UIC Law Review

Volume 17 | Issue 3 Article 6

Summer 1984

Intrustions upon Informational Seclusion in the Computer Age, 17 J. Marshall L. Rev. 831 (1984)

John A. McLaughlin

INTRUSIONS UPON INFORMATIONAL SECLUSION IN THE COMPUTER AGE

INTRODUCTION

The use of computers[1] as a means of accumulating information concerning the personal, economic, and social status of individuals has become widespread[2] in our modern "information society."[3] Government agencies and private business concerns now use computers to collect, analyze, store, and disseminate mass quantities of private and confidential information about individuals.[4] Additionally, the small cost of personal home computers has made information processing available to members of the general public.[5] The advent of data-banks which can be accessed by remote computer terminals through common telephone lines presents an unprecedented potential for the collec-

1. Essentially, a computer is a machine which "receives, stores, manipulates and communicates information." Toong & Gupta, *Personal Computers*, SCIENTIFIC AMERICAN, December 1982, at 87. "Information is entered into the computer by means of a keyboard or is transferred into it from secondary storage on magnetic tapes or disks. The computer's output is displayed on a screen . . . [or on] a separate printer unit." *Id.* at 88. Computers can transmit or receive signals from other computers by use of a device called a *modem*, which transmits computer signals over common telephone lines. *Id.*

2. Tunick, *Computer Law: An Overview*, 13 LOY. L.A.L. REV. 315, 332 (1980) (presenting an overview of computer law for legal practitioners with little background in the area of computers). Computers are used, for example, to manipulate information about an individual's credit, medical services, employment, insurance and education. *Id.* at n.84.

3. *See* THE REPORT OF THE PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977) [hereinafter cited as PRIVACY REPORT]. The report, which apparently coined the term "information society," recommends that Congress take measures to accord individuals the right to exert some control over information which is maintained about them by the government and private business concerns. For a discussion of the federal legislation that was enacted after the Privacy Study, see Trubow & Hudson, *The Right to Financial Privacy Act of 1978: New Protection from Federal Intrusion*, 12 J. MAR. J. PRAC. & PROC. 487 (1979).

4. Soma & Wehmhoefer, *A Legal and Technical Assessment of the Effect of Computers on Privacy*, 60 DEN. L.J. 449 (1983) (calling for an international convention to ensure that privacy protections are maintained by binding agreements that govern information flows).

5. Presently, for a total cost of less than $400, computer systems can be purchased which can interact with remote data-banks. *Super Systems for Under $1,000*, MONEY GUIDE, 1984, at 130. In 1981, approximately 2.8 million computers were sold. Soma & Wehmhoefer, *supra* note 4, at 453. By 1985, it is estimated that computer sales, worldwide, will exceed 50 million units. *Id.* "As computers become more readily available to individuals, more personal data will be accessible in machine readable form." *Id.*

tion and dissemination of personal information with increasing speed.[6]

The potential for abuse that has accompanied the ability to make remote computers interact with one another has generated much concern about the individual's privacy interest in computer stored information.[7] Today's newspapers report of computer enthusiasts penetrating the computer files of banks, hospitals and even government agencies.[8] Generally, as each data-bank is penetrated, private and confidential information concerning individuals is divulged.[9] Intruders who intentionally gain unauthorized access to personal information do so at the expense of others' privacy interests. They must be held accountable for their acts. The courts, therefore, must be prepared to apply the law of privacy to this new phenomenon.

The right of privacy recognizes the right to be free from unauthorized intrusions into private matters.[10] This comment maintains that information files in computer data-banks which contain private and confidential information about individuals constitute areas of seclusion which current privacy principles can and must protect. Following a brief discussion of the new

---

6. Sokolik, *Computer Crime—The Need for Deterrent Legislation*, 2 COMPUTER L.J. 353, 355 (1980) (discussing the "explosion" of computer technology).

7. Concern about the effects of computers on privacy has generated a significant amount of commentary. *See, e.g.*, Freedman, *The Right of Privacy in the Age of Computer Data and Processing*, 13 TEX. TECH. L. REV. 1361 (1982) (advocating that general and specific standards of privacy law be transformed into binding covenants among the nations); Linowes, *Must Personal Privacy Die in the Computer Age?*, 65 A.B.A.J. 1180 (1979) (urging establishment of a national privacy policy with consistent guidelines); Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1089 (1969) (examining the existing legal framework's capacity to deal with information related problems in the computer age); Soma & Wehmhoefer, *supra* note 4; Tunick, *supra* note 2.

8. *See, e.g., Computer Whiz Held in Defense "Break-in"*, Chicago Sun-Times, Nov. 4, 1983, at 13, col. 1 (reporting that a young computer enthusiast had used his personal home computer "to tap into an international computer network linking research agencies working for the Defense Department"); *Computers Seized as FBI Probes Wire Fraud*, Chicago Sun-Times, Oct. 14, 1983, at 11, col. 3 (reporting that 12 homes in six states had been raided by the FBI and that computer equipment was seized which "may have been used illegally to tap corporate and other commercial computers for economic gain or to cause damage").

9. *See* Miller, *The Dossier Society*, 1971 U. ILL. L.F. 154 (examining the implications of data technology and information systems on individual privacy).

10. *See, e.g.*, Vernars v. Young, 539 F.2d 966 (3d Cir. 1976) (intrusion into private mail actionable); Hamberger v. Eastman, 106 N.H. 107, 206 A.2d 239 (1964) (landlord's concealing of a listening and recording device in tenant's bedroom actionable). *See generally* Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389-92 (1960).

threat to informational privacy, this comment examines and resolves key issues that may arise in applying the privacy action of *intrusion upon seclusion* to the computer age's new means of invading privacy. Finally, this comment concludes that a cause of action exists for unauthorized intrusions upon informational seclusion.

THE RIGHT OF PRIVACY

Recognition of privacy as an independent right is usually considered to have emanated from an article written by Samuel Warren and Louis Brandeis in 1890.[11] Warren and Brandeis urged that then existing doctrines, especially those found in the law of intellectual property, provided principles upon which an independent right of privacy could be recognized.[12] Shortly thereafter, in *Pavesich v. New England Life Insurance Co.*,[13] the Supreme Court of Georgia became the first court to recognize an independent right of privacy.[14] Since *Pavesich*, the vast majority of jurisdictions have adopted the right, either judicially or by statute,[15] recognizing that the right of privacy is the "most com-

11. Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). According to Dean Prosser, the right of privacy "is perhaps the outstanding illustration of the influence of legal periodicals upon the courts." W. PROSSER, HANDBOOK OF THE LAW OF TORTS 802 (4th ed. 1971). For a thorough report of the impetus of Warren and Brandeis' article, see Prosser, *supra* note 10, at 383.

12. Warren & Brandeis, *supra* note 11, at 197-205.

13. 122 Ga. 190, 50 S.E. 68 (1905) (defendant's use of plaintiff's name and picture in an advertisement held to be an invasion of plaintiff's privacy). Only three years earlier, the right of privacy had been rejected by the New York Court of Appeals in Roberson v. Rochester Folding Box Co., 171 N.Y. 538, 64 N.E. 442 (1902) (defendant made unauthorized use of plaintiff's picture to advertise flour).

14. At the time of *Pavesich*, other courts were also beginning to seriously consider the right of privacy. *See, e.g.*, Itzkovitch v. Whitaker, 115 La. 479, 482, 39 So. 499, 500 (1905) ("Every one who does not violate the law can insist upon being let alone. In such a case the right of privacy is absolute.").

15. Adoption of the right of privacy has generally occurred in the courts. *See, e.g.*, Reed v. Real Detective Pub. Co., 63 Ariz. 294, 162 P.2d 133 (1945); Goodrich v. Waterbury Republican-Am., Inc., 188 Conn. 107, 448 A.2d 1317 (1982); Pavesich v. New England Life Ins. Co., 122 Ga. 190, 50 S.E. 68 (1905); Eick v. Perk Dog Food Co., 347 Ill. App. 293, 106 N.E.2d 742 (1952); Munden v. Harris, 153 Mo. App. 652, 134 S.W. 1076 (1911); Hamberger v. Eastman, 106 N.H. 107, 206 A.2d 239 (1964); Billings v. Atkinson, 489 S.W.2d 858 (Tex. 1973); Roach v. Harper, 143 W. Va. 869, 105 S.E.2d 564 (1958).

Some courts preferred to leave adoption of the right of privacy to the legislature. *See, e.g.*, Brunson v. Ranks Army Store, 161 Neb. 519, 524-25, 73 N.W.2d 803, 806 (1955); Yoeckel v. Samonig, 272 Wis. 430, 434, 75 N.W.2d 925, 927 (1956). The legislatures responded. *See, e.g.*, NEB. REV. STAT. §§ 20-201 to 211 (Supp. 1982) (recognizing traditional rights of action for invasion of privacy); R.I. GEN. LAWS § 9-1-28.1 (Supp. 1983) (adopting rights of action for intrusion, publication of private facts, false light and appropriation); WIS. STAT. § 895.50 (1982) (recognizing cause of action for invasion of privacy ex-

prehensive of rights and the right most valued by civilized men."[16]

In 1960, Dean Prosser categorized the more than 300 privacy cases that had been decided since 1890.[17] Prosser found that the law of privacy was comprised of four types of invasions which, though having almost nothing in common, constituted an interference with the plaintiff's right "to be let alone."[18] Prosser categorized the four types of invasions as: 1) intrusion upon seclusion or solitude;[19] 2) public disclosure of private facts;[20] 3) placing the plaintiff in a false light;[21] and 4) appropriation of

---

cept for the false light action). *See generally* R. SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (1981) (providing a survey of statutes relating to privacy).

16. Olmstead v. United States, 277 U.S. 438, 478 (1927) (Brandeis, J., dissenting) (holding that the fourth amendment does not prohibit wiretaps). The view of Justice Brandeis eventually prevailed in Katz v. United States, 389 U.S. 347 (1967) (holding that the fourth amendment protects the privacy of people and not places).

17. *See* Prosser, *supra* note 10.

18. *Id.* at 389.

19. *Id.* at 339-92. *See infra* text accompanying notes 52-66 for a discussion of the intrusion upon seclusion action.

20. Prosser, *supra* note 10, at 392-98. Generally, one who publicly discloses private facts or matters concerning the plaintiff will be held liable if the disclosure of such facts would be considered highly objectionable to persons of ordinary sensibilities. *Id. See, e.g.*, Briscoe v. Reader's Digest Ass'n, Inc., 4 Cal. 3d 529, 483 P.2d 34, 93 Cal. Rptr. 866 (1971) (publication of plaintiff's name in connection with criminal activity that plaintiff was involved in 11 years earlier was highly objectionable and actionable); Munley v. ISC Financial House, Inc., 584 P.2d 1336 (Okla. 1978) (creditor's agents, who left their business cards tacked to debtor's apartment door following attempts to contact debtor, did not conduct themselves in an objectionable manner). Prosser defined the protected interest as "that of reputation, with the same overtones of mental distress that are present in libel and slander." Prosser, *supra* note 10, at 398. When the published matter is of legitimate concern to the public, or is newsworthy, the publication will not give rise to liability. *See, e.g.*, Miller v. News Syndicate Co., 445 F.2d 356 (2d Cir. 1971) (news article reporting of plaintiff's participation in a heroin smuggling syndicate held newsworthy); Hubbard v. Journnal Pub. Co., 69 N.M. 473, 368 P.2d 147 (1962) (newspaper article which reported that plaintiff's older brother sexually assaulted her and was required to spend 60 days in juvenile home held newsworthy).

21. Prosser, *supra* note 10, at 398-401. One who publicizes matter which places another in a false light is liable for invasion of privacy if the false light would be considered objectionable by reasonable persons. *Id. See, e.g.*, Leverton v. Curtis Pub. Co., 192 F.2d 974 (3d Cir. 1951) (article "They Ask to be Killed" using a picture of a child that had been hurt in an accident); Rinsley v. Frydman, 221 Kan. 297, 559 P.2d 334 (1977) (publication that plaintiff, a doctor, had been mentally ill held actionable). If the published statements are true, there is no liability for false light. *See, e.g.*, Goodrich v. Waterbury Republican-Am., Inc., 188 Conn. 107, 448 A.2d 1317 (1982) (publication that liens and law suits had been filed against plaintiff not actionable because publication was true).

the plaintiff's name or likeness.[22] Prosser's categorization was subsequently adopted by the American Law Institute[23] and has been generally accepted by the courts.[24]

The right of privacy has been variously defined as the right to be let alone,[25] the right of one's peace of mind,[26] the right to autonomy,[27] and the right to control knowledge about oneself.[28] Perhaps the most inclusive statement of the right, however, was that of Warren and Brandeis, who suggested that the right was "that of inviolate personality,"[29] the right of the "individual's independence, dignity and integrity."[30] "Inviolate personality" recognizes that every individual is unique and must be able to determine for himself how personal information will be circulated.[31] Without "inviolate personality," individuality cannot

22. Prosser, *supra* note 10, at 401. Appropriation of the plaintiff's name or likeness for benefit or advantage constitutes an invasion of plaintiff's privacy. *Id.* The interest protected by this tort, according to Prosser, is plaintiff's proprietary interest in the exclusive use of his identity. *Id.* at 406. *See, e.g.*, Pavesich v. New England Life Ins. Co., 122 Ga. 190, 50 S.E. 68 (1905) (defendant used plaintiff's name and picture for advertising purposes); Zacchini v. Scripps-Howard Broadcasting Co., 47 Ohio St. 2d 224, 351 N.E.2d 454 (1976) (television station showed film of plaintiff's performance as a "human cannonball"—held not actionable because it was newsworthy). *See also* Hinish v. Meir & Frank Co., 166 Or. 482, 113 P.2d 438 (1941) (defendant signed plaintiff's name on a telegram to the governor recommending that the governor veto certain proposed legislation).

23. *See* RESTATEMENT (SECOND) OF TORTS §§ 652A-652I (1977).

24. *See, e.g.*, Winegard v. Larsen, 260 N.W.2d 816, 822 (Iowa 1977); Nelson v. Times, 373 A.2d 1221, 1223 (Me. 1977); Hamberger v. Eastman, 106 N.H. 107, 110, 206 A.2d 239, 241 (1964). It was the courts' general acceptance of Prosser's categorization that prompted Professor Bloustein to write an article attempting to demonstrate that Prosser was wrong. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 964 (1964) (considering privacy to be a unitary tort, as opposed to four, which constitutes an assault upon human dignity).

25. *E.g.*, Estate of Berthiaume v. Pratt, 365 A.2d 792, 795 (Me. 1976).

26. Fairfield v. American Photocopy Equip. Co., 138 Cal. App. 2d 82, 86, 291 P.2d 194, 197 (1955) (invasion of a person's privacy "impairs the mental peace and comfort of the person and may cause suffering much more acute than that caused by bodily injury"), *aff'd second appeal*, 158 Cal. App. 2d 53, 322 P.2d 93 (1958).

27. *E.g.*, Price v. Sheppard, 307 Minn. 250, 257, 239 N.W.2d 905, 910 (1976) ("At the core of . . . privacy . . . is the concept of personal autonomy . . . ."). *See* Bazelon, *Probing Privacy*, 12 GONZ. L. REV. 587, 588 (1977) (privacy as "the unitary concept of separation of self from society").

28. *E.g.*, Fried, *Privacy*, 77 YALE L.J. 475, 483 (1968) (viewing privacy as necessary to "ends and relations of the most fundamental sort: respect, love, friendship and trust").

29. Warren & Brandeis, *supra* note 11, at 205.

30. Bloustein, *supra* note 24, at 971.

31. *Id. See* A. WESTIN, PRIVACY AND FREEDOM 33 (1967). "In democratic societies there is a fundamental belief in the uniqueness of the individual, in his basic dignity and worth as a creature of God and a human being, and in the need to maintain social processes that safeguard his sacred individuality." *Id.* In order to maintain individuality, individuals must be able "to

exist.[32]

However one chooses to define the right of privacy, it is rather certain that the definition would encompass a right to grant or deny access to private and confidential information about ourselves to others.[33] There are certain aspects of each individual's life, or particular facts concerning each individual's past, which individuals consider to be "nobody's business." The various definitions reflect this fact.[34]

THE THREAT TO INFORMATIONAL PRIVACY

In the past, information concerning particular individuals was highly decentralized.[35] Individual records were rarely circulated beyond their place of origin.[36] Personal information was difficult to secure and compile, making large quantities of information concerning one individual unavailable.[37] Computer technology, however, has made these protections part of a lost era.[38] Information can now be collected, analyzed and disseminated quickly and in great quantity.[39]

---

determine for themselves when, how, and to what extent information about them is communicated to others." *Id.* at 7.

32. *See* A. WESTIN, *supra* note 31, at 46 (discussing why individuality plays an important role in society).

33. *See* Fried, *supra* note 28, at 482 (defining privacy as "the *control* we have over information about ourselves") (emphasis in original). *See also* Duncan & Wolfe, *Informational Privacy: The Concept, Its Acceptance and Affect on State Information Practices*, 15 WASHBURN L.J. 273, 276 (1976) (defining informational privacy as "the right of an individual to control the collection, maintenance, use and dissemination of personal information").

34. *See, e.g.*, Duncan & Wolfe, *supra* note 33, at 276; Freedman, *supra* note 7, at 1362 (privacy as "the individual's ability to control the circulation of information about him or her—a power that is essential to maintaining social relationships and personal freedom"); Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 236 (1977) (privacy "as an autonomy or control over the intimacies of personal identity"); Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34, 35-6 (1967) (privacy as "the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him are limited").

35. Miller, *supra* note 9, at 158. Information concerning particular individuals was "limited and local in nature." PRIVACY REPORT, *supra* note 3, at 3. Records pertaining to births, baptisms, marriages and deaths were generally maintained by local churches. *Id.* Financial records were generally maintained by local merchants and bankers, and credit was usually extended solely on the basis of the creditor's personal knowledge of the borrower's credit history and circumstances. *Id.* at 4.

36. PRIVACY REPORT, *supra* note 3, at 4.

37. Miller, *supra* note 9, at 158.

38. *Id.*

39. Sokolik, *supra* note 6, at 355. The rate at which computer technology has progressed is exemplified by the following analogy:

> If the aircraft industry had evolved as spectacularly as the computer industry over the past 25 years, a Boeing 767 would cost $500 today, and it would circle the globe in 20 minutes on five gallons of fuel. Such per-

Government agencies and private businesses now compile information about individuals "as a matter of course."[40] Banks, hospitals, universities, corporations and government agencies have become information hoarders. According to Professor Arthur Miller:

> [E]ach time a citizen files a tax return, applies for life insurance or a credit card, seeks government benefits, or interviews for a job, a dossier is opened under his name and his informational profile is sketched. It has now reached the point at which whenever we travel on a commercial airline, reserve a room at one of the national hotel chains, or rent a car we are likely to leave distinctive electronic tracks in the memory of a computer—tracks that can tell a great deal about our activities, habits, and associations when collected and analyzed.[41]

The threat to informational privacy becomes exceedingly clear[42] when one considers the fact that some individual at a remote computer terminal can gain unauthorized access to such files and use or abuse the information as he chooses.

Advances in computer security have been unable to prevent unauthorized access to computer data-banks.[43] The ability to recognize the vulnerability of data-banks and to develop adequate safeguards lags behind the ability of intruders to gain access to personal files.[44] The lack of adequate safeguards

---

formance would represent a rough analogue of the reduction in cost, the increase in speed of operation and the decrease in energy consumption of computers.

Toong & Gupta, *supra* note 1, at 87.

40. PRIVACY, A PUBLIC CONCERN: A RESOURCE DOCUMENT 1 (K. Larsen ed. 1975). *See infra* text accompanying note 41.

41. Miller, *supra* note 9, at 155.

42. Courts have also taken notice of the threat to privacy which is posed by the computer age. *See, e.g.*, Whalen v. Roe, 429 U.S. 589, 605 (1977) ("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.").

43. Volgyes, *The Investigation, Prosecution, and Prevention of Computer Crime: A State-of-the-Art Review*, 2 COMPUTER L.J. 385, 392 (1980). "[M]ultiple users, dispersed access, and remote manipulation pose problems that lie outside of the sphere of conventional prevention and detection methods." *Id.* Management's ability to institute controls cannot keep up with computer technology. *Id.* Recognizing potential threats to a computer system takes time, and instituting adequate safeguards takes an even longer time. *Id.* According to some security experts, however, the amount of computer invasions could be sharply decreased by simple precautions such as instituting longer computer passwords. Browne, *Locking Out the Hackers*, DISCOVER, Nov. 1983, at 30, 38. If computer data-bank owners recognized the vulnerability of their computers, a significant number of intrusions which now occur could be stopped. *Id.* at 31.

44. Volgyes, *supra* note 43, at 392. Upon gaining access to a computer's data-banks, an intruder can perpetrate such crimes as fraud, embezzlement, theft, larceny, extortion, espionage and sabotage. *Id.* at 386. *See, e.g.*, Ward v. Superior Court, 3 Computer L. Serv. Rep. 206 (Cal. Super. Ct. 1972)

"threaten[s] to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-top.' "[45]

Informational privacy refers to the right of an individual to control the extent to which private and confidential information concerning himself will be collected, maintained, used and disseminated.[46] It is a right to control the way in which an individual's personal attitudes and beliefs will be known to others.[47] It is a right which encompasses the power to ensure that private information which has been disclosed for a particular purpose will remain confidential.[48]

A right of individuals to maintain areas of informational seclusion is essential to preserving individuality.[49] Individuality cannot exist when one's "every need, thought, desire, fancy or

---

(defendant allegedly gained unauthorized access to a remote computer and stole a trade secret). *See also supra* note 8.

Computer crime has been the subject of much commentary. *See, e.g.*, Ingraham, *On Charging Computer Crime*, 2 COMPUTER L.J. 429 (1980) (discussing problems encountered by prosecutors when charging computer crime); Kling, *Computer Abuse and Computer Crime as Organizational Activities*, 2 COMPUTER L.J. 403 (1980); Sokolik, *supra* note 6 (discussing the need for computer crime legislation).

In order to combat computer crime, some states have enacted "computer crime" statutes. *See, e.g.*, CAL. PENAL CODE § 502 (West Supp. 1983); ILL. REV. STAT. ch. 38, §§ 15-1, 16-9 (1983); N.M. STAT. ANN. §§ 30-16A-1 to 4 (Supp. 1983); UTAH CODE ANN. §§ 76-6-701 to 703 (Supp. 1983). *See generally* M. BENDER, COMPUTER LAW: EVIDENCE AND PROCEDURE § 4.07, at 4-71 (1982) (complete list of current computer crime statutes). As a representative example, the Utah computer crime statute provides, in part:

> 76-6-703 Computer Fraud Act—Offenses—Degree of Offense. Any person who willfully gains access to any computer, computer system, computer network, computer software, computer program or any computer property, who knowingly and willfully provides false information or who causes any other person directly or indirectly to enter false information into any computer, computer system, computer software, computer program, and thereby devises or executes any scheme or artifice to defraud or obtain money, property, or services, including the unauthorized use of computer time, under false pretenses, representations, or promises, including representations made to a computer, and thereby alters, damages or destroys any computer, computer system, computer network, computer software, computer program, or computer property, is guilty of a criminal offense . . . .

UTAH CODE ANN. § 76-6-703 (Supp. 1983).

45. Warren & Brandeis, *supra* note 11, at 195.

46. *See* Comment, *The Use and Abuse of Computerized Information: Striking a Balance Between Personal Privacy Interests and Organizational Information Needs*, 44 ALB. L. REV. 589, 601 (1980) [hereinafter cited as *The Use and Abuse of Computerized Information*] (proposing enactment of statutes to resolve conflicts between individual privacy rights and business information needs).

47. *Id.* at 600.

48. *Id.* at 602.

49. *See supra* notes 29-32 and accompanying text.

gratification is subject to public scrutiny."[50] If personal privacy is to survive the computer age, all courts must recognize the right of individuals to maintain areas of informational seclusion. Absent strict application of privacy law to this new means of invading informational privacy, the computer age "will turn society into a transparent world in which our home, finances, and our associations are bared to the most casual observer."[51] Unauthorized prying into private or confidential information of or about another is an intrusion upon seclusion which ought to be held actionable with limited restriction.

INTRUSION UPON SECLUSION

Intentional intrusion upon the solitude or seclusion of another constitutes an actionable invasion of privacy if reasonable persons would consider the intrusion highly offensive.[52] This form of invasion of privacy does not require that the private matters intruded upon be publicized[53] but, rather, consists solely of an intentional[54] intrusion into places or affairs in which an individual maintains an expectation of privacy.[55] The defendant's intrusion may be physical as, for example, by unau-

50. Bloustein, *supra* note 24, at 1003. According to Professor Bloustein, without informational privacy:

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

Id.

51. Miller, *supra* note 9, at 154.

52. *See, e.g.*, Vernars v. Young, 539 F.2d 966 (3d Cir. 1976) (intrusion into personal mail actionable); Welsh v. Pritchard, 125 Mont. 517, 241 P.2d 816 (1952) (defendant landlord and his wife entered tenant's premises and remained for 17 days and nights in living room); Hamberger v. Eastman, 106 N.H. 107, 206 A.2d 239 (1964) (eavesdropping into tenant's private affairs with a concealed microphone actionable). *See generally* Prosser, *supra* note 10, at 389-92. Not all jurisdictions have recognized a cause of action for intrusion upon seclusion. *See, e.g.*, Kelly v. Franco, 72 Ill. App. 3d 642, 646, 391 N.E.2d 54, 57-8 (1979) (noting that, in Illinois, actions for invasion of privacy are limited to appropriation of one's name or likeness).

53. *E.g.*, Phillips v. Smalley Maint. Serv., Inc., 435 So. 2d 705, 709 (Ala. 1983); Lamberto v. Brown, 326 N.W.2d 305, 309 (Iowa 1982). *See* Prosser, *supra* note 10, at 389-92.

54. For a discussion of the standard of fault in privacy cases, see Note, *Tortious Invasion of Privacy: Minnesota as a Model*, 4 WM. MITCHELL L. REV. 163, 197-205 (1978).

55. *E.g.*, LeCrone v. Ohio Bell Tel. Co., 120 Ohio App. 129, 201 N.E.2d 533 (1963) (telephone conversations). *See also* Phillips v. Smalley Maint. Serv., Inc., 435 So. 2d 705 (Ala. 1983) (employer's intrusive and coercive sexual demands upon employee, including inquiry into nature of employee's sexual relationship with husband, held actionable as an intrusion).

thorized entry into plaintiff's home or private room.[56] Alternatively, the intrusion may be mechanical, such as by eavesdropping or wiretapping.[57]

The applicability of the intrusion upon seclusion action to the computer age problem of unauthorized access rests primarily upon resolution of two issues. The first issue is whether computer data-banks constitute areas of *seclusion*. The second issue is whether gaining unauthorized access to such data-banks from a *remote* computer terminal constitutes an actionable *intrusion*. In order to state a cause of action for intrusion upon seclusion, both of these issues must be answered in the affirmative.[58]

---

56. *E.g.*, Newcomb Hotel Co. v. Corbett, 27 Ga. App. 365, 108 S.E. 309 (1921) (intrusion into plaintiff's hotel room); Welsh v. Pritchard, 125 Mont. 517, 241 P.2d 816 (1952) (intrusion into plaintiff's apartment).

57. *E.g.*, Rhodes v. Graham, 238 Ky. 225, 37 S.W.2d 46 (1931) (wiretap); Hamberger v. Eastman, 106 N.H. 107, 206 A.2d 239 (1964) (microphone). Wiretapping has been made criminal in a majority of states. *See, e.g.*, CAL. PENAL CODE § 632 (1970 & Supp. 1983); ILL. REV. STAT. ch. 134, § 15a (1983). For a complete list of wiretapping statutes, see R. SMITH, *supra* note 15, at 23.

58. Once the plaintiff has proved that the defendant intruded into an area in which plaintiff had a reasonable expectation of privacy, general damages will be presumed if reasonable persons would consider the intrusion highly offensive. *See, e.g.*, Roach v. Harper, 143 W. Va. 869, 105 S.E.2d 564 (1958) (plaintiff stated cause of action for invasion of privacy without alleging special damages). The fact that the plaintiff did not suffer any pecuniary harm from the invasion is not important, although proof of such damage can increase defendant's liability. Prosser, *supra* note 10, at 409. While some courts will only award nominal damages absent proof of pecuniary harm, most courts will permit compensatory damages for mental suffering without proof of any physical harm if the defendant's invasion was willful. *See, e.g.*, Olan Mills, Inc. of Texas v. Dodd, 234 Ark. 495, 353 S.W.2d 22 (1962) (plaintiff in appropriation case allowed to recover damages for humiliation, embarrassment, mental anguish, loss of weight from worry, and lack of sleep without showing physical injury); Trevino v. Southwestern Bell Tel. Co., 582 S.W.2d 582, 584 (Tex. Civ. App. 1979) (plaintiff, unable to prove actual damages, and failing to offer any evidence of mental suffering, awarded $50 nominal damages for trespass and invasion of privacy).

In awarding damages for unauthorized entry into another's information files, the courts will probably adhere to these general rules in compensating the plaintiff for intrusion upon seclusion. However, in many instances, the measure of compensatory damages may be inadequate. When the intrusion does not result in pecuniary harm or mental distress, plaintiff may not bring an intrusion action because of the prospect of recovering nominal damages. Additionally, nominal or compensatory damages will not act as an adequate deterrent to intrusions upon informational seclusion when, for example, the intruder is a large corporation which gains more through its intrusions than it costs to compensate its victims. It is apparent that, in order to deter intentional intrusions upon informational privacy rights, and to encourage assertion of such rights, courts must be prepared to award punitive damages.

Punitive damages have traditionally been awarded upon a showing that the defendant acted with malice, or that his conduct was willful. *See, e.g.*, Welsh v. Pritchard, 125 Mont. 517, 241 P.2d 816, 821 (1952) (exemplary damages awarded against defendant who "invaded and destroyed the privacy

Data-Banks as Areas of Seclusion

Liability for intrusion upon seclusion can only be predicated upon a defendant's intrusion into an area in which the plaintiff held an expectation of privacy.[59] In determining what affairs of an individual may be protected by expectations of privacy, the courts generally employ a standard of reasonableness.[60] The plaintiff must demonstrate an actual subjective expectation of privacy in the particular affairs, and that expectation must be one which society will accept as reasonable.[61] Courts have found reasonable expectations of privacy in, for example, one's person,[62] home,[63] bank accounts[64] and telephone conversations.[65]

Courts have held, and no one would dispute, that one's filing cabinet or desk drawer generally constitutes an area of seclusion.[66] If an intruder enters the filing cabinet or desk in order to obtain private information, such conduct would amount to an actionable intrusion upon seclusion. The situation is no different when an intruder gains unauthorized access to computer files

---

and sacredness" of plaintiff's home). *See generally* J. GHIARDI & J. KIRCHER, PUNITIVE DAMAGES: LAW AND PRACTICE § 4.14 (1981). Punitive damages have also been used by the courts in order to deter conduct. *Id. See, e.g.*, Strum, Rutger & Co. v. Day, 594 P.2d 38, 47 (Alaska), *cert. denied*, 454 U.S. 894 (1979); Campbell v. Government Employees Ins. Co., 306 So. 2d 525, 531 (Fla. 1974). Intentionally gaining unauthorized access to private or confidential information files with the intent of acquiring private information concerning the plaintiff is in willful disregard of plaintiff's privacy rights and, because few states have adopted criminal sanctions (*see supra* note 44), may provide a proper case for awarding punitive damages. In the absence of intent or willfulness, punitive damages would not be proper. *E.g.*, Estate of Berthiaume v. Pratt, 365 A.2d 792, 795 (Me. 1976).

59. *See* cases cited *infra* notes 62-65.

60. *E.g.*, Harms v. Miami Daily News, Inc., 127 So. 2d 715 (Fla. 1961) (jury question as to whether a reasonable person would find telephone calls objectionable). "It is clear . . . that the thing into which there is a prying or intrusion must be, and be entitled to be, private." Prosser, *supra* note 10, at 391.

61. *See, e.g.*, Vernars v. Young, 539 F.2d 966 (3d Cir. 1976) (finding reasonable expectations of privacy in personal mail).

62. *E.g.*, Galella v. Onassis, 487 F.2d 986 (2d Cir. 1973) (granting injunctive relief against defendant who was hindering plaintiff's movement in public).

63. *E.g.*, Welsh v. Pritchard, 125 Mont. 517, 241 P.2d 816 (1952) (defendant landlord and his wife entered tenant's premises and remained for 17 days and nights).

64. *E.g.*, Burrows v. Superior Court of San Bernardino County, 13 Cal. 3d 238, 529 P.2d 590, 118 Cal. Rptr. 166 (1974) (evidence resulting from unauthorized disclosure by bank of plaintiff's account suppressed).

65. *E.g.*, LeCrone v. Ohio Bell Tel. Co., 120 Ohio App. 129, 201 N.E.2d 533 (1963) (eavesdropping).

66. *See, e.g.*, Pearson v. Dodd, 410 F.2d 701 (D.C. Cir.) (intruders broke into plaintiff's office and took private information), *cert. denied*, 395 U.S. 947 (1969).

containing private information. The information is no different, either in its content or reference, and the individual's interest in keeping the information private has not changed. Only the means of storing the information is different.

Related to this first issue is the question of whether computer files maintained by third parties, such as hospitals or banks, constitute areas of the individual's seclusion. This question necessarily raises the issue of what status the courts give confidential information. Except in those few situations where disclosure of the particular information would directly infringe upon constitutional guarantees, some courts have been reluctant to extend privacy protection to confidential information held in organization files.[67]

Given the way in which modern information systems can infringe upon the personal autonomy of private individuals, however, any such continued distinction between private and confidential information must be discarded. The determinative factor must be, as in all intrusion cases, whether the individual who disclosed private information reasonably expected that it would remain confidential. If the expectation of confidentiality was reasonable, any intrusion into files containing the information should be actionable.[68] Thus, assuming an actual subjec-

67. *The Use and Abuse of Computerized Information*, *supra* note 46, at 596. *See, e.g.*, United States v. Miller, 425 U.S. 435 (1976) (finding no legitimate expectation of privacy in the contents of checks and deposit slips). *Miller* was overruled by the Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401 *et. seq.* (1982). *See generally* Trubow & Hudson, *supra* note 3.

The confidentiality of information maintained in organizational files has been protected when disclosure of such information would infringe, for example, upon the right to association. *See, e.g.*, NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958) (protecting the confidentiality of organization membership lists). *See also The Use and Abuse of Computerized Information*, *supra* note 46, at 595. Confidentiality has been protected in other contexts. *See, e.g.*, Vernars v. Young, 539 F.2d 966 (3d Cir. 1976) (protecting expectations of privacy in mail); Burrows v. Superior Court of San Bernardino County, 13 Cal. 3d 238, 529 P.2d 590, 118 Cal. Rptr. 166 (1974) (confidentiality of bank records protected); LeCrone v. Ohio Bell Tel. Co., 120 Ohio App. 129, 201 N.E.2d 533 (1963) (telephone conversations protected).

68. The proper party plaintiff in an intrusion upon informational seclusion case would be the individual about whom the information concerns, not necessarily the party storing the information. It is generally agreed that the right of privacy pertains only to individuals. *See* Prosser, *supra* note 10, at 408-9. Corporations and partnerships cannot assert an invasion of privacy. *Id.* When an intrusion upon information about the plaintiff occurs, the plaintiff may be able to join as a defendant the entity or individual which was storing the information, alleging disclosure of private facts (*see* discussion *supra* note 20). However, under the present state of the law, that party might not be held liable for the disclosure if the disclosure was not deliberate. *See* Grenier, *Computers and Privacy: A Proposal for Self-Regulation*, 1970 DUKE L.J. 495, 499 (examining the computer privacy problem and how it will affect computer system operators). Further, the limited nature of the "publication" may preclude liability. *See infra* note 87. How-

tive expectation of privacy, computer data-banks can constitute areas of seclusion.

Intrusions from Remote Terminals

Once it is determined that data-banks can constitute areas of seclusion, it is necessary to address the issue of whether gaining unauthorized access to a data-bank from a *remote* computer terminal constitutes an actionable *intrusion*.[69] Courts which have traditionally required a trespass[70] may be hesitant to apply the intrusion upon seclusion tort to this new means of invading privacy. If, however, those courts concentrate on the results of the intrusion, and the prying nature of the defendant's conduct, rather than on the means employed to effectuate the intrusion, the intrusion requirement of the tort will be met.

The fact that the defendant never physically enters a domain under the plaintiff's control should be irrelevant in defending an invasion of privacy. Use of a computer to gain unauthorized access to computer files is similar to other means of invading seclusion which courts have generally accepted as giving rise to a cause of action. For example, prying into the plaintiff's private conversations or activities by mechanical means constitutes an actionable intrusion upon seclusion.[71]

The unreasonableness of the intrusion should not depend on the means employed to effectuate the intrusion. Whether the

---

ever, the public interest in preserving the privacy and confidentiality of personal information may engender new formulations of privacy law in order to ensure complete informational privacy. Grenier, *supra*, at 501. There may come a day when the courts "simply hold the computer service company *absolutely* liable for the unauthorized release" of information, even if the traditional requirements of the publication action are not met. *Id.* at 502 (emphasis in original).

69. Access to computer data-banks is often effectuated from a remote computer terminal. *See, e.g.*, Ward v. Superior Court, 3 Computer L. Serv. Rep. 206 (Cal. Super. Ct. 1972) (where defendant allegedly gained unauthorized access to a remote computer and stole a trade secret). *See also supra* note 8.

70. Some jurisdictions have traditionally required that the intrusion be physical, analogous to a trespass. *E.g.*, Kobeck v. Nabisco, Inc., 166 Ga. App. 652, 305 S.E.2d 183 (1983) (wife had no cause of action against her employer for showing her absentee record to her husband because she suffered no physical intrusion of her privacy). The more progressive and accepted view, however, does not require a physical trespassory invasion. *See, e.g.*, Dietemann v. Time, Inc., 449 F.2d 245, 249 (9th Cir. 1971); Pearson v. Dodd, 410 F.2d 701, 705 (D.C. Cir.), *cert. denied*, 395 U.S. 947 (1969). The view rejecting the requirement of a physical intrusion recognizes that "[o]ne's emotional sanctum is certainly due the same expectations of privacy as one's physical environment." Phillips v. Smalley Maint. Serv., Inc., 435 So. 2d 705, 711 (Ala. 1983).

71. *E.g.*, Rhodes v. Graham, 238 Ky. 225, 37 S.W.2d 46 (1931) (wiretap); Hamberger v. Eastman, 106 N.H. 107, 206 A.2d 239 (1964) (microphone).

intruder uses a third telephone, a hidden microphone, or a computer terminal to accomplish the intrusion into plaintiff's private matters is not relevant. The fact remains that, by *any* means, the intruder invaded an area surrounded by reasonable expectations of privacy. It is the intrusion which is actionable, not the means employed. Courts, therefore, should not hesitate to find tort liability when an intruder uses a remote computer terminal. The substance of the tortious conduct is the prying, not a trespass.

Application of Traditional Limiting Factors to the Intrusion Upon Informational Seclusion Action

Few rights are absolute. In privacy law, several factors often act to limit or vitiate causes of action for invasion of privacy. The most common factors are consent and public concern. Though arguments can be made that such limitations should be made equally applicable in intrusion upon informational seclusion cases, it is apparent that such application would be in disregard of the fundamental concerns which a right of informational privacy seeks to protect.

Consent

Plaintiff's consent to investigation or disclosure of personal information will preclude an action for invasion of privacy.[72] Consent may be given either expressly or impliedly.[73] Implied consent to the investigation of personal information usually arises in connection with applications for credit, insurance, employment and government benefits. When an individual makes such applications, he impliedly consents to investigation of the accuracy of information appearing on the application.[74] The individual consents, however, only to *reasonable* investigations.[75]

---

72. *See* Prosser, *supra* note 10, at 419-20.

73. *Id. See, e.g.*, Smith v. WGN, Inc., 47 Ill. App. 2d 183, 185, 197 N.E.2d 482, 484 (1964); Anderson v. Low Rent Housing Comm'n of Muscatine, 304 N.W.2d 239, 249 (Iowa), *cert. denied*, 454 U.S. 1086 (1981).

74. *E.g.*, Molton v. Commercial Credit Corp., 127 Ga. App. 390, 193 S.E.2d 629 (1972) (authorization for credit bureau to obtain information that might assist in deciding to grant a home loan). *Cf.* Jeffers v. City of Seattle, 23 Wash. App. 301, 597 P.2d 899 (1979) (plaintiff waived right of privacy pertaining to his medical condition by requesting a disability pension).

75. *Reasonable* investigations are those which are limited to the collection of information which is relevant and necessary to the decision being made. *See The Use and Abuse of Computerized Information*, *supra* note 46, at 601. Overzealous collection of private information by "objectionable snooping techniques," or collection of information "irrelevant to *any* legitimate business purpose," can constitute an actionable intrusion upon seclusion. Tureen v. Equifax, Inc., 571 F.2d 411, 416 (8th Cir. 1978) (emphasis in

What the individual does not consent to is an overly intrusive investigation into matters which have little or no relation to the matter at hand. The individual should not be held to have consented to wholesale intrusions into his entire informational past.

Express authorizations to perform indiscriminate informational searches can be recognized, absent elements of unconscionability. *Implied* authorizations, however, should not be recognized as a limit on the right to informational seclusion. To allow a decision maker to "plug" his computer into any system containing information concerning the applicant, on the basis of some "implied" consent, would be in absolute disregard of the applicant's privacy rights. Computers are used to store a wide variety of personal information. While some of the information contained in the data file may be relevant to the matter at hand, other information may not be relevant. Because of the risk that irrelevant information might be disclosed, the law cannot risk implied waivers of the right of informational seclusion.

Matters of Public Concern

An important limitation to actions involving publication arises when the published matter is of legitimate concern to the public.[76] When the general public interest requires that private or confidential information concerning the plaintiff be known, no cause of action for invasion of privacy will accrue upon publication of such information.[77] Though compelling arguments can be made which support extension of the public interest limitation to actions for intrusion upon informational seclusion, such

---

original) (consumer reporting firm did not violate plaintiff's privacy by searching its own files for information concerning plaintiff).

76. "It has always been considered a defense to a claim of invasion of privacy by publication . . . that the published matter complained of is of general public interest." Pearson v. Dodd, 410 F.2d 701, 703 (D.C. Cir.), *cert. denied*, 395 U.S. 947 (1969). *See, e.g.*, Miller v. News Syndicate Co., 445 F.2d 356 (2d Cir. 1971) (newspaper article reporting of plaintiff's participation in a heroin smuggling syndicate held newsworthy); Jacova v. Southern Radio & Television Co., 83 So. 2d 34 (Fla. 1955) (newscast showing plaintiff in gambling raid on cigar store); Hubbard v. Journal Pub. Co., 69 N.M. 473, 368 P.2d 147 (1962) (article concerning sexual assault of plaintiff). *But see* Briscoe v. Reader's Digest Ass'n, Inc., 4 Cal. 3d 529, 483 P.2d 34, 93 Cal. Rptr. 866 (1971) (publication of plaintiff's name in connection with criminal activity 11 years earlier no longer of legitimate concern to the public). The privilege to publish that which is of legitimate concern to the public received constitutional protection in Time, Inc. v. Hill, 385 U.S. 374 (1967). In *Time*, a false light case, the court held that publication of misstated facts would not be actionable unless the misstatements were made with knowledge of falsity or in reckless disregard of the truth. *Id.* at 389-91. *See generally* W. PROSSER, *supra* note 11, at § 118.

77. *See supra* note 76.

an extension cannot be made without disregarding those fundamental beliefs upon which the intrusion upon seclusion action is based.

Those in favor of extending the limitation to the intrusion action would argue, for example, that no reasonable distinction can be made between the actions of intrusion and publication of private facts.[78] Either the public has a right to be informed of matters of legitimate public concern, or it does not. The only distinction that can be drawn between the two causes of action is the nature of the defendant's conduct in relation to the information. It is absurd to allow the publication of certain facts because they are of legitimate public concern and, on the other hand, to condemn the gathering of such information merely because the plaintiff locked it in his filing cabinet or computer data-bank. Either the public has a right of access to such information, or it does not.

In response to this argument, those *not* in favor of extending the limitation of the publication action to the intrusion action would urge that it is not the information's seclusion which the cause of action protects but, rather, the *individual's* seclusion. The right to maintain the privacy and confidentiality of personal information is only an aspect of the solitude that the right of privacy was intended to protect. The right of privacy protects individuality.[79] In order to protect and foster individuality, however, a right to control access to private and confidential information must be protected.[80] The courts have recognized this.

In *Pearson v. Dodd*,[81] for example, a United States senator brought suit against newspaper columnists that had published columns which related to his alleged past misdeeds.[82] The columnists had obtained their information from two former employees of the plaintiff who had entered the plaintiff's office without authority and had taken the information.[83] After the court determined that the publication of the information was privileged, it next addressed plaintiff's argument that, because the columnists knew how the information had been obtained, they had committed an actionable intrusion upon seclusion.[84]

78. *See supra* note 20 for a brief statement of the publication of private facts action. *See also supra* note 76.

79. *See supra* text accompanying notes 25-34.

80. *See supra* text accompanying notes 49-51.

81. 410 F.2d 701 (D.C. Cir.), *cert. denied*, 395 U.S. 947 (1969).

82. *Id.* at 703.

83. *Id.*

84. *Id.* at 704-05.

Though the court rejected the plaintiff's argument,[85] it indicated that it would have held the columnists liable for intrusion had they been the ones who took the information from the plaintiff's office. The court stated:

> Where there is intrusion, the intruder should generally be held liable whatever the content of what he learns. An eavesdropper to the marital bedroom may hear marital intimacies, or he may hear statements of fact or opinion of *legitimate interest to the public*; for purposes of liability [for intrusion upon seclusion] that *should make no difference*.[86]

Pearson recognized that the intrusion action is designed to protect an interest different from that which the publication of private facts action is designed to protect. While the publication action protects a right to keep private information private,[87] the intrusion action seeks to protect a right of solitude. Information which is maintained within an area of seclusion is protected, not merely because it is private, but because it is an aspect of a greater right to individual autonomy within protected areas of seclusion.

Once it is agreed that computer data-banks, like offices and marital bedrooms, constitute areas in which individuals can have reasonable expectations of privacy, the courts must recognize that intrusions into such data-banks violate the individual's right of privacy and must be actionable no matter what type of information is revealed. Those seeking access to private or confidential information concerning individuals must be allowed to do so only with the express authorization of the individual or, alternatively, through the courts, which would act in a manner consistent with the privacy rights of the individual.[88] Absent

---

85. *Id.* at 705. The court rejected the plaintiff's argument because to hold the columnists liable for intrusion "would establish the proposition that one who receives information from an intruder, knowing it has been obtained by improper intrusion, is guilty of a tort." *Id.* The court was not prepared "to go so far." *Id. Accord* McNally v. Pulizter Pub. Co., 532 F.2d 69 (8th Cir.) (newspaper not liable for intrusion by its mere receipt of private facts which were obtained tortiously), *cert. denied*, 429 U.S. 855 (1976).

86. Pearson v. Dodd, 410 F.2d 701, 705 (D.C. Cir.), *cert. denied*, 395 U.S. 947 (1969) (emphasis added).

87. While the publication of private facts action is designed to keep private information private, defendant generally will not be held liable when the publication is limited in scope. *See, e.g.*, Peacock v. Retail Credit Co., 302 F. Supp. 418 (N.D. Ga. 1969) (disclosure limited to clients of reporting agency), *aff'd*, 429 F.2d 31 (5th Cir. 1970), *cert. denied*, 401 U.S. 938 (1971). In order to be actionable, the publication must be to a large number of persons; it must be circulated through the community. *E.g.*, Tureen v. Equifax, Inc., 571 F.2d 411, 418-19 (8th Cir. 1978); Kinsey v. Macur, 107 Cal. App. 3d 265, 270-71, 165 Cal. Rptr. 608, 611 (1980).

88. In some circumstances, the legitimate interests of the public may outweigh the individual's right to maintain reasonable areas of informational seclusion. In those cases, after a determination has been made that

such authorization or court approval, intrusion upon informational seclusion must constitute an actionable violation of the individual's right of privacy.

CONCLUSION

The use of computers as a means of invading informational seclusion becomes more frequent every day. Whether technological advances will ever be able to prevent computer intrusions is unknown. Traditional privacy principles must be invoked to respond to this new means of invading privacy. The courts must recognize the individual's interest in maintaining areas of informational seclusion.

For those jurisdictions which have recognized a cause of action for intrusion upon seclusion, providing a civil remedy for victims of informational intrusion will not require new formulations of their privacy law. In those jurisdictions which have not recognized the intrusion action, such as Illinois,[89] it must be recognized that adoption of a civil remedy for informational intrusion is necessary in order to vindicate the victim's privacy rights and to act as a deterrent to such conduct. Only through recognition of the right to informational seclusion can the right of privacy survive the computer age.

John A. McLaughlin

---

the individual must surrender some of his rights to seclusion, the court should conduct an *in camera* examination of the information in order to separate that which is of greater interest to the public from that which is not. *See* Industrial Found. of the South v. Texas Indus. Accident Bd., 540 S.W.2d 668, 686 (Tex. 1976), *cert. denied*, 430 U.S. 931 (1977). Respect for the individual's right of privacy commands, however, recognition of a presumption that the public generally will have no legitimate interest in obtaining private information about particular individuals. *See id.* at 685. Judicially compelled disclosure must be the exception, not the rule.

89. *E.g.*, Kelly v. Franco, 72 Ill. App. 3d 642, 646, 391 N.E.2d 54, 57-8 (1979) (noting that actions for invasion of privacy in Illinois are limited to appropriation of one's name or likeness for commercial purposes). *But see* Midwest Glass Co. v. Stanford Dev. Co., 34 Ill. App. 3d 130, 133-34, 339 N.E.2d 274, 277 (1975) (indicating that public disclosure of a private debt may constitute an actionable invasion of privacy). *See generally* Comment, *Privacy in Illinois: Torts Without Remedies*, 17 J. MAR. L. REV. 799 (1984).