized by the courts. *See, e.g.*, Flake v. Greensboro News Co., 212 N.C. 780, 195 S.E. 55 (1938) (unauthorized use of plaintiff's features and person in connection with advertisement). *See* Gordon, *Right of Property in Name, Likeness, Personality and History*, 55 NW. U.L. REV. 553 (1961).

13. *See* Olan Mills, Inc. v. Dodd, 234 Ark. 495, 353 S.W.2d 22 (1962) (picture appropriated); Brociner v. Radio Wire Television, 15 Misc. 2d 843, 183 N.Y.S.2d 743 (N.Y. Sup. Ct. 1959) (name appropriated); Young v. Greneker Studios, 175 Misc. 1027, 26 N.Y.S.2d 357 (N.Y. Sup. Ct. 1941) (person's likeness appropriated in form of a manikin).

14. Several courts describe the right of publicity as a property right; an exclusive license for the use of a name, called a "right of publicity," which entitles the licensee to enjoin its use by a third person. S. Haelan Lab. v. Topps Chewing Gum, 202 F.2d 866 (2d Cir. 1953). *See* Cepeda v. Swift & Co., 415 F.2d 1205 (8th Cir. 1969); Ettore v. Philco Television Broadcasting Corp., 229 F.2d 481 (3d Cir. 1956). *See also* Nimmer, *The Right of Publicity*, 19 LAW & CONTEMP. PROBS. 203 (1954).

> An individual claiming a violation of his right of publicity must show: (1) that his name or likeness has publicity value; (2) that he himself has "exploited" his name or likeness by acting "in such a way as to evidence his . . . own recognition of the extrinsic commercial value of his . . . name or likeness, and manifested that recognition in some overt manner"; and (3) that defendant has appropriated this right of publicity, without consent, for advertising purposes or for the purposes of trade.

Lerman v. Chuckleberry Pub. Co., 521 F. Supp. 228, 232 (S.D.N.Y. 1981) (citations omitted).

15. CAL. CIV. CODE § 3344(a) (West 1981) (statutory remedy for the knowing use, without consent, of another's name, photograph, or likeness for the purposes of advertising or solicitation of purchases). *See* Eastwood v. Superior Court for Los Angeles City, 149 Cal. App. 3d 418, 198 Cal. Rptr. 342 (2d Dist. 1983) (unauthorized use of celebrity's name in retail telecast advertisements and in connection with a published defamatory article constitutes actionable infringement of a person's right of publicity under civil code).

16. RESTATEMENT (SECOND) OF TORTS § 652D (1977). The required elements of a tortious invasion of privacy based on public disclosure of private facts

who considers the information to be no one else's business, and the public, who demands the "right to know."

"False light" publicity. This fourth privacy tort involves the portrayal of the individual to the public in a false and offensive manner.[17] Although it is difficult to define the precise interest protected here, self image is a likely focus for the tort[18] in that one's reputation seems to be at stake.[19] The "false light" projected need not be defamatory, though it must be objectionable to a reasonable person.[20]

The privacy tort of "false light," and the separate tort of defamation, involve the publication of *untrue* information. On the other hand, privacy invasions of private facts involve the publication of truthful information,[21] a tort which invites conflict with first amendment free speech rights.

PRIVACY AND THE UNITED STATES CONSTITUTION

Apart from common law tort, federal constitutional privacy questions have also emerged in the last twenty years. These issues, however, have involved what generally is referred to as "autonomy"—the right of the individual to make personal decisions with-

---

are: 1) a public disclosure, 2) a disclosure of private facts, and 3) a disclosure that is offensive and objectionable to a reasonable person of ordinary sensibilities. *See* Forsher v. Bugliosi, 26 Cal. 3d 792, 608 P.2d 716, 163 Cal. Rptr. 628 (1980).

The public's right to know is implied in the first amendment. Bloustein, *Privacy Tort Law and the Constitution: Is Warren and Brandeis' Tort Petty and Unconstitutional as Well?*, 46 TEX. L. REV. 611, 624 (1968) (The Meikeljoh theory on the first amendment provides that disclosure is not the press' right to speak, but the public's right to know).

17. RESTATEMENT (SECOND) OF TORTS § 652E (1977). A false privacy claim is different from a private facts claim in that (1) the matter published need not be private, (2) the plaintiff can be a public personage, and (3) the publication must be false or portray the plaintiff in a distorted light. Rinsley v. Brandt, 446 F. Supp. 850, 854 (D. Kan. 1977). *See* Adreani v. Hansen, 80 Ill. App. 3d 726, 400 N.E.2d 679 (1980) (plaintiffs accused of greed and disgraceful business practices in letter to editor); Bureau of Credit Control v. Scott, 36 Ill. App. 3d 1006, 345 N.E.2d 37 (1976) (plaintiff claimed that collection agency, by making phone calls to plaintiff at work, jeopardized her job).

18. The aspect of reputation closely allies the false light privacy claim to that of defamation. In fact, many suits contain causes of action for both libel and false light privacy. *See, e.g.*, Creisler v. Petrocelli, 616 F.2d 636 (2d Cir. 1980) (employee of publishing firm claimed she was portrayed in a novel as a transsexual); Torentz v. Westinghouse Elec. Corp., 472 F. Supp. 946 (W.D. Pa. 1979) (plaintiff named as a communist on radio call-in show).

19. False light invasions do not always carry reputational harm. A privacy violation does not depend upon the altered attitudes of other persons toward the plaintiff. It depends upon how the plaintiff is made to feel about himself. *See* Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 963, 1003 (1964).

20. W. PROSSER & W. KEETON, LAW OF TORTS § 117 (5th ed. 1984).

21. *See supra* note 16.

out government interference.[22] Informational privacy is rarely involved in these disputes, except perhaps for one's right to read obscene materials, or to be free from wiretapping. Professor Seng's article in this Symposium is an excellent discussion of constitutional privacy questions.[23]

WHAT IS INFORMATION LAW?

Presently, there is no discrete legal discipline called "information law." Though that may change in the future, the subject now involves a composite of legal concepts including torts, criminal law, contracts, personal and intellectual property, and statutory and constitutional concepts. Individual privacy, the public's "right to know," free speech and press, and state security interests have been increasingly in conflict as the courts, legislatures, and executive agencies try to sort the informational relationships between individuals, the private sector, government, and society as a whole.

To a large measure, the current emphasis on privacy and information has been the result of the much-vaunted "information revolution" occasioned by the development of the digital computer. A creation of the 40's, improved in the 60's, but a phenomenon of the 80's, the computer is having an incredibly pervasive national and international effect. The silicon chip and solid-state circuitry, which permit miniaturization, have increased performance and decreased costs, making possible the incredible growth of computer capability and availability. The microcomputer is coming to the forefront in this decade providing sophisticated computer power for anyone with a relatively small amount of capital and a bit of interest in this amazing technology.

A natural conflict often exists between those who want to receive information and those who want to sequester it; the desire seems to depend upon one's role or interest at the moment. For example, a newspaper reporter usually is interested in gathering information and disseminating everything he knows unless, of course, it happens to be information about a "confidential source," in which case the journalist desires to keep that source's identity securely hidden. Each of us wants information about others, yet we desire to keep information concerning ourselves private, except when self disclosure suits our purposes. The desire to control per-

22. *See generally* Henkin, *Privacy and Autonomy*, 74 COLUM. L. REV. 1410 (1974).

23. Seng, *The Constitution and Informational Privacy or How So-Called Conservatives Countenance Governmental Intrusion into a Person's Private Affairs*, 18 J. MAR. L. REV. 871 (1985).

sonal information may be the heart of privacy,[24] though surely it conflicts with public curiosity.

These conflicts of information interests abound in that each of us wears a variety of "hats," and the information relationships in connection with any particular role will vary. It is the domain of information law to examine these various interests and relationships and to seek a conceptual framework for the proper management of information. Without such guidance, information could become freely available without regard to personal privacy, state security, or business needs.

Fair Information Practices

Though it was Warren and Brandeis who sounded the early warning regarding privacy threats which result from the combination of curiosity and technology, others adopted the theme when the digital computer became prevalent. Arthur Miller complained about "The Assault on Privacy,"[25] and Alan Weinstein talked of "Privacy and Freedom."[26] Elliot Richardson, while Secretary of Health Education and Welfare, was also concerned about the mass of information maintained in his agency's files, thus prompting him to commission a special task force to consider the matter. The task force's 1973 report, entitled "Computers, Records and the Rights of Citizens,"[27] suggested "fair information practices" for dealing with personal information. These principles have become the conventional wisdom of privacy advocates, and can be summarized as follows:

1. Maintain no secret personal information systems. Some information may be *confidential* and available only to authorized persons, but the fact of its existence should not be a secret.

2. Collect only that personal information which has been authorized for a legal purpose. Often information may be gathered at

---

24. Without informational privacy,

> [t]he individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feeling of every man. Such a being, although sentient, is fungible; he is not an individual.

Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 1003 (1964).

25. A. MILLER, THE ASSAULT ON PRIVACY (1971) (concerned with governmental assaults on privacy for the sake of law enforcement and national security where nearly everyone has been reduced to a file).

26. A. WEINSTEIN, PRIVACY AND FREEDOM (1967) (every individual is unique and thus he must be able to determine for himself when, how, and to what extent information concerning him is communicated to others).

27. SECRETARY ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEPT. OF HEALTH, EDUCATION & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973) (OSHEW Publication No. (D)73-94).

the whim of record-keepers, and not because it is specifically required. The best way to protect informational privacy is to restrict the kind and amount of personal information that may be collected.

3. Be sure that information is accurate, timely, and complete. Incorrect information can be dangerous and stale, while fragmentary information can be misleading or useless.

4. Give the data subject access and review rights to information about himself. It is fair to let one know what personal information is being used to make decisions, and the data subject can help ensure information accuracy. While it is feasible that a data subject may want information about himself to be incorrect, audit procedures should be sufficient to validate information accuracy.

5. Use data only for the purposes for which it was collected. This prevents unnecessary surprises because information supplied for a specific purpose should not be given for some other reason.

6. Protect data against unauthorized use, loss, alteration, or disclosure. The integrity of valuable information should be safeguarded.

These principles are a good starting point regarding how personal information should be managed. There may be exceptions to these rules depending upon the special needs of a particular information system. For example, the data subject should not have the right, in the course of a criminal investigation, to view collected information pertaining to him and his case. These general principles are basically sound, however, and a convincing "show cause" should be required to negate compliance with them.

Freedom of Information

While informational privacy is a growing concern, so is the right of citizens to know what their government is doing. This latter interest led to the passage of freedom of information legislation, both at the federal and state levels.[28] Such regulations permit the public, upon request, to acquire information maintained in government files, subject to certain exceptions. The pressure to release government information, which presumably is everybodies' business, and to close down personal information in government files, which arguably is nobody's business except the data subject's, creates important conflicts which information policy must resolve.

28. *See infra* notes 26 & 39.

Federal Laws to Regulate Information

As interest in information and privacy has grown, Congress has passed laws to regulate some information practices. Here is a chronological list of the more significant legislation:

Freedom of Information Act (1966).[29] This act makes federal records, with some exceptions, available for public inspection and copying. One exception covers information that would constitute a "clearly unwarranted invasion of privacy"[30] if it was published. What this "clearly unwarranted invasion of privacy" standard means has been the subject of much litigation.[31]

Fair Credit Reporting Act (1970).[32] This legislation, the first to regulate information maintained in the private sector, requires credit investigation and reporting agencies to make files available to the data subjects for inspection and copying.

Crime Control Act of 1973.[33] This law requires states that had received federal funds for upgrading their criminal justice information systems to adopt privacy and security programs to protect and regulate information in those systems. Every state has such a program, established either by legislation, regulation, or both.[34]

Privacy Act of 1974.[35] This is the principle legislation Congress enacted to regulate personal information in federal data banks. The fair information practices discussed earlier have been incorporated into this Act, and Richard Ehlke's article in this Symposium is an excellent update and evaluation of the law.[36]

Family Education Rights and Privacy Act (1974).[37] Popularly

---

29. 5 U.S.C. § 552 (1976).

30. *Id.* at §§ 552(b)(6) (regarding personnel, medical, and similar files) & (b)(7)(C) (regarding investigatory records compiled for law enforcement purposes).

31. *See, e.g.*, New England Apple Council v. Donovan, 725 F.2d 139 (1st Cir. 1984) (government may withhold identities of law enforcement personnel only if disclosure would constitute unwarranted invasion of privacy, and court is required to balance competing interests at stake); Antonelli v. FBI, 721 F.2d 615 (7th Cir. 1983) (agency may refuse to confirm or deny existence of records proclaimed to be exempt as investigatory records, disclosure of which would constitute an unwarranted invasion of personal privacy if requester failed to identify general public interest in disclosure); Lame v. United States Dept. of Justice, 654 F.2d 917 (3d Cir. 1981) (privacy exemption does not prohibit all disclosures which invade personal privacy, but only disclosures which entail unwarranted invasions of privacy).

32. 15 U.S.C. § 1681 (1977).

33. 42 U.S.C. § 3789g (Supp. II 1980).

34. *See, e.g.*, Criminal Justice Information Act, ILL. REV. STAT. ch. 38, § 210-1 (1983) ("[t]he purpose of this Act is to coordinate the use of information in the criminal justice system; to promulgate effective criminal justice information policy . . . .").

35. 5 U.S.C. § 552a (1977).

36. Ehlke, *The Privacy Act After a Decade*, 18 J. MAR. L. REV. 829 (1985).

37. 20 U.S.C. § 1232g (1977).

known as the "Buckley Amendment," this law requires schools and colleges to give students (or their parents) certain rights to personal information, and sharply limits the disclosure of student records to third parties.

Right to Financial Privacy Act of 1978.[38] This law regulates the way in which federal agencies may gain access to bank records. The law does not deal with state agency or private party requests. This legislation was the Congressional response to *United States v. Miller*, wherein the Supreme Court held that the individual does not have privacy expectations concerning his bank records.[39]

Privacy Protection Act of 1980.[40] This law establishes the procedures for law enforcement agencies to acquire print media records. The Supreme Court's decision in *Zurcher v. Stanford Daily*, which permitted law enforcement access to a newspaper's files, gave rise to this legislation.[41]

Electronic Fund Transfer Act of 1980.[42] Though this legislation mandates no specific privacy protection, it requires each bank to notify its customers about routine third party disclosures of personal records.

State Regulation of Information

Many states have passed laws dealing with freedom of information and various aspects of informational privacy.[43] There is no uniformity or consistency among the states regarding what or how information should be regulated. Suffice it to say that the average person has virtually no informational privacy protection at the state level, though a variety of laws exist. Less than a dozen states have constitutional provisions protecting privacy, and where there are such provisions, the scope of protection has been narrow.[44]

---

38. 12 U.S.C. § 3401 (Supp. II 1978).

39. United States v. Miller, 425 U.S. 435 (1975). Legislative history shows that the Right to Financial Privacy Act was passed due to congressional disagreement with *Miller*. *See* H.R. Rep. No. 1383, 95th Cong. 2d Sess. 34 (1978).

40. 42 U.S.C. § 2000aa-11 (Supp. IV 1981).

41. Zurcher v. Stanford Daily, 436 U.S. 547 (1978) (student newspaper published articles and photographs of a clash between demonstrators and police at a hospital).

42. 15 U.S.C. § 1693 (Supp. III 1979).

43. *See, e.g.*, ILL. REV. STAT. ch. 116, § 201 (1984) ("[t]his act is not intended to be used to violate individual privacy . . ."). *See also id.* at § 207(b)(c)(v) (regarding exemptions for information that constitutes a clearly unwarranted invasion of personal privacy, specifically investigatory records).

44. Seng, *supra* note 23, at 889-91.

Privileged Communications

Privileged communications between individuals in certain relationships (spousal, attorney-client, doctor-patient, priest-confessor, etc.) are somewhat related to informational privacy.[45] Most of these questions are raised in connection with discovery of evidence in litigation, however, and do not actually regulate the general availability of this information to third parties in circumstances other than lawsuits. Privacy analogies may nonetheless be drawn from privileged communications because the law regards these communications as confidential between the parties and not subject to disclosure in litigation.

OPEN QUESTIONS FOR INFORMATION LAW

There are far many more unresolved questions in the informational privacy rights area than there are answers. As previously mentioned, one of the major tasks of this annual Symposium is to track developments in the area; another is to encourage dialogue that can help provide solutions. The Benton National Moot Court Competition in Information Technology and Privacy Law has addressed some of these questions in the past, and other issues will be topics for future competitions. The winning briefs from the 1984 competition appear in this Symposium, and it is planned that this practice will continue in the future.

Here is a list of a few of the perplexing and unresolved privacy questions that must be addressed and resolved in the future:

* To what extent are the fair information practices discussed above applicable to private individuals? These principles were developed with governmental agencies or certain regulated businesses in mind; can they govern the information practices of the individual working at home with his personal computer?

* Should informational privacy rights extend to artificial persons as well as natural individuals? In the United States, unlike European nations, only natural individuals enjoy privacy rights. Though corporations have protection for trade secrets, some important proprietary information may not meet trade secret standards, yet may be vital to the company's business interests.

* What harm can trigger an informational privacy claim? Must there be some tangible loss, or is the mere outrage of the individual, due to an unjustifiable disclosure of personal information,

45. *See, e.g.*, Canadian Javelin, Ltd. v. SEC, 501 F.Supp. 898 (D.D.C. 1980) (fundamental prerequisite for use of attorney-client privilege under 5 U.S.C. § 552 is confidentiality at decision-making level both at time of communication and subsequent thereto).

enough to support a cause of action? The old "special damages" tort law question is thus presented in a new context.

* If regulation of personal information is desirable, should it be accomplished by federal or state government? Some information relationships may be more amenable to regulation by one level of government than the other.

* Should specific federal or state agencies be charged with the duty to monitor informational privacy? In remembrance of George Orwell's "Big Brother," there is some aversion to an information "czar." Yet, how else can the interests of the individual be monitored and safeguarded?

* How can the public be assured of quality news media information practices in the face of the first amendment? Frequently, public figures and private individuals complain of overreaching press coverage into one's personal affairs. How do we distinguish between a legitimate public "right to know" and a prying curiosity regarding someone else's business?

* Should there be a national identification card? Though the subject has been discussed recently in connection with the identification of illegal aliens, it has other important privacy ramifications. For instance, a good way to assure that information does not find its way into the wrong file is through a unique personal identifier. The fear of "Big Brother" may overshadow this benefit, however, because such an identifier may be used with electronic data bases to match files or conduct surveillance.

* What should be the privacy protections for electronic mail? We know what to expect when mail is sent first class in an envelope, as opposed to open communications on a post card. How should communications be classified when they are transmitted from one computer to another in the business or home environment?

* What is the liability of the automated record-keeper who is subjected to unauthorized tampering? For instance, when a "hacker" breaks into a credit reporting company's computer files and changes information about a customer, can the record-keeper be liable for damages to the customer because the information was not protected from unauthorized access?

* What is the responsibility of one who operates an electronic bulletin board, a device which permits individuals to communicate with each other through telephonically accessible computers. Increasing instances of anonymous callers posting illicit, obscene, or defamatory information on such boards raise questions concerning the liability of the bulletin board operator.

Clearly, a challenging and important set of questions, both of law and policy, remains unresolved. Though the quality of life is undoubtedly improved through advances in information and communications technology, this should not require the sacrifice of personal privacy. We desire to contribute to the discussion of these issues in our annual symposium. We welcome your interest and participation. Join the dialogue, and help examine the problems.