VIDEOTEX: A WELCOME NEW TECHNOLOGY OR AN ORWELLIAN THREAT TO PRIVACY?

I. INTRODUCTION

The information distribution services of teletext[1] and videotex constitute an innovative mass medium which will shortly be available for consumer use. These systems, often described as electronic publishing,[2] have the potential to deliver new and valuable services to the public. Teletext and videotex, which disseminate verbal and pictorial information for display to the user, have the capacity to produce major changes in our daily lifestyle.[3] Their anticipated widespread use poses fundamental issues concerning the right of privacy.

This Note will examine the technology of electronic publishing, concentrating on the possible uses of the medium and the potential abuse of personal privacy. In order to understand fully the potential threat to privacy, this Note will explore the right of privacy as well as the principles underlying current privacy-based legislation which may be applicable to electronic publishing. The safeguards currently afforded consumers by means of industry codes and proposed and existing legislation will also be analyzed. The analysis will reveal the ineffectiveness of the majority of these safeguards in protecting informational privacy.

II. BACKGROUND—HOW THE SYSTEMS OPERATE

Teletext is a one-way system in which information is broadcast as part of a television signal.[4] Television consists of separate "scans" during which an electron beam flashes the picture on the screen sixty times a second. Between each scan there is a pause lasting a thousandth of a second. Teletext signals, transmitted on a continuous cycle, are inserted in the unused portion of the television signal. A teletext user simply pushes a button on his keypad to "grab" the page of information he wishes and transfer it to a visual image on his

---

[1] The term teletext, used in this discussion, is also called broadcast videotex, a process in which information is transmitted over the air. Teletex, not to be confused with teletext, is a computer-based information service provided by Radio Shack. Larratt, *Videotex for T.V.—How it Works*, RADIO ELECTRONICS, Dec. 1981, at 47.

[2] Rudell, *Entertainment Uses for Teletext, Videotext*, N.Y.L.J. July 22, 1982, at 1, col. 1. Teletext and Videotex utilize electronic means, such as microwave, cable television and broadcast signals to transmit information to an individual. *Id.*

[3] *Id.*

[4] Fantel, *Videotex to Expand What a T.V. Can Do*, N.Y. Times, Oct. 7, 1982, at C3, col. 1.

television. The signals are transferred to the television by a decoder attached to the television. The page or "frame," of information, such as airline schedules or supermarket prices, remains on the screen until the user pushes a button to gain access to another page or until he reverts to a regular television broadcast.[5]

Videotex is an interactive or two-way communication system. Utilizing ordinary telephone lines or cable, videotex enables a user to receive information and to respond to the screen.[6] The user would not only be able to see supermarket prices, but he would also be able to order goods with his credit card. A videotex subscriber may request information from a computer data base containing seventy five thousand to one hundred thousand "pages" of information, as opposed to the two hundred "pages" currently being used for teletext.[7]

The potential uses for these two systems are diverse. Videotex and teletext have the capability of providing numerous services, including publication, financial, teleshopping, message, entertainment, educational and home monitoring services.[8] These systems and their services are appealing because they are easy to use, accessible twenty four hours a day and rapidly provide the requested information.[9] Videotex[10] systems are currently being used in market tests[11] across the

---

[5] *Id.*

[6] The Lexis legal research system is an example of this system. Wiley & Neustadt, *Videotex Calls for New Legal, Regulatory Thinking*, Legal Times of Washington, July 6, 1981, at 11, col. 1.

[7] Rudell, *supra* note 2, at 2, col. 3.

[8] Publication service would provide news, financial, sports and congressional information. Financial services would enable a consumer to utilize market reports, accounting services and electronic banking. A user would enjoy the convenience of mail order merchandising, ticket and reservation services and comparative shopping information with teleshopping. Electronic mail, word processing and a community bulletin board are a few of the highlights of the message service. Included in entertainment service are video games and schedules of events. Educational services would provide instruction and drilling in school subjects. A monitoring service would establish remote home security devices to detect fire, smoke or intruders, as well as automatic control of home devices to maintain optimal energy efficiency. D. Collingwood Nash & J.B. Smith, *Interactive Home Media and Privacy Issues*, REPORT TO THE FEDERAL TRADE COMMISSION, OFFICE OF POLICY PLANNING, at 20 (January 15, 1981). Of these potential uses, the most popular use of teletext will be information retrieval. Videotex is likely to become important in the area of information retrieval, computer games and transactions, including shopping and banking. Tydeman, *Videotex: Ushering in the Electronic Household*, THE FUTURIST, Feb. 1982, at 57.

[9] Sigel, *The Year of Living Dangerously: Videotex*, 9 PRIVACY J. 6 (June 1983).

[10] The term "videotex" is used here as a generic term to include one-way and two-way communication systems.

[11] Most of the tests supply news, weather and sports information. New York's Chemical Bank offers Pronto, a system which has advanced beyond the test stage and is now marketed statewide. Pronto enables a bank customer to check his bank balance, move funds from one account to another and directly transfer funds to pay any of the 400 participating merchants. Although the

United States[12] predominately supplying news, weather and sports information.[13]

Videotex subscribers currently use television sets to receive information. Such use has hampered the growth of the technology because the televisions produce blurred images. However, this problem will be alleviated as consumers replace their television sets with video components designed specifically for the system.[14] Another problem hampering the videotex explosion is the incompatability of the various systems being used which limits the amount of information available to a consumer.[15] In addition, consumers are not investing in the systems as they are unsure which system is preferable. Moreover, information providers are not spending the money necessary to create data bases until they can be certain there will be customers to take advantage of their services. Despite these obstacles, however, mass marketing for the public should be available within a year or two.[16] Consequently, it is expected that some form of videotex will be used by ten to fifteen percent of all American households in the year 1990, and by thirty to

---

system automatically balances a checkbook, it does not allow for deposits or withdrawals. Another marketed system is Viewtron, provided by Knight Ridder. Viewtron recently introduced teleshopping and telebanking services as well as games and movie reviews to Florida residents. The majority of videotex systems, however, have not progressed beyond the test pilot stage. Quinn, *Banking by Computer*, NEWSWEEK, Nov. 21, 1983, at 85. Times-Mirror Cable and Comp-U-Card jointly provide the Los Angeles vicinity with an at-home buying service, which currently enables consumers to purchase a variety of merchandise, including theater tickets. This system will soon provide information as to airline seat availability and location, enabling consumers to book their own seats. Participants in Columbus, Ohio were able to request a desired book from the card catalog of the Columbus library system and receive the book in the mail. A test in Coral Gables, Florida featured a community bulletin board. In Ridgewood, New Jersey, CBS and A.T.&T. are presently testing videotex to two hundred viewers, with the New York Times participating as one of the information providers. Tydeman, *supra* note 8, at 55-57; Fantel, *supra* note 4.

The "information provider" is the company which supplies the videotex system with the pages of information. The "system provider" is the company which supplies the videotex terminals and operates the videotex services. *See Window on the World: The Home Information Revolution*, BUSINESS WEEK, June 29, 1982, at 77. *See also* Sigel, *supra* note 9, at 5.

[12] Tydeman, *supra* note 8, at 55. Similar interactive home media systems are being tested or marketed in other countries, including: Antiope (France), Captain (Japan), Prestel (Britain) and Telidon (Canada). Neustadt, Skall & Hammer, *The Regulation of Electronic Publishing*, 33 FED. COMM. L.J. 331, 342. (Summer 1981).

[13] The provided information is available from such varied industries as wire services, newspapers, publishers, retail stores, advertising agencies and entertainment corporations. Nash & Smith, *supra* note 8, at 61.

[14] Fantel, *supra* note 4.

[15] Wiley & Neustadt, *supra* note 6, at 11.

[16] *Id.* As the market becomes saturated with these systems, the current price of two hundred dollars for a television decoder and adapter, which is not yet commercially available, is likely to drop.

Fantel, *supra* note 4, at 3; Neustadt, Skall & Hammer, *supra* note 12, at 337-38.

forty percent of the households in the year 2000. These percentages are significant since projections indicate that there will be over one hundred million households in the United States by the year 2000.[17]

III. The Potential Abuses of Videotex

Once the videotex explosion occurs and there is widespread public use of interactive home media systems, system operators will be collecting massive amounts of personal data from subscribers.[18] Whether the subscriber is ordering goods and services, answering inquiries, retrieving information or utilizing the security service, he will be conveying his interests, choices and views to the central computer. A home profile would thus be available simply by collating personal information about checking and charge account expenditures, magazine subscriptions, health conditions, contributions made to charitable organizations, viewing of sexually oriented films and the hours an owner leaves his home and turns on his security system.[19] To the extent that detailed personal records of family data will be available, there is a potential for abuse and violation of an individual's right to privacy.

The potential threat to privacy involves four types of exposure: intrusion, interception, misuse of information and aggregation by household.[20]

A. *Intrusion*

Intrusion is possible with those videotex systems offering home security devices.[21] Warner Amex's Qube System provides such a service. The system detects fire, smoke, sound and movement and moni-

---

[17] Pace, *Videotex in Years to Come*, N.Y. Times, Sept. 1, 1982, at D15, col. 5; Tydeman, *supra* note 8, at 57.

[18] Teletext systems are one-way systems, therefore the aggregation of personal information poses no threat to privacy. However, in one teletext test, the terminals were equipped with meters to record responses in order to evaluate the project. Privacy of records could become an issue if teletext systems were to utilize such meters to include itemizations for billing policies. Nash & Smith, *supra* note 8, at 82. Because privacy of records in teletext systems is not an issue at present, this Note will analyze the privacy threat as it exists solely in the context of videotex.

[19] Westin, *Home Information Systems: The Privacy Debate*, Datamation, July 1982, at 103. This information is given to the information provider by the system provider, in order to fill subscriber orders. The system provider does not keep a record of specific frames selected by a subscriber; it merely keeps an accounting of the incurred charges. Therefore, the danger of a home profile collation exists vis-a-vis the information provider. Nash & Smith, *supra* note 8, at 71, 84.

[20] *Id.* at 6.

[21] *Id.*

tors energy load. This is done by scanning the household every six seconds while recording such information as whether the television is on, what channel is being viewed, and which was the last response button pressed. A utility company may use information concerning a consumer's energy load not only to regulate heat at the user's request, but also to develop energy policies that affect the household.[22]

Another form of intrusion involves the undesired reception of obscene, unwanted or objectionable material.[23] It may be impossible to prevent this unwanted information from being received in the home.[24] Political or moral objections may, therefore, increase since videotex would provide accessibility to such objectionable matter.[25]

B. *Interception*

Interception involves unauthorized access or eavesdropping on private communication to the "head-end."[26] This could occur at several points. Interception may first occur by a third computer diverting the communication between the television or home console and the head-end computer. When a subscriber sends a message to the head-end computer, the message and the code number identifying the user terminal pass through the first "bridge gate controller"[27] and into the system. Once the message passes this first bridge gate controller, it is free from the possibility of diversion. However, before this point, there are as many as 256 terminals that potentially could pick up a signal. The signal would be weak, but it would flow back downstream

---

[22] *Id.*

[23] The system providers do not control the contents of the information. This is the responsibility of the information providers who have discretion to determine obscenity according to their own standards. *Id.* at 80.

[24] This problem is not unique to videotex. Such intrusion of unwanted programs likewise occurs in other media, including over-the-air broadcasting and one-way cable systems. *Id.* at 7. The Qube system provides subscribers with two alternative safeguards to prevent exposure to unwanted material. The subscriber may entirely block the reception of the sexually-oriented "adult" channel, or he may have a special lock-key terminal to prevent children from viewing this channel. Nash & Smith, *supra* note 8, at 47. A law will shortly take effect in the State of New York which will require every cable television company to offer each subscriber a locking device to control reception of programs. The device must be specifically requested by the subscriber and there is a ceiling on the price that the company may charge for the device. N.Y. EXEC. LAW § 829a (1983).

[25] Nash & Bollier, *Protecting Privacy in the Age of Hometech*, TECHNOLOGY REVIEW, Aug.-Sept. 1981, at 68.

[26] Head-end is the central cable company. *Id.*

[27] The bridge gate controller is the device in an interactive T.V. cable transmission system that permits messages to go upstream as well as downstream. Nash & Smith, *supra* note 8, at 112.

to the other terminals. Normally, terminals are designed to ignore such signals. However, a terminal could be designed specifically for such interception.[28] Although it would be both difficult and expensive to develop such a terminal, the range and potential application of available information may justify its design.[29] A scrambler could eliminate this problem, but since this is only a potential threat, it is unclear how much protection would be needed and who should pay for it.[30]

Interception may also occur at the head-end computer through either unauthorized tapping into the data or an improper communications link.[31] The Qube system has developed security techniques to

---

[28] *Id.* at 7, 49. Currently, there are two federal laws protecting personal communications. However, these statutes were written before such technological advancements as videotex. Consequently, interception of videotex may fall outside the scope of these statutes. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 mandates criminal sanctions against interception of wire communications and regulates wiretapping by law enforcement officials. However, "intercept" is defined within Title III as the "aural acquisition of the contents of any wire or oral communication," 18 U.S.C. § 2510(4) (1982), and it is doubtful that videotex would fall within the term "aural." Moreover, "wire communications," as defined by this law, involves transmission provided by a common carrier, 18 U.S.C. § 2510(1) (1982), and cable television is not considered a common carrier. Neustadt, Skall & Hammer, *supra* note 12, at 405-06.

Section 605 of the Communications Act, 47 U.S.C. § 605 (1976), prohibits unauthorized interception of signals. However, this act is limited to over-the-air-services and would not include videotex. *Id.* at 406.

[29] Nash & Smith, *supra* note 8, at 49.

[30] *Id.* at 48. Although this potential problem exists because of inherent flaws in the computer systems, it is unlikely that the system providers would pay for such safeguards. It is more likely that the subscriber would pay for additional safeguards. *See supra* note 24, and *infra* text accompanying notes 173-76.

[31] Nash & Smith, *supra* note 8, at 51. A recent episode in Milwaukee has demonstrated the vulnerability of computers to unauthorized interception. A group of teenagers gained access to more than sixty business and government computer systems, including those at the nuclear weapons facility at Los Alamos, New Mexico, Manhattan's Sloan-Kettering Cancer Center and a bank in Los Angeles. There is no specific federal law prohibiting unauthorized entry into computers under which these teenagers may be prosecuted. The Wisconsin law which provides a criminal penalty for unauthorized entry into computers has no effect on access gained to computers outside the state.

The number of computer raiders, or hackers as they are called, is estimated to be in the thousands. Gaining access to a computer requires a home computer, a device called a modem which controls the transmittal of computer data over telephone lines and some degree of computer skills. Hacking, which is considered a challenging game by its participants, is estimated to cause as much as $300 million annually in losses in the United States. Unauthorized computer access has flourished due to the growth of nationwide data networks, the low level of security at computer centers, the widespread use of home computers and the increasing expertise of computer users. In view of the computer caper in Milwaukee and the disclosure of widespread hacking across the country, there is a growing need for the enactment of a federal law prohibiting such computer penetration. *Hundreds of Youths Trading Data on Computer Break-Ins*, N.Y. Times, Sept. 5, 1983, at A1, col. 2; *Rising Use of Computer Networks Raise Issues of Security*

protect against unauthorized access by personnel within the head-end facility.[32] There is an elaborate system of physical locks, double computer passwords known only to authorized system operators, and triple computer passwords which are changed daily. In addition, only a few authorized operators possess the expertise needed to conduct viewer polls. To protect against improper access through a remote terminal hooked up to the system, Qube developed a patchboard through which all external telephone communications must be routed. The operators, who must manually link all terminal connections to the system, are instructed to make the connections only to known and approved individuals.[33]

Of even greater concern than such security failures is the possibility of legal access to data by an external agency, such as a subpoena by a judicial source.[34] Telephone toll records, credit card receipts, bank records and other data on individuals kept in organizational files have been obtained for law enforcement investigations, legislative hearings and judicial proceedings.[35] Therefore, it is conceivable that the government would seek similar information from videotex system operators when the information is considered relevant to an investigation or prosecution.[36]

For example, in 1980, in Columbus, Ohio, a local movie-house operator was arrested for showing two obscene movies, one of which was shown on Qube's pay adult channel.[37] The defense attorney, claiming that the films did not violate community standards of ob-

---

and Law, N.Y. Times, Aug. 26, 1983, at A1, col. 3; *Trial and Error by Intruders Led to Entry Into Computers*, N.Y. Times, Aug. 23, 1983, at A1, col. 5.

[32] Nash & Smith, *supra* note 8, at 51.

[33] *Id.*

[34] Nash & Bollier, *supra* note 25, at 70.

[35] One airline company estimated that ten to fifteen investigators a day (federal, state, local and other) gain access to the airline's computer in order to obtain information concerning a traveler. The computer divulges such data as the flights traveled by an individual, seat number, time of flight, telephone contact and hotel reservations. An investigator may also receive a printout of the entire passenger list of a specified flight to learn who may be the traveling companion of an individual.

Similarly, a federal law enforcement agency, in its investigations, may seek the help of the Post Office Department, which utilizes a procedure known as "mail cover" operations. A mail cover consists of mechanically scanning a piece of mail and recording the name and address of the sender, the date and place of the postmark and the class of the mail. This procedure, which reveals correspondence and possible suspect relationships between individuals, is only used when the information may be instrumental in solving a crime. A. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS AND DOSSIERS 42-44 (1971).

[36] Westin, *supra* note 19, at 103.

[37] Nash & Smith, *supra* note 8, at 52-57.

scenity, subpoenaed Qube's records to demonstrate the widespread appeal of such films. Although Qube supplied general viewing statistics concerning the particular film and the patterns of the adult channel, the system provider asserted it would go to the Supreme Court before it gave access to its individual records. It is questionable how other interactive home media corporations would react in a similar situation.[38]

C. *Misuse of Information*

Misuse of information involves the use of personal information without the subscriber's knowledge or consent for commercial purposes. Videotex systems provide three types of information which are susceptible to exposure: viewing choices, viewer responses and security information.[39] Release of such information could not only be damaging or embarrassing,[40] but more importantly, a viewer's selection patterns may be misused. For example, just as library circulation records were used as incriminating evidence during the McCarthy era, television and movie selection records could be similarly misused.[41] Home security devices used to detect intruders could be used to monitor the subscriber's movements. Insurance companies could use personal medical information to raise risk factors and premiums.[42] Moreover, misuse of information would infringe upon the important privacy concept of an individual's right to control the use and accuracy of information.[43]

---

[38] *Id.*

[39] Nash & Bollier, *supra* note 25, at 70.

[40] There are many documented instances illustrating the threat posed to individuals by modern information-gathering practices. For example, an individual was entitled to damages where his insurance policy was cancelled on the basis of unverified reports that the insured was a "hippy-type," had participated in demonstrations and was a suspected drug user. Millstone v. O'Hanlon Reports, Inc. 383 F. Supp. 269 (E.D.Mo. 1974), *aff'd*, 528 F.2d 829 (8th Cir. 1976). In addition, an individual sought expungement of his arrest record which he believed would impede his employment opportunities where the arrest was made without probable cause. Menard v. Mitchell, 328 F. Supp. 718 (D.D.C. 1971), *rev'd sub. nom. on other grounds*, Menard v. Saxbe, 498 F.2d 1017 (D.C. Cir. 1974).

[41] Nash & Smith, *supra* note 8, at 48.

[42] Nash & Bollier, *supra* note 25, at 70.

[43] *See infra* text accompanying notes 79-83. *See also* Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICHIGAN L. REV. 1089, 1114-1119 (1969).

The use of electronic funds transfer[44] (EFT) presents another area for abuse.[45] EFT records would reveal a subscriber's daily purchases, expenditures, preferred products, merchants patronized, charitable or religious contributions and travel habits. Although EFT records would be enormously beneficial to law enforcement officials in monitoring cash flow and combating corruption and organized crime, there is little assurance that the privacy of ordinary individuals would be properly protected in view of past abuse of wiretap surveillance.[46]

D. *Aggregation of Data*

Aggregation of data by household constitutes the fourth area of informational abuse.[47] Data which may be insignificant when isolated can be damaging when compiled.[48] Furthermore, a character profile of a person, household or group may be assembled from personal information stored in the computer.[49] These "psychographic" profiles developed from viewer program or purchase choices could then be used to devise marketing strategies to which members of the household would be particularly vulnerable.[50] Advertisers, direct-mail marketers and cable television operators are already exploring ways to gather demographic data on cable viewers and to identify audiences.[51] The temptation for cable television companies to sell personal data to third parties would undoubtedly increase as the use of interactive

---

[44] Electronic funds transfer would incorporate banking and billing into videotex systems. Nash & Bollier, *supra* note 25, at 70.

[45] *Id.*

[46] *Id. See* United States v. Donovan, 429 U.S. 413 (1977), where government agents failed to identify in a wiretap application those individuals whose communications they expected to intercept. Similarly, in United States v. George, 465 F.2d 772 (6th Cir. 1972), government agents failed to comply with limitations contained in an order authorizing interception of telephone calls.

[47] Nash & Smith, *supra* note 8, at 8-9.

[48] *Id.*

[49] The compilation of personal information is not unique to videotex. Dossiers are compiled and maintained on individuals who apply for credit, insurance, medical care or employment benefits. Private, as well as government agencies use such dossiers extensively. *See* A. WESTIN, PRIVACY AND FREEDOM 158-61 (1967).

[50] Nash & Smith, *supra* note 8, at 8-9. For instance, a New Jersey firm has developed a data bank on doctors so that drug companies can promote their products in a manner most appealing to doctors. A. MILLER, *supra* note 35, at 43. Profiles developed from videotex responses will easily provide companies with similar relevant data.

[51] The four major rating firms, Nielsen, Arbitron, Gallup and Media Statistics, are viewing cable television as a source of new business. If consumers are able to order merchandise immediately after seeing an advertisement, the effectiveness of the commercial will be evident. Nash & Bollier, *supra* note 25, at 70, 72.

home media expands.[52] In addition, aggregated information could be used by a parent corporation, possibly giving an unfair competitive advantage in an unrelated area.[53]

These four areas of possible threats to privacy, although not exhaustive of potential informational abuses, reflect a growing concern in today's technologically expanding world. Inasmuch as interactive home media services are expected to grow significantly, the privacy issues may soon become a fearsome reality. In anticipation of the videotex revolution, it is essential to understand the consequences of these threats to privacy on potential subscribers. An historical analysis of the right to privacy is necessary to comprehend the ramifications of this impending technological explosion.

IV. The Right of Privacy

The concept that privacy is an interest that should be protected by law was first developed in an 1890 article by Samuel Warren and Louis Brandeis.[54] The article was written in response to the increasing use of the telephone, microphone, camera and other contemporary technological developments that threatened an individual's right "to be let alone."[55] Warren and Brandeis argued that individuals could be protected from these new technologies under the common law which secured "to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[56] The courts gradually adopted this theory, and today the right of privacy is established in the common law of most states.[57]

The common law tort of invasion of privacy is generally recognized as falling within four categories: intrusion upon an individual's seclusion or solitude; public disclosure of embarrassing facts; putting

---

[52] *Id.* at 70.

[53] In 1980, Warner Communications Corp. sold half of its interest in the Qube system to American Express Co. and formed Warner Amex Cable Communications, Inc. The Warner Amex entity has subsidiary corporations in such fields as book and magazine publishing, direct-mail marketing, insurance, finance and travel services, home computer sales and credit card services, among others. Considering the diversity and enormity of the Warner Amex corporate structure, it is not difficult to comprehend the usefulness of aggregated data obtained through interactive home media systems. Smith, *One Perspective on Warner Amex Cable*, 9 Privacy J. 3-6 (Feb. 1983).

[54] Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

[55] Cooley, Torts 29 (2d ed. 1888), quoted in Warren & Brandeis, *id.* at 195.

[56] Warren & Brandeis, *supra* note 54, at 198 (footnote omitted).

[57] W. Prosser, J. Wade & V. Schwartz, Cases & Materials on Torts 1058 (6th ed. 1976).

the plaintiff in a false light in the public eye; and appropriation of the plaintiff's name or likeness for commercial purposes.[58]

Although not specifically mentioned in the United States Constitution, a constitutional right of privacy has been inferred. In *Griswold v. Connecticut*,[59] the Supreme Court held that a state prohibition on birth control counseling violated this right. Justice Douglas, writing for the Court, held that the specific guarantees of the first, third, fourth, fifth and ninth amendments created penumbras or "zones of privacy."[60] Together these penumbras create a positive constitutional right of privacy entitling an individual to make personal choices and decisions without fear of governmental intervention.[61]

Subsequent cases elaborated upon this concept. Privacy was found to include the right to distribute contraceptives to unmarried couples[62] and the right to have an abortion.[63] However, the Court has generally limited the doctrine to issues concerning marriage, procreation, contraception, family relationships, child rearing and education.[64]

Despite limitations on the right of privacy doctrine, the Supreme Court has persistently linked the concept of privacy to the fourth amendment ban on unreasonable searches and seizures.[65] In the landmark decision of *Katz v. United States*,[66] the Court based the fourth amendment decision[67] on an individual's reasonable expectation of

---

[58] Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960). In this article Prosser first analyzed the tort of invasion of privacy and categorized it into four areas. *See* RESTATEMENT (SECOND) OF TORTS (1976).

[59] 381 U.S. 479 (1965).

[60] *Id.* at 484.

[61] *Id.* at 484-85.

[62] Eisenstadt v. Baird, 405 U.S. 438 (1972). "If the right of privacy means anything, it is the right of the *individual*, married or single to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child." *Id.* at 453.

[63] Roe v. Wade, 410 U.S. 113, *reh'g denied*, 410 U.S. 959 (1973).

[64] Carey v. Population Servs. Int'l, 431 U.S. 678, 684-85 (1977).

[65] Clark, *Constitutional Sources of the Penumbral Right to Privacy*, 19 VILL. L. REV. 833, 856 (1974). This was first articulated in Boyd v. United States, 116 U.S. 616 (1886), where a section of the Federal Customs Revenue Act of 1874 was held to be an unconstitutional violation of the fourth and fifth amendments. The statute authorized a court to require a defendant in revenue cases to produce specified papers and invoices. Failure to produce these papers would have resulted in an affirmation of the allegations. Clark, *supra*, at 857.

[66] 389 U.S. 347 (1967). The Court held that the government's activities in electronically listening to and recording an individual's words spoken into a telephone receiver in a public telephone booth violated the privacy upon which the individual justifiably relied.

[67] The Supreme Court held that an individual's fourth amendment rights were violated when his conversation in a public telephone booth were electronically listened to and recorded

privacy. The Court held that what a person knowingly exposes to the public, even in his own home or office, is not the subject of protection, "[b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[68]

The Supreme Court has been unwilling to extend the constitutional right of privacy to include an individual's interest in preserving the confidentiality of personal information which he has disclosed or which has been collected by others without his knowledge.[69] In *United States v. Miller*,[70] the Supreme Court rejected a fourth amendment challenge to the Bank Secrecy Act[71] which required recordkeeping of all bank transactions. The Court refused to extend its notion of privacy to protect this personal information from being subpoenaed by the government. The underlying rationale was that the documents were negotiable instruments, containing information voluntarily conveyed during the ordinary course of business. The Court failed to find a legitimate expectation of privacy in the deposit slips, checks and other transactional records,[72] and emphasized that when a person voluntarily conveys information to another, he takes the risk that this information may then be conveyed to the government.[73]

Similarly, in *Whalen v. Roe*[74] a New York statute that established a state computer file of individuals receiving certain prescription drugs was upheld. The Court refused to hold that such a file would invade an individual's privacy due to the extensive and adequate

---

by the government, even though there was no physical trespass of the area. This decision therefore overruled Olmstead v. United States, 277 U.S. 438 (1928) which required physical trespass for a fourth amendment violation. 389 U.S. at 353.

[68] *Id.* at 351-52. Justice Harlan, in his concurring opinion, created a two-pronged test for determining whether a person is entitled to fourth amendment protection for a particular situation. Harlan's test requires, first, that a person exhibit a subjective expectation of privacy, and second, that the expectation be one that society is prepared to accept as reasonable. Harlan found that there was a reasonable expectation of privacy in an enclosed telephone booth. *Id.* at 361 (Harlan, J., concurring). Similarly, it is arguable that when an individual sits in the privacy of his own home and relates confidential information, such as financial or medical data, he has a reasonable expectation of privacy from governmental intrusion.

[69] Comment, *The Use and Abuse of Computerized Information: Striking a Balance Between Personal Privacy Interests and Organizational Information Needs*, 44 ALBANY L. REV. 589, 595 (1980).

[70] 425 U.S. 435 (1976).

[71] 12 U.S.C. § 1829b(d) (1976).

[72] 425 U.S. at 442. The Court utilized the reasonable expectation of privacy analysis developed in Katz. *See supra* notes 66-68 and accompanying text.

[73] 425 U.S. at 443. The Miller decision was statutorily overruled by the provisions of the Right of Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (1982) which now protects the records of financial institutions from governmental intrusion.

[74] 429 U.S. 589 (1977).

safeguards written into the statute.[75] However, Justice Stevens, writing for the Court, did take note of the potential threat imposed by the storage of information:

> A final word about issues we have not decided. We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. . . . We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional—or by a system that did not contain comparable security provisions.[76]

Justice Brennan, concurring, emphasized that the records were available to a limited number of officials and that there were numerous safeguards protecting confidentiality.[77] In noting the potential danger involved, Justice Brennan commented: "The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology."[78]

Although the Court has refused to extend the constitutional right of privacy to protect personal data, the dicta of Justice Stevens and Justice Brennan in *Whalen* reveals an awareness of the dangers in-

---

[75] The New York statute requires that the prescriptions for the specified drugs be prepared by the physician in triplicate on an official form. A copy of the form is to be retained by the physician, the second by the dispensing pharmacist and the third is to be sent to the New York State Department of Health in Albany. The Department of Health records the data contained in the form on magnetic tapes for processing by a computer. These computer tapes are kept in a locked cabinet. When the tapes are used, the computer is run "off-line" so that no outside terminal can intercept the data. The forms are retained in a vault for five years and then they are destroyed. The vault is located in a room surrounded by a locked wire fence and is protected by an alarm system. *Id.* at 593-94. It is questionable whether the Court would have found that there had been no invasion of privacy if the statute had failed to provide such extensive safeguards.

[76] *Id.* at 605-06.

[77] *Id.* at 606-07 (Brennan, J., concurring).

[78] *Id.* at 607.

volved. Moreover, scholars are currently defining privacy in terms of personal information. Privacy is "the *control* we have over information about ourselves."[79] It has also been defined as "an autonomy or control over the intimacies of personal identity."[80] One commentator noted that "[p]rivacy is a limitation of others' access to an individual. . . . A loss of privacy occurs as others obtain information about an individual, pay attention to him, or gain access to him."[81] The right of privacy has been referred to as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[82] The latter definition requires that the individual have the right to limit the nature and extent of data aggregated, a right to insure the accuracy of the records maintained and a right of confidentiality in the information collected.[83] These new definitions of privacy indicate that although the Court has failed to adequately respond to the threats imposed by modern technology,[84] scholars recognize the need to expand an existing legal concept to accommodate contemporary society.

Notwithstanding the Court's reluctance to expand the right to privacy, Congress has enacted several federal privacy-related laws since 1966.[85] In particular, Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[86] and the Privacy Act of 1974[87] are

---

[79] Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968).

[80] Gerety, *Redefining Privacy*, 12(2) HARV. C.R.-C.L. L. REV. 233, 236 (Spring 1977).

[81] Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 428 (Jan. 1980).

[82] A. WESTIN, *supra* note 49, at 7. *See e.g.*, A. MILLER, *supra* note 35, at 25.

[83] Comment, *supra* note 69, at 600-02.

[84] Nash & Smith, *supra* note 8, at 28.

[85] The Fair Credit Reporting Act, 15 U.S.C. § 1681a-1681t (1982), mandates that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce by providing credit information in a manner that is fair and equitable to the consumer while regarding the confidentiality, accuracy, relevancy and proper utilization of the information. The Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (1976 and Supp. V. 1981), provides a scheme to regulate the information practices of federally funded educational institutions. The statute provides for fair practices in the collection of data, access by parents and students of majority age to the student's educational records and dissemination of personally identifiable information. The Freedom of Information Act, 5 U.S.C. § 552 (1982), gives every person the right to look at government records, except for certain exempt areas, such as classified information concerning national defense or foreign policy. Only the Fair Credit Reporting Act attempts to regulate the information practices of private business. The Freedom of Information Act and the Family Educational Rights and Privacy Act are efforts to limit the possibility of informational abuse by governmental agencies. However, these statutes are significant inasmuch as they indicate Congress' recognition of the need to regulate the collection of data. At present, videotex subscribers will have to rely on the enactment of statutes to protect the privacy of their data in view of the fact that the courts have not recognized the right of informational privacy. *See* Nash & Bollier, *supra* note 25, at 73.

[86] 18 U.S.C. §§ 2510-2520 (1982).

[87] 5 U.S.C. § 552a (1982).

relevant to this discussion. Title III of the Omnibus Crime Control and Safe Streets Act provides criminal sanctions for interception of oral communications and regulates wiretapping by law enforcement agencies. The Act prohibits wiretapping by persons other than authorized law enforcement officers engaged in the investigation or prevention of specified types of serious crimes; only after a court order authorization is obtained upon a showing and finding of probable cause may a wiretap be obtained.[88] To eliminate the possibility of a fourth amendment violation, precautionary measures are mandated: the communications to be intercepted must be specified; normal investigative procedures must be inadequate; the duration of interception must be limited; efforts must be made to minimize interceptions which do not relate to the subject matter under investigation; and progress reports may be required by the authorizing judge.[89] These principles and provisions could be adapted to provide guidelines for the interception of data from computer terminals by government agencies.[90] If such highly specific guidelines were created, it would serve to reduce the risks of exposure of videotex subscriber information.

The Privacy Act of 1974 governs the collection, maintenance, use and disclosure of personal data contained within the federal data banks. The Act establishes three important principles.[91] First, there is the right of an individual to know what information exists in a data bank and the right to have errors concerning the information corrected.[92] Second, there is a restriction on the type of information concerning an individual that may be collected and how that information may be disclosed to third parties.[93] Third, there is a fiduciary duty on the part of the information collectors. The Act provides for civil remedies in the case of irresponsible use of data[94] and criminal penalties where there are willful or intentional violations.[95] These principles could be applied to privately-owned data banks where the dangers are not dissimilar.[96]

---

[88] 18 U.S.C. §§ 2516, 2518 (1982). *See* Gelbard v. United States, 408 U.S. 41 (1972).

[89] 18 U.S.C. § 2518 (1982). *See* United States v. Focarile, 340 F. Supp. 1033 (D. Md.), *aff'd*, 469 F.2d 522 (4th Cir. 1972), *aff'd*, 416 U.S. 505 (1974).

[90] Nash & Bollier, *supra* note 25, at 73.

[91] *Id.*

[92] 5 U.S.C. § 552a(d) (1982).

[93] 5 U.S.C. §§ 552a(b),(e) (1982).

[94] 5 U.S.C. § 552a(g)(1) (1982).

[95] 5 U.S.C. § 552a(i) (1982).

[96] Nash & Bollier, *supra* note 25, at 73.

The Privacy Act of 1974 established the Privacy Protection Study Commission[97] to report on the implementation of the Privacy Act and other privacy issues. The Commission's report found that there were gaps in the law which would not provide privacy protections for new technological developments, such as interactive home media.[98] The Commission recognized the need for explicit guidelines to protect privacy during routine information gathering. It also noted concern over the informal collection and sharing among organizations of information[99] which would not ordinarily be defined as confidential. In addition, the Commission found that it was difficult to prove unauthorized disclosure or misuse of information, and that the penalties imposed for violations of the Act were too lenient.[100]

The Commission recommended a code, involving four principles, which was endorsed by President Carter in 1979:

> (1) Individuals should be told, when they contract for a service, what personal information will be collected and how it will be used.
> (2) Individuals should be able to see the records concerning them and to correct errors.
> (3) Individuals should be told when an adverse decision (e.g., a refusal to extend credit) is based on recorded information (e.g., a credit reporting system).
> (4) Government access to personal records should be through a formal process, creating a paper trail to deter abuse. Whenever practical, the individual should be notified and given an opportunity to go to court.[101]

These principles can be implemented through state and federal legislation protecting information contained in public data banks. Such legislation may be the only means available to afford protection to videotex subscribers. To some extent, some of these provisions have been implemented through the adoption of state and voluntary regulations.[102] However, the majority of these codes and statutes fail to ensure the videotex subscriber with sufficient privacy safeguards.

---

[97] This commission was created by Congress under the Privacy Act of 1974, Pub. L. No. 93-579 §5, 88 Stat. 1896 (1974), *amended by* Pub. L. No. 95-38, 91 Stat. 179 (1977).

[98] Nash & Bollier, *supra* note 25, at 73.

[99] *See supra* note 53 and accompanying text.

[100] Nash & Bollier, *supra* note 25, at 73.

[101] Neustadt, Skall & Hammer, *supra* note 12, at 408.

[102] Some municipal governments, including Boston, Massachusetts, Lexington, Kentucky, Milwaukee, Wisconsin, and Tuscon, Arizona, have issued subscriber privacy protections. How-

V. Industry Codes

Some of the companies involved with interactive home media have developed formal written policies for protecting consumer privacy.[103] For instance, in 1981, Warner Amex Cable Communications, operator of the Qube system, promulgated its Code of Privacy.[104] This established the first comprehensive guidelines by an operator of an interactive home media system.[105] Although this Code may represent "well-formulated and responsible voluntary action by a service provider,"[106] the Code, because of its vague and ambiguous provisions, fails to guarantee informational privacy.

The Warner Amex Code states that the company will provide "adequate" physical safeguards to ensure the confidentiality of any information provided.[107] However, there is no elaboration of what these safeguards entail. Under the Code individualized information concerning viewing responses cannot be aggregated "unless the subscriber has been advised in advance and given adequate opportunity not to participate."[108] This provision provides Warner Amex with sole discretion to determine what is an "adequate opportunity." The opportunity to allow a consumer to prevent the aggregation of personal data is an important safeguard, and one which can be too easily circumvented in the context of this provision. In addition, Warner Amex expressly reserves the right to compile bulk data for the purpose of developing new services or improving existing ones.[109] Although Warner Amex will not release such aggregated data where the identity of the individual is ascertainable, the company implicitly reserves the right to otherwise sell or rent individual information.[110] Warner Amex also promises not to make subscriber information available to government agencies unless compelled to do so by court order or subpoena. If Warner Amex is required to make such information available, it will "promptly notify the subscriber prior to responding if permitted to do

---

ever, a 1981 Wisconsin study determined that, in general, municipal ordinances were poorly written and did not deal with essential issues. Therefore, the study concluded that legislation is needed at the state and federal level. Westin, *supra* note 19, at 104.

[103] Nash & Bollier, *supra* note 25, at 74.

[104] *See* Warner Amex Cable Communications Code of Privacy (1981).

[105] Westin, *supra* note 19, at 104.

[106] *Id.*

[107] Warner Amex Cable Communications Code of Privacy ¶ 2.

[108] *Id.* ¶ 3(B).

[109] *Id.* ¶ 4.

[110] *Warner Amex Privacy Code*, 8 Privacy J. 2 (Feb. 1982).

so by law."[111] Subscribers are guaranteed the right to examine any information pertaining to them and to correct the data "upon a reasonable showing" that it is inaccurate.[112] It is quite possible that a Qube subscriber, in danger of having incorrect personal information on record, would disagree with Warner Amex on the definition of a "reasonable showing." Similarly, Warner Amex's promise to keep individual subscriber information "for only as long as is reasonably necessary"[113] is a term which is too indefinite to ensure any real protection. The Code further states that subscriber mailing lists will be made available to third parties only after providing subscribers with the opportunity to have their names removed from these lists.[114] Third parties who provide services to Warner Amex subscribers would be required to adhere to the company's Code of Privacy.[115] In addition, Warner Amex will comply with federal, state and local laws concerning subscriber privacy.[116]

It is essential to note that the Code, by not expressly forbidding Warner Amex from offering a discount to any subscriber who waives these provisions, tacitly permits such discounts.[117] Moreover, Warner Amex may release individual or cumulative data to its many affiliates without violating any applicable state law or city ordinance.[118] Consequently, while Warner Amex may be applauded in its attempt to guarantee privacy, the provisions are extremely vague and offer ample opportunity for the service provider to avoid strict compliance with the ostensible intent of its Code.

The Cox Cable Communications Code of Subscriber Privacy[119] is an example of a code which is even more likely to foster abuse of informational privacy. The Cox Code states that personal information

---

[111] WARNER AMEX CABLE COMMUNICATIONS CODE OF PRIVACY ¶ 5.

[112] *Id.* ¶ 6.

[113] *Id.* ¶ 7.

[114] *Id.* ¶ 8.

[115] *Id.* ¶ 10.

[116] *Id.* ¶ 9.

[117] Smith, *supra* note 53, at 6. A privacy bill was introduced in the Maryland House of Representatives by State Legislator Joan Pitkin. A. 1320, Gen. Assembly Sess., 1983, Maryland, would specifically prohibit a company from requesting a subscriber to sign a waiver permitting use of personal data. In addition, the bill would not permit a subscriber to be penalized for withholding permission to use or disclose data. *In The Courts,* 9 PRIVACY J. 7 (March 1983).

[118] This provides the opportunity to utilize personal information within the various components of a corporate structure. Such an opportunity signifies a tremendous marketing strategy for the corporation. Even if the videotex company is not a monetary success, its existence is crucial for the information it provides within the corporate family. *Id.* 3-6. *See* Smith, *supra* note 53, at 6.

[119] COX CABLE COMMUNICATIONS CODE OF SUBSCRIBER PRIVACY (1982).

will not be disseminated to any third party, except "with the consent of the subscriber" and "upon service of an order of a court or government agency having jurisdiction, after first advising the subscriber of such service, if *reasonably possible.*"[120] According to the Code, an individual need not be informed that his personal data has been made available for government scrutiny since Cox is only obligated to report this disclosure if reasonably possible. The information may also be disseminated "[a]s reasonably required incidental to a justifiable audit."[121] This provision could easily make banking and other information available to the public. Cox will allow an individual to "review his records for accuracy" and corrections will be made "upon written request and submittal of appropriate documentation."[122] In spite of the Code's assurance that it will "utilize best efforts to safeguard subscriber information from unwarranted disclosure,"[123] in essence it assures little protection. Rather, due to subtle disclaimers and vague policies, this Code may provide the impetus for much abuse of individual privacy.

In spite of the industry's commendable efforts to establish standards for protecting consumer privacy,[124] the codes do not provide penalties for employees who violate these rules, nor damages to injured subscribers.[125] Furthermore, it is quite possible that not all operators will adopt these rules, especially when such provisions decrease profits from secondary uses of subscriber information.[126] In addition, if a third party or the government seeks to compel information through the courts, it is unlikely that a voluntary code could withstand such opposition.[127] Consequently, a voluntary code could

---

[120] *Id.* ¶ A(1),(2) (emphasis added).

[121] *Id.* ¶ A(3).

[122] *Id.* ¶ C.

[123] *Id.* ¶ B.

[124] In addition to the voluntary codes established by specific companies offering videotex services, a model code has been introduced by the association representing videotex companies. The Videotex Industry Association released its MODEL PRIVACY GUIDELINES FOR VIDEOTEX SYSTEMS (1983) which firmly states that there have been no privacy abuses involving videotex. The guidelines allow the disclosure of individually identifiable information under prescribed conditions: to provide a service requested by the subscriber; to maintain operation of a system; to prevent the unauthorized use of a system; to bill users; and to compile bulk information for market research purposes. Individual data would also be released under compulsory legal process. In all other instances the subscriber's consent would be required. In addition, the videotex operator reserves the right to modify the guidelines. *Privacy Guidelines for Videotex*, 9 PRIVACY J. 6 (July 1983).

[125] Westin, *supra* note 19, at 104.

[126] *Id.*

[127] *Id.*

not provide the necessary protections that could effectively be achieved through the legislative process.

VI. State and Federal Legislation

Several states have enacted legislation in an attempt to furnish the safeguards which are not adequately provided for by voluntary industry codes. In 1981, Illinois became the first state to enact legislation to protect informational privacy in the realm of home media systems. The Communications Consumer Privacy Act,[128] effective since 1982, provides assurance that there will be no audio or visual intrusion by a communications company without the subscriber's knowledge or permission.[129] This provision is intended to prevent intrusion of the home security devices that monitor houses for fire and theft.[130] The Illinois statute also prohibits the installation or maintenance of such a device without the subscriber's written consent.[131] In addition, the system operator may not give anyone a list containing the subscriber's name without notice to the subscriber,[132] nor may the operator disclose the individual's viewing habits without his written consent.[133] A $10,000 fine may be imposed for violation of these provisions, and an injured party may commence an action for damages.[134] The Illinois statute is not comprehensive and results in interstices in the law. For instance, the legislation does not provide for the correction of inaccurate information, the time period for which the individual information may be retained and to what extent individual subscriber responses will be aggregated.

Following in the footsteps of Illinois, Wisconsin, in 1982, became the second state to enact cable privacy legislation.[135] Based on the legislative finding that "the use of cable television may infringe on the right of privacy in this state,"[136] the law encompasses two major regulations. First, it requires operators to give any requesting subscriber a device which enables the subscriber to control and prevent

---

[128] Ill. Ann. Stat. ch. 38, ¶ 87-1 (Smith-Hurd Supp. 1983).

[129] *Id.* ¶ 87-3(a)(1). California's recently enacted privacy bill similarly assures a subscriber that there may not be visual or audio intrusion without consent. Cal. Penal Code § 637.5(a)(1) (West Supp. 1983).

[130] *In California: Cable TV Protection*, 8 Privacy J. 1 (Sept. 1982).

[131] Ill. Ann. Stat. ch. 38 ¶ 87-3(a)(4) (Smith-Hurd Supp. 1983).

[132] *Id.* ¶ 87-3(a)(2).

[133] *Id.* ¶ 87-3(a)(3).

[134] *Id.* ¶ 87-3(b).

[135] Wis. Stat. Ann. § 134.43 (West Supp. 1983).

[136] 1981 Wis. Laws C.271, § 1.

the reception and transmission of signals in the home. It would control all messages except those recurring at constant intervals, such as the fire and security systems. A subscriber would not incur additional costs for such a service.[137] The second provision forbids any person who does not have the subscriber's written consent from the following acts: monitoring the subscriber's cable equipment or the use of it, except for service or billing purposes; providing "anyone"[138] with information that discloses, or reasonably leads to disclosure of any "aspect of the behavior" of the subscriber or his household, including "individual habits, preferences or finances"; or conducting research that requires the response of any household member, unless that individual has received written notification before the research begins and at least once each month while the research continues.[139]

A subscriber's name and address may be given to a third party only for billing purposes or for purposes of sending program listings. The name and address may only be supplied if the subscriber is given written notification and does not object.[140] A penalty of $50,000 may be imposed for a first offense of this statute and up to $100,000 for a second offense. A subscriber may also be entitled to damages and injunctive relief.[141] Like the Illinois statute, the Wisconsin statute does not regulate the correction of inaccurate information,[142] the destruction of information after a reasonable period of time or the ordering of information by a court.

In 1982, New York State Attorney General Robert Abrams submitted the Cable Privacy Act to the state legislature.[143] The pending bill has been described as the most comprehensive state bill pertaining

---

[137] WIS. STAT. ANN. § 134.43(1)(a)-(d) (West Supp. 1983). Compare this to a recently enacted New York statute, N.Y. EXEC. LAW § 829a (1983), which requires each cable television company to offer a locking device to control the transmittal of messages. New York cable companies are permitted to charge customers for the device although there is a ceiling on the price. *See supra* note 24.

[138] Although the statute prohibits a company from disclosing information to "anyone," it is possible that corporations will argue that disclosures within the corporate structure do not fall within the prohibition. Smith, *supra* note 53, at 6.

[139] WIS. STAT. ANN. § 134.43(2)(a)-(c) (West Supp. 1983).

[140] *Id.* § 134.43(2m)(a)-(b).

[141] *Id.* § 134.43(3)-(4).

[142] Unlike the Illinois and Wisconsin statutes, California's privacy legislation does permit a customer to inspect and correct any information about himself stored by the cable company. CAL. PENAL CODE § 637.5(d) (West Supp. 1983).

[143] A.11052, S.8765, 205th Ann. Leg. Sess., New York (1982). This bill, which never came out of committee in 1982, was reintroduced with minor amendments in 1983. A.6337, S.5357, 206th Ann. Leg. Sess., New York (1983). A.6337 is currently in the Governmental Operations Committee and S.5357 is currently in the Senate Energy Committee.

to cable privacy.[144] The bill was submitted in response to the legislative findings that the collection of personal information by cable television companies "poses a serious threat to the personal privacy of the citizens of New York."[145]

In many respects the provisions of the New York bill parallel those of the Warner Amex Code although the New York bill is more extensive.[146] Whenever an application is made for cable television services, the subscriber is to be notified of the type of information the company expects to collect from the subscriber, and to whom and under what circumstances subscriber information would be disclosed.[147] In addition, a subscriber is to be provided with a clear, concise and nontechnical description of the privacy rights to be afforded the subscriber under this legislation.[148] Subscriber authorization would be required before a cable television company arranges for the transmission of signals to monitor individual household viewing patterns or practices. No subscriber is to be penalized for failure to authorize such a transmission, nor is the authorization to be a condition for receiving service.[149] The bill mandates that individually identifiable information, which is to be collected only upon subscriber authorization, is to be destroyed upon completion of the permissible uses of that information.[150] In addition to establishing a right of access to the subscriber's own file,[151] the statute would provide the basis for a legal right of privacy to prevent a person, corporation or government from obtaining individually identifiable information without subscriber authorization.[152] The proposed statute also specifies extensive requirements to ensure accuracy in the files and obligates the operators to correct inaccurate or outdated information.[153] Moreover, the bill amends the applicable Penal Law to include in the definition of "wiretapping" the interception of signals transmitted over cable television systems.[154] Thus, any interception of videotex messages transmitted from subscriber terminals over cable television systems would

---

[144] Gerberg, *Cable Protection Bill Submitted in New York*, 8 PRIVACY J. 1 (Feb. 1982). *See* Memorandum in Support of New York A.11052, S.8765, at 3.

[145] N.Y.EXEC. LAW § 833(a) (Tent. Draft 1982).

[146] Westin, *supra* note 19, at 106.

[147] N.Y. EXEC. LAW § 833(i)(a)-(b) (Tent. Draft 1982).

[148] *Id* § 833(i)(3).

[149] *Id* § 833(c).

[150] *Id* § 833(d)(2)-(3).

[151] *Id* § 833(f).

[152] *Id* § 833(e).

[153] *Id* § 833(g)-(h).

[154] *Id* § 833(p)(2).

constitute unlawful wiretapping. In addition to creating civil and criminal penalties for violation of the bill,[155] the bill gives authority to the Commission on Cable Television to prescribe further regulations to effectuate the legislation[156] and to the Office of the Attorney General to enforce the provisions.[157]

In addition to these statutes, legislation has been proposed on the federal level. In 1982 Senator Barry Goldwater sponsored the Cable Telecommunications Act to amend the Communications Act of 1934.[158] The Act, which would give the Federal Communications Commission regulatory authority over cable,[159] includes a section on "Protection of Subscriber Privacy."[160] By defining broadband telecommunications[161] as "wire communication" within the meaning of the Omnibus Crime Control and Safe Streets Act of 1968,[162] the section would prohibit wiretapping, or unauthorized interception, of cable signals.[163] The act would require the written consent of a subscriber before a cable system could collect or disclose personally identifiable information, for uses other than billing or detecting interception.[164] If a court orders such disclosure, the subscriber must be notified within fourteen days.[165] Upon purchasing the service, each subscriber is to be notified of his privacy rights, including the nature, location and availability of information collected.[166] In addition, a subscriber would be entitled access to all information collected concerning him.[167] Any violations of this privacy would entitle the sub-

---

[155] *Id* § 833(l)-(m).

[156] *Id* § 833(k).

[157] *Id* § 833(n).

[158] S.2172, 97th Cong., 2d Sess. (1982). The bill never came out of committee in 1982 and was reintroduced with some changes in 1983. S.66, 98th Cong., 1st Sess. (1983). The bill was passed in the Senate on June 14, 1983 and is currently in the House Committee on Energy and Commerce.

[159] S.2172 § 604.

[160] *Id* § 610.

[161] Broadband telecommunications is defined as "any receipt or transmission of electromagnetic signals over one or more coaxial cables or any other closed transmission medium." *Id.* § 603(3).

[162] 18 U.S.C. § 2510(1) (1982).

[163] S.2172, 97th Cong., 2d Sess. § 610(b) (1982). Wiretapping or unauthorized interception of cable signals would be controlled by 18 U.S.C. §§ 2510-2520 (1982).

[164] S.2172, 97th Cong., 2d Sess. § 610(d)-(e) (1982).

[165] *Id* § 610(f).

[166] *Id* § 610(g).

[167] *Id* § 610(h).

scriber to recover civil damages[168] while subjecting the cable operator to criminal prosecution.[169]

VII. The Response to Privacy Legislation

Spokesmen for the interactive home media industry are opposed to legislation at this time.[170] They contend that there is no need to enact premature regulatory legislation since there have been no known abuses of subscribers' privacy. The industry views the New York bill as especially threatening because of its detailed provisions.[171] Furthermore, because the field is still in the early process of rapid development and the privacy issues are unclear, videotex companies argue that any restrictions may be potentially crippling.[172] Instead, it has been suggested that the protection of privacy be left to the free market.[173] Under such a theory, privacy is viewed as an economic commodity, the production of which involves the loss of informational resources. A subscriber, in order to retain his privacy, must in effect pay for it through increased subscription rates. This desired privacy limits the amount of information available to the industry. The loss of this information will result in far-reaching economic effects.[174] However, this theory is defective in several respects.[175] Since it is likely that only one interactive cable system will service a community, it is doubtful that a subscriber could bargain freely to sell his personal information at market value. Even if there is a competitive market in the community, consumers will not be aware of how and to what extent their information will be used in order to place a value on that information in the bargaining process. In addition, enabling the rich to purchase more privacy than the poor seems to violate basic democratic principles. When privacy is no longer seen as a basic right, but as a commodity which is available to the highest bidder, exploitation is inevitable.[176]

Proponents of the legislation emphasize that enacting laws now, before the systems become operational, is desirable for reasons of cost

---

[168] *Id* § 610(i).

[169] *Id* § 611.

[170] Westin, *supra* note 19, at 106.

[171] *Id.*

[172] Nash & Bollier, *supra* note 25, at 74.

[173] *Id.*

[174] *Id.* For an economic analysis of the right of privacy, *see* Posner, *The Right of Privacy*, 12 Ga. L. Rev. 393 (Spring 1978).

[175] Nash & Bollier, *supra* note 25, at 74.

[176] *Id.* at 74-75.

efficiency and convenience.[177] Exploring the question in the present and implementing discoveries will minimize breaches of privacy.[178] However, some consider legislation like the New York bill to be unduly costly, restrictive and cumbersome, and others would prefer to see a uniform set of rules on the federal level.[179]

VIII. Conclusion

The profound changes that will occur with the development and use of videotex demand immediate attention. The potential impact of videotex is enormous; it promises to revolutionize and simplify our daily living. Videotex has the capability to deliver, at the push of a button any time of the day or night, unlimited amounts of information to individuals in a quick, efficient and convenient manner. Unfortunately, this same system could quickly destroy individual privacy by filtering vast quantities of intimate information to commercially exploitative enterprises, overzealous government enforcement officials or the idly curious. When a subscriber file, consisting of an individual's financial data, buying habits and personal preferences, is accessible to the public, the groundwork is laid for George Orwell's *1984* scenario. This situation is even more alarming in view of prior judicial decisions concerning governmental access to bank records,[180] drug prescription records[181] and other similar personal data.

Videotex subscribers may be totally unaware of these privacy risks. Therefore, it is imperative that consumers be educated prior to subscribing to a system. Each potential user must have a basic understanding of the operations of the system and the manner in which their privacy may be affected. Consumer education is, however, only the first step required in a strategic approach toward adequate protection of privacy rights.

Formal standards must be developed for ensuring informational privacy. However, it will not suffice to allow videotex companies, whose primary focus is on profits, to voluntarily provide for consumer privacy protection. Nor does it seem logical to wait until the occurrence of an informational privacy breach before formulating legislation. It will prove to be most beneficial, to the public and to the industry, to enact legislation now while videotex is still in its infancy.

---

[177] Gerberg; *supra* note 144, at 1; *In The States,* 9 Privacy J. 7 (March 1983).

[178] Nash & Smith, *supra* note 8, at 19.

[179] Westin, *supra* note 19, at 106.

[180] United States v. Miller, *supra* notes 70-73 and accompanying text.

[181] Whalen v. Roe, *supra* notes 74-78 and accompanying text.

Such action would deter any abuses and allow the safeguards to be built into the system. Given the highly dynamic nature of videotex, legislation could be modified to accommodate the growing technology. Furthermore, protection will be available to the public on an equal basis, regardless of personal wealth.

Insofar as multistate operations will be the norm in videotex, legislation on the federal level is necessary. The public interest will be best served if a federal bill is modeled on the proposed New York legislation. This bill provides a solid framework for effectively protecting informational privacy. The provisions encompass all areas of potential abuse and reassuringly establish an expectation of privacy in individually identifiable information. Admittedly, this bill is more demanding on the industry than the proposed United States Senate bill. Nevertheless, any harsh burdens the provisions may impose on the industry could be reflected in a higher fee for use of the service, which subscribers would arguably pay to ensure their privacy.

Society is presently on the threshold of an electronic technological explosion. Such revolutionary advancements must not be hindered by possible abuses of the system. Instead, these issues must be confronted and resolved with appropriate laws. Once effective legislation is enacted, individuals will confidently approach 1984 utilizing videotex systems without fear of an Orwellian intrusion into their private lives.

Mindy Elisa Wachtel