
Pat Washburn
More than 100 years ago, the French historian Alexis de Tocqueville noted: "If the private rights of an individual are violated . . . the manners of a nation" are corrupted, jeopardizing the entire society.¹

Our computerized society gives many people cause to be concerned about their privacy. For example, a 1979 Louis Harris survey showed that sixty-four percent of Americans were worried about “threats to personal privacy” compared to only forty-seven percent in 1978.² One major reason for increased concern about the rights of privacy is the rapidly increasing use of computers, which may be used to compile and disseminate personal information.

"Legislation in effect, such as the Privacy Act of 1974 and the Fair Credit Reporting Act, are inadequate," says David F. Linowes, former chairman of the United States Privacy Protection Commission. "They treat only pieces of the [computer] problem, and not very effectively at that."³

Willis Ware, a Privacy Protection Commission member, is even more pessimistic.

The bottom line of this issue is that . . . personal information has no legal protection; organizations that hold it do with it as they wish. The individual has no standing to contest what an organization does with it. Organizations holding personal information have discovered—and one would anticipate they would—that information is a valuable commodity; it can be bought, sold, bargained, used and can produce revenue.⁴

Use of computers has dramatically altered the availability, and hence the security, of stored data. Formerly, personal information usually remained private for a number of reasons: large quantities

¹. Linowes, Must Personal Privacy Die in the Computer Age?, 65 ABA J. 1181, 1184 (1979).
². Id.
³. Id.
of personal information were not generally collected; compilations of information remained decentralized; most of the data was superficial; access to the data was limited; it was difficult to compile complete information on any individual member of a highly mobile society; and most people were unable to interpret the recorded data.\(^5\)

Security of personal information is not the only problem. Use of computers requires a restructuring of the broad concept of the right of privacy. As with most questions of public policy, the problem is not whether a particular right is legitimate but that it comes into conflict with other rights. Although the absence of precise definitions poses a difficulty in itself, most people would agree that an individual has some right to keep information about himself from inspection by the general public, assuming the purpose of doing so is not in the service of criminal acts. The conflicting right is that of society as a whole to have certain kinds of information that contribute to the general good. For example, most people would agree that a person should not have information about criminal acts in his distant past held against him forever—yet statistical [non-individualized] information about crime trends is usually thought to be valuable. Since maintaining the data needed to provide statistical trends holds the possibility of abuse of data about individuals, the two rights are in conflict. Finding a proper balance between these goals is one of the most difficult aspects of this issue, and yet it must be attempted.\(^6\)

Electronic journalism is one of many new industries which will depend heavily upon computers. The impact of electronic journalism on society will be enormous. In the future, people will be able to shop for virtually anything over their home television set. Many workers will stop commuting because they will use the television to communicate with business associates. Viewers in Columbus, Ohio, currently have access to stored information on television screens.

I. QUBE

QUBE, owned by Warner-Amex Cable Communications, is a two-way interactive cable system. For about $12.95 per month, a QUBE customer receives thirty television channels and the ability to “talk” with a computer via a small keyboard attached to his television. Currently, this interactive capacity can be used to accomplish many tasks: voting in a town meeting; ordering books, records

\(^5\) A. Miller, The Assault on Privacy 26 (1971).
\(^6\) Association for Computing Machinery Committee—Computers and Public Policy, A Problem List of Issues Concerning Computers and Public Policy, 4 Computer L. Serv. § 5-0, art. 1, at 12 (1976).
and clothes; kayoing people on a local gong show; taking educational courses; or asking to view an adult movie. In addition, QUBE is considering an electronic funds transfer (EFT) service, which would allow subscribers to pay for the products that they order by transferring money from their bank accounts to the businesses’ accounts.7

Although many viewers have enjoyed playing with the two-way interactive system, not everyone has been pleased with its potential. “I’m not sure I want the Iranian situation solved by Carter going on TV—or worse yet, Tom Snyder—and asking should I do A, B or C and having that as the basis for a decision,” said Paul Fox, an electrical engineer in the Office of Plans and Policies at the Federal Communications Commission.8 John Wicklein, a Boston journalist and educator, discussed subtler and more dangerous problems:

Playing the system [talking to the computer], subscribers are only vaguely aware that the preferences they state, the products they select, the personal opinions they express can all be stored in the computer’s memory and tallied, analyzed, and cross-referenced with demographic financial information that is known about them. Several subscribers I interviewed said that they were not concerned about this. One young woman told me, “I don’t feel that I have any reason to be afraid—I may be naive, but I don’t care if my opinions are recorded.” Their attitudes seemed to be, Who would want that stuff, anyway? Who could profit by it?

Someone might.9

Wicklein used a hypothetical situation to illustrate the deleterious effects on individual privacy from an interactive cable system run by unscrupulous managers.

At the cable-company headquarters, the information sales department, which works around the clock, is compiling for its confidential clients data the computer has collected concerning subscribers who have ordered computer profiles from the system.

Client 1, Mayor Paxton’s campaign manager, is delighted to learn that Arnold [Johnson], whose wife [another candidate for mayor] is a feminist and a supporter of legislation to eliminate legal restrictions concerning sex, has expressed an opinion against one of her campaign stands. He chuckles at the use he can make of the fact that Arnold also watched a porno movie while his wife was out. He knows what time Martha left the house because the cable company, at the mayor’s request, has installed a motion sensor to monitor the Johnson’s doorway from outside the house . . . .

Client 2, a publisher of skin magazines, also gets notification of

the porno-film selection, and sends the Johnsons a sales brochure in a plain manilla envelope.

Client 3, a local environmental group trying to decide whether to work for Mrs. Johnson, is disappointed to learn that she would unthinkingly order an aerosol [from a store via the interactive system] that is dangerous to the ozone layer.

Client 4, a national credit-rating company, finds that the department store has rejected Mrs. Johnson's purchase on credit and puts that datum into her dossier for the next customer who purchases credit-rating information on her. It also enters a correction regarding the Johnsons' bank balance, which the computer obtained when Arnold paid for [a] book [using electronic funds transfer].

Company officials realize that subscribers may be concerned about invasions of privacy. Gustave M. Hauser, president and chairman of Warner Cable (now Warner-Amex), told the New York Times: “People who buy the service will simply have to accept that they give up a bit of their privacy for it. Beyond that, we'll try to protect their privacy all we can.” Vivian Horner, a Warner vice president, also acknowledges that the service may threaten subscribers' privacy, but she believes that marketplace forces will inhibit any significant threat to privacy. “People don't think of the telephone as an invasion of privacy,” she says. “Yet each call you make is recorded. When people get as used to two-way cable as to the telephone, they will take it much as a matter of fact. If people feel threatened by it, they will drop it—the economic base will keep it honest.”

QUBE's security procedures consist of limiting access to the computer's records to three top-level executives and limiting entrance to the area housing the computer to those working there. Leo Murray, vice president/public relations for Warner Amex, noted with pride that there have been no complaints about information stolen from QUBE's computer. “Anyway, the information we have is infinitesimal compared to what the banks or the credit agencies have,” he said. He indicated that he believed burglars wouldn't find it worthwhile to steal from QUBE. He also noted that, as an additional safeguard, the information is dumped after several months.

There is little doubt that QUBE, which has grown from 1,500 subscribers on December 1, 1977 to 44,000 subscribers, is only the first of a number of sophisticated two-way interactive systems that

10. Id. at 41.
11. Id. at 40.
12. Id.
13. Id.
will enter the market in the near future. In January, 1980, Warner-Amex began cable service in Norwood-Amberly Village, Ohio, and a two-way interactive system is expected eventually to serve thirty-seven suburban communities around Cincinnati. In addition, Warner-Amex is planning systems in Houston and Pittsburgh.\textsuperscript{15} "We'd like to be in every city in the country," says Murray.\textsuperscript{16}

A brief historical analysis reveals that the consumer's right of privacy is far more vulnerable to computerized invasion by the private sector than by governmental agencies.

\section*{II. BRIEF HISTORY OF COMPUTER-RELATED PRIVACY LEGISLATION}

Public officials have only recently recognized that computers posed a threat to personal privacy. In 1965 when a committee of the Social Science Research Council recommended the creation of a National Data Center for the development and preservation of data for use in economic research, the Committee also recommended that the data should be protected from outside groups, both in the federal government and the private sectors.\textsuperscript{17}

As a result of these recommendations the Special Subcommittee on the Invasion of Privacy of the House Committee on Government Operations conducted a series of hearings on the computer and invasion of privacy. Subcommittee chairman Cornelius E. Gallagher outlined the hearings' objectives:

What we seek at this point is to create a climate of concern, in the hope that guidelines can be set up which protect the confidentiality of reports and prevent invasion of individual privacy, while at the same time allowing government to function more efficiently and facilitating the necessary research of scholars in statistical analysis.\textsuperscript{18}

Following extensive testimony, the subcommittee concluded that computer technology was "inadequate to prevent the grave encroachment upon personal privacy that would follow from a National Data Center."\textsuperscript{19} The subcommittee had three objections: centralized information would leave the individual's past constantly open to exposure; centralized computer dossiers would be extremely vulnerable to unauthorized access; and systems containing

\begin{flushleft}
\textsuperscript{16} Telephone interview, supra note 14.
\textsuperscript{18} \textit{The Computer and Invasion of Privacy: Hearings before the Special Subcomm. on Invasion of Privacy, House Comm. on Government Operations}, 89th Cong., 1st Sess. 195 (1966).
\end{flushleft}
statistical information would be as much a threat to privacy as intelligence systems.20 As a result of these objections, the National Data Center was not created. The House Committee on Government Operations recommended that "no work be done to establish the national data bank until privacy protection is explored fully and guaranteed to the greatest extent possible to the citizens whose personal records would form its information base."21

The Fair Credit Reporting Act of 197022 was the first legislation enacted that directly addressed the computer problem. Recognizing that computers never forget, cannot distinguish between correct and incorrect material, and can be manipulated by anyone knowing the right commands, the Act gave individuals the right to review their own credit file and challenge the fairness, accuracy and timeliness of the information.

In the same year, the Committee on Scientific and Technical Information of the Federal Council of Science and Technology established a panel on the legal aspects of information systems. Three years later, in 1973, the panel held a Washington symposium which outlined the following proposals for federal standards on computer privacy: disclosure to individuals as the purposes for which information is being collected; disclosure of the uses to which the information will be put and a consent requirement before the information can be used in other ways; disclosure of who will have access to the information; whether the information will contain a person's name or be identified in some other way; and a statement of how long the information will be retained.23

In 1972, Elliott L. Richardson, in his capacity as Secretary of Health, Education and Welfare, established the Secretary's Advisory Committee on Personal Data Systems to "analyze the consequences of using computers to keep records about people."24 The HEW report in mid-1973 called for two things: "(1) A code of fair information practices—the notion that information ought to be used fairly; (2) . . . the notion that . . . there is a mutual interest of both parties to see to it that a record is complete, accurate, timely and relevant, and used properly."25

Finally, in 1974, President Ford signed the much-amended Pri-

20. Id. at 5.
21. A. Miller, supra note 5, at 58.
24. Id. at 8.
25. W. WARE, supra note 4, at 2.
vacy Act. The Act covered only federal data banks, but it established many of the suggested safeguards. The Act permits individuals to have access to their records and gives them the right to correct errors. No disclosure of personal information may be made without written consent: The Act imposes limitations on the material collected and retained to that which is relevant to an agency, and civil penalties are provided for record-keeping errors.26

Both the Fair Credit Reporting Act and the Privacy Act have been criticized heavily for a glaring inadequacy. Although the Congress has thus attempted to regulate the content, currency and accuracy of data collected, it has not provided well for enforcement. For example, under the Fair Credit Reporting Act, enforcement authority rests with the Federal Trade Commission (FTC), which has been lax, relying upon private enforcement by the consuming public. Among other problems, few consumers have the funds necessary to engage in expensive litigation where the FTC declines to act, resulting in very little litigation in the area. The Privacy Act of 1974 . . . suffers from the same shortcoming since it, too, places the ultimate enforcement burden on the consumer.27

The 1974 Act also established the Privacy Protection Study Commission, which was instructed to study the privacy safeguards needed in the private sector. Commission chairman David F. Linowes was shocked by some of the findings.

Although the Financial Right of Privacy Act of 1978 places limited constraints on some government agencies' access to financial records, in most other areas government has almost unbridled access to records based on a survey of Privacy Protection Commission conducted, up to 99 per cent of government requests for information from credit card companies were granted, even if the request was made by telephone or in the course of an informal visit. The subject was never notified and no record was made of the information given or to whom.28

The Commission also found evidence that information from tax returns was being used for political purposes or for harassment of neighbors, private companies who obtained information from the Internal Revenue Service by impersonating revenue agents, and numerous illegal exchanges of personal information among federal agencies.29

In its 1977 report to the President and Congress, the commission

28. Linowes, supra note 1, at 1182.
29. Id. at 1183.
stressed three objectives which should be built into any computer legislation: "to minimize intrusiveness, to maximize fairness, and to create a legitimate and enforceable expectation of confidentiality when this expectation is warranted." To accomplish these objectives, it recommended the following:

Only information that is relevant to the decision at hand should be collected, and it should be used only for that purpose. Before an organization transfers information to a third person, it should obtain the subject's approval.

The individual should be informed which sources will be contacted to get information, how the data will be used, and to whom they will be disclosed. No information should be obtained under false pretenses or through the impersonation of others.

You should have the right to see and copy records about yourself from any organization that keeps a file on you, including your employer. If you question its accuracy, you should have the right to correct the record. Where the point is in dispute, a statement explaining your position should be made part of the permanent file.

Secret files should be outlawed, so that you know where records about you exist.

Government officials who want to gain access to your records should be required to present proper authorization before being permitted to do so, and you should be notified when a disclosure is made.

Organizations should only employ service and support firms whose privacy standards and principles are equivalent to those of the organization being served.

As a penalty for a violation of these principles, the Commission recommended reimbursement of court costs, actual damages and general damages, with the latter ranging from $1,000 to $10,000.

Congress still has not passed a bill addressing the problem in the private sector. However, most of the things suggested by the Privacy Protection Study Commission are included in a series of bills introduced by Representative Barry M. Goldwater, Jr. (R-California) which have received considerable publicity.

Not everyone is convinced that legislation is needed to protect users of the new electronic journalism systems. Gary Rosche, a Federal Communications Commission attorney, stated that he believes it would be wiser to leave the area unregulated and not pass legislation until abuses arise.

30. Id. at 1184.
31. Id.
32. Id.
On the state level, at least forty states have enacted privacy laws. However, consumer protection is anything but uniform because these laws vary widely. This led one federal judge to compare privacy laws to a “haystack in a hurricane.”

IV. OVERALL LEGAL PROBLEMS

This history indicates that a plaintiff who claims that his privacy was invaded when personal information was stolen from a computer faces major problems.

The difficulty of designing an appropriate legal framework is compounded by the pervasive character of the technology; it permeates both the public and private sectors and has consequences that cut across many traditional legal pigeonholes but do not fit neatly into any of them. Almost every response one might conjure up from the corpus of existing doctrine is bound to seem Procrustean or anachronistic. Thus, although a number of ingenious modifications of contemporary principles have been suggested, no single theory seems extensive enough to respond effectively to the computer’s variegated threat to individual privacy. And so, more than three quarters of a century after Warren and Brandeis provided the impetus for developing the common law of privacy through the power of the pen, we must again goad the law into meeting a challenge to the sanctity of the individual.

While the legal system can be bent to accommodate computer technology the ability or willingness of lawyers to cope with the new technology has been questioned. Because the subject matter is technically complex, many lawyers regard computer law as an esoteric, highly specialized area in which only the prescient and foolhardy dare enter.

V. PROSSER’S FOUR TORTS

Invasion of privacy cases can be divided into four areas suggested by the late William L. Prosser, one of America’s leading torts scholars:

—Intrusion on the plaintiff’s physical solitude.
—Publication of private matters violating the ordinary decencies.
—Putting the plaintiff in a false position in the public eye.

37. A. Miller, supra note 5, at 211.
—Appropriation of some element of the plaintiff's personality (his name or likeness) for commercial use. Each of these torts has application in the computer age.

A. Intrusion

The intrusion tort may provide substantial protection in the computer age because intrusion has been applied in an "extended sense to protect personal information about a subject." In two well-known cases, Zimmermann v. Wilson and Brex v. Smith, the courts refused to allow government officials to examine tax records and bank accounts respectively.

In Brex, the New Jersey Court of Chancery referred to a ringing statement on privacy from an 1887 federal case:

Of all the rights of the citizen, few are of greater importance or more essential to his peace and happiness than the right of personal security, and that involves, not merely protection of his person from assault, but exemption of his private affairs, books, and papers from the inspection and scrutiny of others. Without the enjoyment of this right, all other rights would lose half their value.

In Zimmermann, a Circuit Court of Appeals stated the point more simply: "If due protection of this natural right (the right to be left alone) be denied by the courts, his other rights and his citizenship lose their value."

Not everyone, however, agrees on the usefulness of this sub-area of privacy law in a computerized society. One critic points out some of the problems:

Although the intrusion concept may be a useful approach for remedying wiretapping, electronic eavesdropping or physical or sensory surveillance, it does not afford much protection against misuse of computerized information, which usually does not involve the type of direct physical invasion that this aspect of the privacy tort is designed to deter. Moreover, the intrusion category primarily deals with the nature of the conduct that constitutes the privacy violation, rather than what is subsequently done with the fruits of the invasion; yet in the context of computerized information it is the use of the data that presents the major threat to privacy.

41. 81 F.2d 847 (3d Cir. 1936), modified, 105 F.2d 583 (3d Cir. 1939).
42. 146 A. 34 (N.J. Ch. 1929).
43. Pacific Ry. Comm'n, 32 F. 241, 250 (Ct. Cl. 1887).
44. Zimmermann v. Wilson, 81 F.2d 847, 849 (3d Cir. 1936).
45. A. Miller, supra note 5, at 174.
Many legal scholars believe that *Pearson v. Dodd* 46 will be an important case in computer litigation. This 1969 case involved a charge of invasion of privacy by Senator Thomas Dodd of Connecticut against two Washington columnists, Drew Pearson and Jack Anderson. Two of the Senator's employees copied material from his files and passed the photocopies on to two former Dodd employees, who gave them to Anderson. Although Anderson knew how the material had been obtained, he and Pearson wrote six stories that damaged Dodd's reputation and political career. 47

Judge J. Skelly Wright wrote that the tort of intrusion, unlike any other type of tort for invasion of privacy, does not require that the information be published. "The tort is completed with the obtaining of the information by improperly intrusive means.... Where there is intrusion, the intruder should generally be liable whatever the content of what he learns." 48 Judge Wright also discussed the purpose of extending tort liability to include cases of intrusion:

We approve the extension of the tort of invasion of privacy to instances of intrusion, whether by physical trespass or not, into spheres from which an ordinary man in a plaintiff's position could reasonably expect that the particular defendant should be excluded. Just as the Fourth Amendment has expanded to protect citizens from government intrusions where intrusion is not reasonably expected, so should tort law protect citizens from other citizens. The protection should not turn exclusively on the question of whether the intrusion involves a technical trespass under the law of property. The common law, like the Fourth Amendment, should "protect people, not places." 49

A more recent case, *Birnbaum v. United States*, 50 may also be applicable in computer cases. In 1970, Norman Birnbaum, a sociology professor at Amherst College, wrote professors in Canada and Rumania about an upcoming meeting involving the sociology of religion. He sent copies of both letters to another professor in Moscow. The Central intelligence Agency, as part of a twenty year program opened the Moscow letter and copied it before resealing it and sending it on. 51 Birnbaum discovered this unauthorized copy when he asked the CIA for his file under the Freedom of Information Act. 52

---

47. Id. at 703.
48. Id. at 704-05.
49. Id. at 704.
51. Id. at 971.
52. Id. at 971-72.
In finding the CIA guilty of intrusion, the district court noted that "the common law right [to solitude and seclusion] extends beyond the plaintiff's immediate physical environment and is infringed by examinations of bank accounts or of personal records under false pretenses, or by opening of mail."\(^5\) The court then discussed whether the plaintiff had in fact been harmed:

The plaintiffs in these cases suffered none of the tangible indicia of harm for which a dollar value may easily be assigned. They experienced no financial losses. Their jobs, their reputations and prestige in their communities did not suffer. They were not subjected to intrusive or humiliating investigations by the government. Their homes were not broken into. They were not assaulted or detained. They lost no time from work and incurred no medical expenses. . . . The lack of objective harm is, however, no bar to recovery.\(^5\)

**B. Publication of Private Matters**

Publication of private matters may become the most useful form of the privacy torts in computer cases, but even this tort faces problems. One major problem is the requirement that the private facts be disclosed to the public at large. In several notable cases, *Brents v. Morgan*,\(^5\) and *Biederman's of Springfield, Inc. v. Wright*,\(^5\) courts have awarded damages even though the number of people who witnessed the invasion of privacy was small. But in computer cases, courts will have to decide if one person is sufficient to constitute the public at large.

The publicity requirement is particularly troublesome in terms of preserving the security of computerized personal data, since the critical dissemination may take place when one user of a time-share system permits another to have access to private files, or when the operators of two different systems agree to exchange tapes or interconnect computers. Once an unauthorized user has gained access to an individual's computerized file, he can use what he has learned in ways that may damage the data subject without disseminating its contents further. Even if the victim is able to trace his injury to the improper use of the file, he may be prevented from suing successfully if the transfer of his file to another user or a different computer system is not treated as satisfying the publicity prerequisite.\(^5\)

A second problem for the tort is that the publicly-disclosed in-

---

53. *Id.* at 977.
54. *Id.* at 987.
55. 221 Ky. 765 (1927).
56. 322 S.W.2d 892 (Mo. 1959).
57. A. MILLER, *supra* note 5, at 177-78.
formation must be facts normally considered to be private. One of the earliest cases in this area was *Grigsby v. Breckinridge*.

In *Grigsby*, a dying woman gave her daughter confidential letters that she had received and saved throughout her life. The daughter made plans to publish the letters, but she was sued by the dead woman's husband, her stepfather, on the grounds that he was "entitled to be guarded against any improper use or exposure of these confidential communications." The Kentucky Court of Appeals, in ruling for the stepfather, said:

By sending them, the authors parted with their right to the possession, control, or reclamation of them without her consent . . . [However], [t]he authors . . . retained a qualified property in their contents which they alone had the right to publish for their own benefit; and therefore, and also because they reflected their emotions and sentiments, they had the right to enjoin publication by the recipient or any other person. This was the author's property to its full extent.

The classification of factual information as private or not may vary, and use of computers may affect the classification process.

Whether the court treats particular facts as private depends largely on the general community's attitude rather than a fixed norm. As a result, the availability of the privacy action is dependent on the community's ability or willingness to distinguish between facts that should be considered part of the public domain and facts that are none of the public's business. But community attitudes are fickle—one need only think of the dramatic shifts in public opinion on such matters as sex and religion in recent years. The danger is that widespread computerization of personal data coupled with continuous demands for data by society's information managers will slowly narrow the community's conception of what is private, which in turn will gradually reduce the effectiveness of the privacy action.

A third problem is the centralization of data in computer banks. Miller speculates that when highly confidential data is commingled with less sensitive material in a computer, the entire mass of data on an individual may "be treated as if it had a rather low level of sensitivity. Consequently, the over-all protection may be less than that which should be accorded to the most personal information stored in the system."

58. 657 Ky. (2 Bush) 480 (1867).
59. *Id.* at 482.
60. *Id.* at 484.
62. *Id.* at 181.
The final requirement is that the disclosure must be offensive to a person with ordinary sensibilities.

By the time large quantities of computerized personal information are available and transfers of machine-readable data are commonplace occurrences, the public may have become anesthetized to what a more sensitive society might view as an "offensive" exposure of private information to public view. The result will be less tolerance for the claim that an individual has the right to determine what aspects of his life may be given publicity. Just as we have become acclimated to the obnoxious and omnipresent quality of television commercials, the revelation of intimate details in a person's computer record may become so normal that it will not satisfy the requisite level of community offense.63

C. False Light

How useful the tort of false light will be in computer cases is not clear. Miller feels that it would be unfortunate not to adapt the false light principle.

Indeed, it is the only one of Dean Prosser's categories that even remotely suggests the type of sensitive analysis that is necessary to come to grips with the range of subtle injuries that can be inflicted in an information-based society. Thus, it would be desirable to refine and expand the false-light doctrine to permit lawsuits by those who have been injured by the dissemination of information that is misleading, has been used out of context, or has become inaccurate because of age, improper supplementation, or failure to include important underlying data. The courts also will have to de-emphasize the requirement of disclosure to the public at large (necessary in false light privacy cases) if the theory is to be responsive to the way in which computerized information will be used in a dossier society.64

D. Appropriation

Wrongful appropriation would appear to be a weak ground for a privacy suit involving a computer. However, it is possible to argue that a full computer dossier is as much a picture of a person as a photograph.65

Unfortunately, this line of reasoning can be criticized as little more than a play on words, and viewed realistically, the likelihood of a court accepting this approach appears small. In addition to their obvious physical difference, the analogy between a photograph and an alpha-numeric file is imperfect because there is no clear point at

63. Id. at 182-83.
64. Id. at 184-85.
65. Id. at 174.
which factual information becomes sufficiently complete to constitute a "picture." Moreover, dissemination of individual items of data to different buyers technically would not be actionable under the logic of the analogy, since it is only the appropriation of the entire "picture" that fits this category of the privacy action. Another difficulty is that there would be no protection against the transfer of inaccurate information, since erroneous data, however detailed they might be, presumably would not be a "likeness" of the person suing. 66

Furthermore, the state in which you are suing can determine the usefulness of appropriation in a privacy action. In the thirty-four states where common law recognizes the right of privacy, it does not have to be demonstrated that the "invasion" resulted in a financial gain. But in five of the six states with privacy statutes—New York, Oklahoma, Virginia, Utah and California—there must be proof of monetary advantage for an appropriation suit to be successful. 67

VI. CONSENT

Consent cases, which are closely related to privacy, will become increasingly complex because of the record-keeping ability of the computer.

There is no way for any one of us to live in today's society without interacting with record systems; there just is no way. Not even a hermit on the top of a remote mountain could accomplish it; sooner or later, some survey-taker would come by. Therefore, as a consequence of existing in today's society, one cannot help revealing information about oneself in exchange for what is expected from society and its institutions. And what do we expect? We expect credit; we expect medical care; we expect education; we expect employment and all the other benefits of an affluent society. For each of them that we must have and must fulfill, information about ourselves will unavoidably be kept in records. 68

This practice of compiling records requires that society specify which activities may be recorded and which require the consent of the subject. Obviously, privacy is not protected unless an individual has the right to approve the release of information in his records. An individual may waive that right by giving the information in exchange for a benefit that he would not have received otherwise. A government report in 1975 noted:

Except for narrow limitations drawn from the First Amendment

66. Id.
68. W. Ware, supra note 4, at 5.
and various antidiscrimination statutes, the government and private corporations are free to seek any information they think relevant. . . . The private individual who needs a job or a credit card is likely to submit to whatever disclosures are necessary to get what he wants, unless they are extraordinarily objectionable. The agency having to make a decision about employment or the grant of credit has no strong interest in minimizing the information sought; it makes sense for it to seek whatever can be processed and appears likely to be relevant. Thus, unless an agency or private organization chooses to restrain itself in the public interest, no one is in the position of answering whether the benefit of having the information outweighs the intrusion upon privacy of getting it.69

Thus, courts may be forced to deal with two kinds of consent: implied consent by the individual seeking something and inferred consent by the recipient of the information.

Often there are questions on . . . forms that are not directly relevant to the purposes of the instrument, but the applicant knows that a recalcitrant refusal to supply some of the information, because it is too personal, will meet with prompt disfavor. . . . It is difficult to conceive of information given under these circumstances as voluntary, but consent to use information obtained in these standard ways is almost always inferred.70

Legally, the information may be used only in the manner consented to and may not be passed on to someone else for the purpose of invading an individual’s privacy. “In practice, however, it is difficult to prevent this kind of traffic in personal information because of the difficulty in tracing it.”71

One of the leading consent cases is Merriken v. Cressman.72 A school district was sued over a proposed drug rehabilitation program. The district sent letters to parents in an attempt to get their consent for their children’s participation, without informing the parents of all of the details of the program. In fact, children who were thought to be potential drug abusers would be reported to the school superintendent, who would then use teachers, guidance counselors and others to try to avert the problem.73

The district court noted that the parents, not the children, were asked to give consent, which was a violation of the students’ constitutional rights. “Waivers of constitutional rights not only must be voluntary but must be knowing, intelligent and done with sufficient

70. Meldman, supra note 19, at 20.
71. Id.
73. Id. at 919-20.
awareness of the relevant circumstances and likely consequences." The court attempted to define proper consent:

[A]ny attempt [in this case] at informed consent does not reach the level that this Court would consider adequate as in the "consent ideally obtained by a physician prior to the performance of surgery." The parents are not aware of the consequences and there is no substitute for candor and honesty in fact . . . . The attempt to make the letter requesting consent similar to a promotional inducement to buy, lacks the necessary substance to give a parent the opportunity to give knowing, intelligent and aware consent.

Finally, the court criticized the school district for planning to reveal the records to the superintendent and others, although the parents and children would have been unaware of it, rather than maintaining "strict confidentiality" of the records.

QUBE poses a special problem in the consent area because users are constantly supplying information about themselves and it is all stored on computers. For example, the fact that a particular person viewed a soft-core pornographic film on his television is recorded. When an announcer asked if gays should be allowed to teach in public schools, the identities and votes of the voters were recorded. This extensive recording concerned the Office of Telecommunications Policy, which suggested that "whether or not control is needed of the equipment used to tell the channel to which an ordinary television set is tuned, it is clear that cable television must be regulated to assure the privacy of individual subscribers."

The entire area of inferred consent is summed up by Arthur Miller as "perhaps the most significant weakness in today's common law privacy action." "In too many instances 'consent' is used as a convenient epithet that places responsibility for a loss of privacy on the victim and absolves the intruder." He concludes with a stinging appraisal of what is needed:

In view of the growing threat to privacy from the new technologies, every assertion of consent and waiver by information system operators must be regarded with considerable skepticism. These defenses always must be carefully evaluated because their effect is to permit data handlers and users to shift the risks of their activities to individual file subjects. If we are to do more than pay lip service to the right of informational privacy, the law must impose a duty of care on the data gatherer that is commensurate with the degree of

75. 364 F. Supp. at 920.
76. Id.
77. K. Greenawalt, supra note 69, at 44.
78. A. Miller, supra note 5, at 185.
79. Id. at 186.
VII. COMPUTER OWNER LIABILITY

When computerized information has been exposed to the public and individual privacy has been invaded, a natural reaction would be to file a negligence suit against the computer owner, claiming that the data was protected inadequately. The liability of the computer owner has been of concern.

The increasing use of computers in sensitive areas of activity in the public and private sectors has led to increasing abuses, because the security systems which would make technology impervious to misuse have not kept up with technological advances in computers. Unfortunately, criminality, as defined by legislatures, is not sufficiently flexible to cope with such clear abuses as . . . negligent disclosure of personal information from data banks.\(^{81}\)

Three federal cases have developed the liability standards for computer owners.

In *Palmer v. Columbia Gas of Ohio*,\(^ {82}\) a class action suit was filed against a Toledo natural gas supplier, charging that the company violated consumers’ constitutional rights of due process because it cut off gas service arbitrarily. Many customers, including some who had paid their bills, were cut off with no warning. The company used a computerized billing system. Whenever readings were not taken at the consumers’ gas meters, the computer would estimate usage, usually below actual usage. Thereafter, when actual readings were taken, consumers would receive cumulative bills that were so high that some of them, particularly low income customers, could not pay.\(^ {83}\)

In ordering new billing and termination regulations, the district court castigated the company, noting that “[t]he evidence as a whole revealed a rather shockingly callous and impersonal attitude upon the part of the defendant, which relied uncritically upon its computer, located in a distant city. . . .”\(^ {84}\)

Computer error presumably will not be tolerated by the courts if the owner has been negligent. Negligence by the owner of a computer was also examined in *Port City State Bank v. American National Bank*.\(^ {85}\) Port City sued for collection on two checks that

---

80. *Id.* at 186-87.
83. *Id.* at 242-43.
84. *Id.* at 243.
85. 486 F.2d 196 (10th Cir. 1973).
American National did not return as insufficient before a midnight
deadline. American National’s defense was that its new computer
developed a memory error, which a repairman assured the bank
could be corrected that day. However, when the computer was
started up the next day, there was a second breakdown, and another
two days were lost before service could be restored. American Na-
tional began using another computer at a bank two hours and thirty
minutes away as soon as they realized that repairs could not be
made immediately. In ruling for American National, the Court of
Appeals found that the bank had demonstrated the diligence re-
quired in an emergency.

The statute does not require perfection on the part of [American
National], and American National’s performance should not be
judged on the basis of 20-20 hindsight . . . . Further, there was evi-
dence to indicate that such computer breakdowns are generally re-
paired very quickly. Thus it would appear that appellee was
justified in its initial delay in adopting emergency procedures based
on its belief [that] such measures would prove unnecessary.

Negligence was expanded further in *United States v. Jones*. This case resulted when the supervisor of accounts payable at a
Canadian firm created a computer account that issued five checks to
a Maryland accomplice. In finding that forgery had been commit-
ted, the district court said:

The mere fact that a computer was used to print these checks
should not be permitted to confuse the matter. The computer was
merely an inanimate and obedient instrumentality employed by
Everston (the supervisor), who himself accomplished everything
necessary to assure the issuance of checks to an unauthorized
payee, and was, as a practical matter, the drawer of the checks.
Like a checkwriting machine or a ball point pen, the computer did
effectively what it was told to do by its program and by the data in-
serted at Everston’s command. Likewise, the keypunch operator’s
function was to follow instructions exactly and to punch into com-
puter cards exactly the information given. It was only by means of
this mechanical process that the computer could digest the informa-
tion, and it is fair to say that the operator, acting routinely, func-
tioned in a sense as an adjunct of the machine. At most, the
computer operator was the innocent agent of Everston.

These cases illustrate that, while human negligence will not be
tolerated, computer malfunctions may be allowed, if the computer

86. *Id.* at 198-99.
87. *Id.* at 200.
89. *Id.* at 966.
90. *Id.* at 969.
owner made a diligent effort to protect the information. The courts must decide where to balance the rights of consumers and computer owners.

The fact that computers pose special problems in gathering evidence clouds the picture even further.

A computer malfunction will probably occur within one or two nano-seconds (billionths of a second). Because humans are unable to monitor these machine functions closely, proof of computer error is extremely difficult. In addition, there are few established minimum standards that govern the conduct of the computer user. Consequently, plaintiffs who suffer injury because of a computer error will attempt to rely on the doctrine of res ipsa loquitur (mere proof that an accident took place is sufficient under the circumstances to warrant an inference that it was caused by defendant's negligence).

In order to establish a res ipsa case, the plaintiff must show that the event—the computer error—does not usually happen in the absence of someone's negligence; that the instrumentality—the computer—was in the defendant's exclusive control; and that the plaintiff did not contribute to his own injury. The successful application of this doctrine to the computer field will ultimately depend on the degree to which courts recognize the "usual reliability" of such machines.91

CONCLUSION

A final decisive factor in the issue of individual privacy and computers is the cost of a security system. Elaborate computer security devices are expensive.

Technological security . . . must be paid for. There has so far been no profit motive within the computer industry for security systems, and it is unlikely that internal competition will generate much interest in developing this phase of the technology. As the computer becomes used more and more in privacy-sensitive areas, however, the industry will be forced to realize that it is marketing a potentially dangerous product. Like any other manufacturer of dangerous merchandise, the computer industry will be expected to take the responsibility for providing the necessary safety features. This responsibility has generally been considered the price that a maker of a dangerous product must pay for the privilege of selling the product to the public. Industries that have attempted to shirk this responsibility have usually found themselves subject to legislative regulations, as the example of the automobile industry demonstrates.92

92. Meldman, supra note 19, at 26 (footnote omitted).
Most people probably do not value privacy enough to pay the price necessary to protect it on computers. Willis Ware believes that the issue of computers and privacy has placed society at a crossroads and that the decisions made through the next generation will have a huge impact on the future of the world.

If the privacy problem is not dealt with now, there is a reasonable expectation that future generations will be raised in a different information culture with a different expectation; the privacy problem will conveniently get overlooked and forgotten. . . . We will find a population that is completely enumerated, i.e., everyone has a universal identifier; we will find much broader use of information to constrain individuals' actions in undesirable or, perhaps, distasteful ways. New generations, having been brought up in a new culture, will accept it. Thus, there is no automatic carry-forward that will assure that the privacy cause will stay prominent in society. There is an immediacy about privacy that indicates we have to do it now.\textsuperscript{93}

\textsuperscript{93} W. Ware, \textit{supra} note 4, at 6.