The John Marshall Journal of Information Technology & Privacy Law

Volume 9
Issue 3 *Computer/Law Journal - Summer 1989*

Article 4

Summer 1989

Individual Privacy and Governmental Efficiency: Technology's Effect on the Government's Ability to Gather, Store, and Distribute Information, 9 Computer L.J. 359 (1989)

C. Dennis Southard IV

INDIVIDUAL PRIVACY AND GOVERNMENTAL EFFICIENCY: TECHNOLOGY'S EFFECT ON THE GOVERNMENT'S ABILITY TO GATHER, STORE, AND DISTRIBUTE INFORMATION

By C. DENNIS SOUTHARD IV

TABLE OF CONTENTS

I. INTRODUCTION

In the last few decades, technology has advanced at a staggering rate.[1] What was science fiction a few short years ago is now science fact.[2] This advance has had a far reaching effect on society. Satellites bring us images of events from the other side of the world, which we watch as they unfold.[3] Microwaves cook our dinners; home computers

1. *See* A. MILLER, THE ASSAULT ON PRIVACY 11 (1971) (noting that the most dramatic aspect of the electronic age may be the rate at which technology has evolved); King, *Eye in the Sky*, FORBES, Dec. 1, 1986, at 216 (quoting former CIA director William Colby). *See also* R. TURN, PRIVACY SYSTEMS FOR TELECOMMUNICATION NETWORKS 1 (1974).

2. *See, e.g.*, G. ORWELL, 1984 (1949) (traditionally associated with governmental invasions of privacy, visions of "Big Brother" watching represent the ultimate government intrusion); L. RON HUBBARD, MISSION EARTH (1986) (providing an excellent representation of the potential of future invasive technology).

3. *See* M. FRANKLIN, MASS MEDIA LAW 936-43 (1987). The use of communications satellites, along with the adoption of new home television delivery systems such as cable,

balance our checkbooks; and stuffed animals tell our children stories.[4] Technology has become an intricate and inextricable part of our daily lives.

The effect of technology on society has generally been favorable. Advances in medicine, science, and industry, have greatly improved our standard of life. The use of high-tech equipment has led to medical advancements in: disease control and identification, artificial limbs and organs, gene splicing and bio-engineering, radiation treatment for cancer, and laser aided surgery, just to name a few.[5] In addition to the scientific aspects of medicine, technology has been a main force behind the rapid growth of the physical sciences. For example, its use in the space program has enabled the development of super-cooled infrared sensors which study distant stars, space structures, precision optics, and optical data storage systems.[6] Finally, factories around the country are becoming more and more reliant on technology. Advances in robotics and automation have dramatically changed traditional industrial processes.[7]

Technology, however, is a sword that can cut two ways. If used properly, it can enable us to streamline our economy and decrease inefficiency in government and industry.[8] For example, the governmental bureaucracy that threatens to overwhelm us might be simplified and centralized by using networks of computer interchanges. One commentator has noted that "[u]sed wisely, data storage could help good administration by making accurate and comprehensive information available to those who have to frame policy and take [sic] key decisions."[9] On the other hand, there is a danger that this technology might be used to manipulate the individual.[10] Personal records, gathered by swiftly improv-

---

satellite master antennas, and home satellite dishes, brings even more information to the viewer by enabling broadcasters to economically distribute national programming which is aimed at the needs and interests of discrete groups. *Id.*

4. *See* Kantrowitz, *High-Tech Toys*, NEWSWEEK, Nov. 2, 1987, at 71, 71-73. Among the most recent developments in recreational technology are "interactive" toys which can respond to touch, light, and sound. Dolls such as Playmates' "Jill" and Worlds of Wonder's "Julie" can speak and sing, while "Talking Cabbage Patch Kids" can even recognize each other, carry on conversations between themselves and sing duets. *Id.*

5. *See generally* R. JONES, FUTURE CONFLICT AND NEW TECHNOLOGY 48-49 (1981) (stating that computers have contributed vitally to the solution of the genetic code).

6. *See id.* at 49.

7. *See id. See also* Sabel, Herrigel, Hazis & Deeg, *How to Keep Mature Industry Innovative*, TECH. REV., Apr. 1987, at 27, 27-35.

8. Miller, *Computers, Data Banks and Individual Privacy: An Overview*, 4 COLUM. HUM. RTS. L. REV. 1, 2 (1972) (discussing the realistic possibilities of a checkless, cashless economy, improved information bases for rational planning, better governmental services to people, and more equitable allocation of human and natural resources).

9. R. JONES, *supra* note 5, at 50.

10. *See* J. RULE, PRIVATE LIVES AND PUBLIC SURVEILLANCE 20-31 (1974).

ing modes of surveillance and stored in "a national data base,"[11] could be recalled instantly and used against the interests of the individual.[12]

The conflict between the positive and negative aspects of technological advancements presents a critical question. As "the need of government and business organizations to have personal information for efficient planning and operation" increases,[13] will the threat to privacy overtake the protection provided by the current legal structure?[14] Because society cannot exist without a certain degree of control, and the individual cannot truly exist without a certain degree of freedom,[15] a balance between freedom and control must be struck. This article attempts to determine the balance between the individual's privacy interest and the government's interest in efficiency, in light of present and future technological developments.

The threat to privacy, posed by the use of new information technologies, comes from both the public and the private sectors.[16] This article, however, focuses on the governmental uses. Parts one and two explain the individual's interest in privacy, and the government's interest in having personal information. Part three discusses the conflict between the individual and governmental interests that occur at three fundamental points: when the information is gathered, when it is stored, and when it is distributed. Finally, part four concludes that, while the existing legal structure provides a foundation for protecting personal privacy, specific provisions need to be made to insure that this protection does not erode as technology advances.

II. INDIVIDUAL PRIVACY INTERESTS

Privacy, in general, is "the quality or state of being apart from company or observation."[17] This definition provides a foundation for the

---

11. *See Government Data Bases and Privacy*, THE FUTURIST, Sept.-Oct. 1986, at 52, 52-53.

12. *See* Field, *"Big Brother Inc." May Be Closer Than You Thought*, BUS. WK., Feb. 9, 1987, at 84, 84-86.

13. W. WARE, DATA BANKS, PRIVACY, AND SOCIETY 6-7 (1973).

14. *See* A. MILLER, *supra* note 1, at 205.

15. One commentator has noted, for example:

> The life of the individual in a society has to strike a balance between freedom and discipline. Too little freedom will strangle the individual initiative on which so much of the advance of society depends; excessive freedom, such as the right to drive an automobile on whichever side of the road as one may from moment to moment choose, can result in disaster.

Jones, *Some Threats of Technology to Privacy*, in PRIVACY AND HUMAN RIGHTS: REPORTS AND COMMUNICATIONS PRESENTED AT THE THIRD INTERNATIONAL COLLOQUY ABOUT THE EUROPEAN CONVENTION ON HUMAN RIGHTS 139 (1973).

16. *See* W. FREEDMAN, THE RIGHT OF PRIVACY IN THE COMPUTER AGE 96-97 (1987).

17. WEBSTER'S NINTH NEW COLLEGIATE DICTIONARY 936 (1988).

right of privacy[18] which has been referred to as "[t]he right to be let alone."[19] Legally, the right of privacy has two main branches, one rooted in tort and the other in the Constitution.[20] Tort law recognizes four basic causes of action for damages: appropriation, intrusion, public disclosure of private information, and false light.[21] The Constitution protects the individual against unwarranted governmental invasion.[22]

Individual privacy also has two separate and distinct branches—physical and informational.[23] Physical privacy relates to intrusions into one's personal life; whereas, informational privacy pertains to the use of personal information by others.[24] More accurately, informational privacy seeks to protect two individual interests. The first is the individual's interest in *aesthetic* privacy. This interest represents the instinctive urge to conceal certain information because it is, by nature, embarrassing or distressing, such as "acts of excretion, sexual intercourse, or profound emotion."[25] In this area, the restriction of information is an end in itself.[26] The second informational privacy interest is protecting *strategic* privacy[27] —for example, a general's desire to conceal troop movements from the enemy. Here, information is restricted as a means to an end;[28] the interest is not in the information itself but

18. The generally accepted origin of the right of privacy is an 1890 law review article by Samuel Warren and Louis Brandeis which reviewed several previous cases where recovery had been allowed on theories of defamation, breach of contract, property rights and breach of confidence. They concluded that these earlier cases had actually been decided on a broader principle, protecting privacy interests, which was entitled to independent recognition. *See* Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). *See also* A. BRECKENRIDGE, THE RIGHT TO PRIVACY 1-10 (1970) (a presentation of the history behind the right of privacy).

19. BLACK'S LAW DICTIONARY 1075 (5th ed. 1979). *See also* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (stating that the right to be let alone is "the most comprehensive of rights and the right most valued by civilized men").

20. *See* 16A AM. JUR. 2D *Constitutional Law* § 601 (1979).

21. *See* RESTATEMENT (SECOND) OF TORTS § 652A (1977) [hereinafter RESTATEMENT]. It is noteworthy that, although they are included under privacy in the Restatement, appropriation (§ 652C), public disclosure (§ 652D), and false light (§ 652E), more accurately prohibit publicity rather than preserve privacy.

22. *See* Eisenstadt v. Baird, 405 U.S. 438, 453 (1973). *See also* L. TRIBE, AMERICAN CONSTITUTIONAL LAW 886-887 (1978).

23. *See* Miller, *supra* note 8, at 2.

24. For the purposes of this Note, physical privacy is violated when the government intrudes in an attempt to gather information. Informational privacy is violated by the storage, recall and dissemination of personal information by others.

25. J. RULE, D. MCADAM, L. STEARNS & D. UGLOW, THE POLITICS OF PRIVACY: PLANNING FOR PERSONAL DATA SYSTEMS AS POWERFUL TECHNOLOGIES 22 (1980) [hereinafter THE POLITICS OF PRIVACY].

26. *Id.*

27. *Id.*

28. *Id.*

in the long-term consequences of having it revealed.[29] The fundamental distinction between these two types of privacy is that the individual is interested in concealing aesthetic information from everyone,[30] but is only interested in withholding strategic information from those who would use that information to the individual's detriment.[31]

The American legal system provides some protection for physical privacy;[32] however, protection of informational privacy is far from adequate.[33] Although the "zone of privacy"[34] protected by the Constitution has been expanded in recent years,[35] it only recognizes those interests which parallel constitutional guarantees.[36] Where the courts have recognized a constitutional right of privacy,[37] they have held that its in-

29. *Id.* There is very little statutory protection for strategic privacy. This lack of protection may be due to the nature of strategic privacy. Concealing information in order to achieve some ulterior end is invariably linked to deceit. Providing legal protection for such motives could be seen as promoting dishonesty which runs contrary to popular concepts of justice. *But see* Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-22 (1982).

30. Under certain circumstances, disclosure of aesthetic information to others will not concern the individual. For example, in the case of personal information given to a doctor or lawyer, or information known by family members, the individual has provided the information voluntarily with the exception of confidentiality. *See* Gross, *Privacy and Autonomy*, in PHILOSOPHY OF LAW 246-47 (J. Feinberg & H. Gross eds. 1980) (originally appearing in NOMOS XIII, PRIVACY 169 (J. Chapman & J. Roland eds. 1971)).

31. *See* THE POLITICS OF PRIVACY, *supra* note 25, at 23.

32. For example, tort law provides protection against intrusion upon privacy and the disclosure of personal information. *See* RESTATEMENT, *supra* note 21. Further, the Constitution provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. CONST. amend. IV. *See also* Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics, 403 U.S. 388, 392 (1971).

33. *See* A. MILLER, *supra* note 1, at 205.

34. "Various [constitutional] guarantees create zones of privacy." Griswold v. Connecticut, 381 U.S. 479, 484 (1965). "The Constitution does not explicitly mention any right of privacy. In a line of decisions, however, going back as far as [1891], the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution." Roe v. Wade, 410 U.S. 113, 152 (1973).

35. *See* W. KEETON, PROSSER AND KEETON ON THE LAW OF TORTS 866-867 (1984).

36. For example, the Supreme Court has stated that "only personal rights that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty,' are included in [the Constitution's] guarantee of personal privacy." Roe v. Wade, 410 U.S. 113, 152 (1973). The Court has also found a right of privacy to be implicit in the First Amendment. *See* NAACP v. Alabama, 357 U.S. 449, 462 (1958) (discussing a constitutionally protected right of association).

37. The Constitution protects the autonomy of the individual regarding certain personal interests, such as: marriage, *see* Loving v. Virginia, 388 U.S. 1 (1967); contraception, *see* Eisenstadt v. Baird, 405 U.S. 438 (1973); procreation, *see* Skinner v. Oklahoma, 316 U.S. 535 (1942); family relationships, *see* Prince v. Massachusetts, 321 U.S. 158 (1944); education, *see* Meyer v. Nebraska, 262 U.S. 390 (1923); and child rearing, *see* Pierce v. Society of Sisters, 268 U.S. 510 (1925). *See also* W. KEETON, *supra* note 35.

fringement is justified only if it is narrowly focused[38] and intended to promote a compelling governmental interest.[39] While this standard may have provided adequate protection at one time, technological advances have made some governmental intrusions into personal privacy—despite being narrowly focused to promote a compelling interest—serious enough to surpass a minimum standard of human expectation.[40]

Advances in informational technologies have facilitated intrusions on physical privacy and have made storage and recall of private information faster and more efficient. Because the extent of these intrusions was not possible in the past, no protection was necessary.[41] However, now that such intrusions are possible, and advances in storage and recall technologies have made the intrusions more serious, some form of protection is now necessary.

Ideally, the scope of the government's authority to infringe on personal privacy should equal the amount of privacy that an individual is willing to forego to promote governmental efficiency.[42] In order to determine where that ideal balance is, it is necessary to understand not only the individual's interest in privacy, but the government's interest in efficiency.

III. THE GOVERNMENT'S INTEREST IN PERSONAL INFORMATION

The government uses personal information for three purposes: "for-

38. *See Roe*, 410 U.S. at 155 (1973).

39. *Id.*

40. Justice Douglas once stated that the right of privacy associated with the institution of marriage was "older than the Bill of Rights—older than our political parties, older than our school system." Griswold v. Connecticut, 381 U.S. 479, 486 (1965). This implies a right of privacy which is inherent in human interactions and which should not be dependent on any special grant from the government.

41. A. MILLER, *supra* note 1, at 26. *See also* OFFICE OF TECHNOLOGY ASSESSMENT, CONGRESS OF THE UNITED STATES, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 67 (1985) [hereinafter OTA] which states:

> Before the widespread use of computer-communication systems, linking various kinds of transactions was very difficult, if not impossible, since transactions were paper based and the cost of matching or linking paper records was prohibitive. In addition, the time delay inherent in paper linkages would negate much of the potential surveillance value.

42. It seems likely that people will be willing to forego some aspect of their privacy if they feel that they will gain more by sacrificing it than they save by protecting it. A good example of this trade-off is society's willingness to sacrifice a section of privacy in order to receive the benefit of increased police efficiency. *See* Gross, *supra* note 30, at 250-51.

mulating policy, fighting crime, and protecting national security."[43] As our society has become larger and more complex, the amount of information the government needs in order to operate effectively has increased.[44] The need for large amounts of information, however, is due not only to the greater size and complexity of our society, but also to the growing role that government plays within it.[45]

One of the government's primary responsibilities is the management of public resources.[46] In order to fulfill this responsibility more efficiently, the government needs access to vast amounts of information in order to determine the existence and quantity of the resources, to judge the best use of the resources—including who is justifiably entitled to their use, and to better understand the effects of their allocation.[47] For example, in order to effectively measure and assess taxes, the government needs information regarding an individual's income, marital status, occupation, bank accounts, medical expenses, and other information which is generally considered personal.[48] Furthermore, much of the money collected through taxes is given out as aid in the form of social security, welfare, unemployment benefits, and other similar programs. Here again, the government needs personal information to decide who is qualified to receive these benefits and to insure that the most efficient use is made of every tax dollar.

The government also uses personal information to fight crime and protect national security. "Perhaps the most significant development in crime technology during the past decade has been the use of computer data banks to store, classify and retrieve vital information on criminal suspects and stolen property."[49] The need for this type of information

43. J. CRAGAN & D. SHIELDS, GOVERNMENT SURVEILLANCE OF U.S. CITIZENS: ISSUES AND ANSWERS 5-6 (1971).

44. *See* W. WARE, *supra* note 13, at 2.

45. *See* M. ROSTOKER & R. RINES, COMPUTER JURISPRUDENCE: LEGAL RESPONSES TO THE INFORMATION REVOLUTION 230-231 (1986).

46. *See* U.S. CONST. preamble. *See also* U.S. CONST. art. I, § 8 (giving Congress the power to lay and collect taxes, regulate commerce, coin money, promote science and art, raise and support the military); McCulloch v. Maryland, 17 U.S. (4 Wheat.) 316, 407-08 (1819).

47. *See* W. WARE, *supra* note 13, at 2-3. Ideally, in a representative democracy, such as ours, each representative reflects the needs and interests of his constituents. Access to large amounts of accurate information about those constituents would better enable representatives to fulfill this function. Such information, if available, could be used to predict the effects of proposed or enacted legislation, to forecast tax revenues in order to accurately budget future spending, to determine eligibility for government programs in order to prevent error or fraud.

48. U.S. Individual Income Tax Form 1040A, Department of the Treasury-Internal Revenue Service (1986).

49. Katzenbach & Tomc, *The Use of Computers in Crime Detection and Prevention*, 4 COLUM. HUM. RTS. L. REV. 49, 50 (1972).

is used to justify increasing government surveillance which intrudes on personal privacy.[50] While most data-gathering activities are well intended,[51] information gathered for security reasons is wide-ranging and may include private information which has little, if any, connection to increasing public protection.[52]

The government's interest in gathering or using personal information unreasonably, or for illegitimate purposes, will always be outweighed by the individual's interest in privacy; however, even when the governmental purpose is legitimate, it must be balanced against the individual's privacy interest. Therefore, in some cases, a legitimate governmental need for personal information will not justify an intrusion on individual privacy. In order to determine where the balance should be struck, each interest must be weighed in relation to how the information will be used. The individual's interest in retaining personal information can conflict with the government's interests in having it during one, or more, of three stages: gathering it, storing it, or distributing it.[53]

IV. STAGES OF CONFLICT

A. GATHERING INFORMATION

As discussed above, the government's primary interest is the availability of personal information.[54] Because easy access to large amounts of information tends to increase overall efficiency, the more information that is available, the more efficient the government can be.[55] To that end, the government gathers vast quantities of information every year.[56] Much of this information is provided voluntarily by the individual in order to receive some benefit or privilege;[57] however, a growing

50. "[The argument] may be stated this way: the greater the ability to watch what is going on, or obtain evidence of what has gone on, the greater the ability to prevent crime." Gross, *supra* note 30, at 250. Gross, however, goes on to state that, once an efficient law enforcement system is established, it does not necessarily follow that an increase in efficiency will result in a reduction in crime. *Id.* at 250-51.

51. *See* Miller, *supra* note 8, at 14.

52. *See* Katzenbach & Tomc, *supra* note 49, at 56 (criminal intelligence gathering may concern anything from telephone bills to reports of personal associations).

53. *See* J. CRAGAN & D. SHIELDS, *supra* note 43, at 7-8.

54. *See supra* text accompanying note 44.

55. *See supra* notes 43-52 and accompanying text.

56. *See Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 92d Cong., 1st Sess. 32-34 (1971) (statement of Arthur R. Miller) [hereinafter *Hearings*].

57. A good deal of information is supplied in exchange for government services; some is provided because it is required by law, such as the census. Although this information is not actually given voluntarily, it is not sought without the knowledge of the individual. *See* W. WARE, *supra* note 13, at 2.

amount is gathered without the individual's knowledge or consent.[58] These clandestine attempts to gather information are usually intended to promote the government's interests in fighting crime or protecting national security,[59] and directly conflict with the individual's interest in physical privacy.[60]

Protection from intrusion into physical privacy by governmental agencies derives primarily from the Fourth Amendment to the Constitution.[61] In the landmark case *Katz v. United States*,[62] Katz was convicted of transmitting wagering information over the telephone. Evidence of the phone conversations was gathered by the FBI using electronic listening devices attached to the outside of a public phone booth. The Court held that Katz had a justifiable expectation of privacy inside the phone booth and when an individual's expectation of privacy is justifiable,[63] an unwarranted intrusion into that privacy violates the Fourth Amendment.[64] This is true even when the intrusion does not involve a physical trespass and is only possible with the aid of technology.[65] The *Katz* case, therefore, is a barrier against the use of technology as a means to gather personal information. In a more recent case, however, the privacy protection provided by *Katz* has been eroded.

In *Dow Chemical Co. v. United States*,[66] the Court upheld the unwarranted use of technologically aided surveillance, based primarily on the type of technology used. Dow claimed that the EPA's unwarranted aerial surveillance of an outdoor chemical processing plant was an unconstitutional search in violation of the Fourth Amendment. The Court found that the processing plant was analogous to an "open field" and, therefore, Dow's expectation of privacy was not justifiable. Much of the Court's rationale for their decision was based on the idea that the surveillance equipment used by the EPA was commonly available to the public. "Here, EPA was not employing some unique sensory device

58. "The widespread use of spike and parabolic microphones, the emergence of various gadgets for electronic eavesdropping, and the ready availability of cameras equipped with esoteric optical devices have made it clear that we no longer enjoy *physical* privacy in our own homes, offices or country retreats." *See Hearings*, *supra* note 56, at 32 (emphasis in original).

59. *See* OTA, *supra* note 41, at 62.

60. *See supra* note 24 and accompanying text for a definition of physical privacy.

61. *See* U.S. CONST. amend. IV.

62. 389 U.S. 347 (1967).

63. Whether a person's expectation is justifiable depends on a two part test. First, whether, by his conduct, the individual has exhibited an expectation of privacy, and second, whether this expectation is one that society recognizes as reasonable. *See* Rakas v. Illinois, 439 U.S. 128, 143-44 (1978).

64. *Katz*, 389 U.S. at 353.

65. *Id.*

66. 476 U.S. 227 (1986).

that, for example, could penetrate the walls of buildings and record conversations in Dow's plants, offices, or laboratories, but rather a conventional, albeit precise, commercial camera commonly used in mapmaking."[67]

While it is true that the camera used in *Dow* could not "penetrate the walls of buildings," it seems clear that its use allowed the penetration of a distance so great that it would have effectively been a solid wall to the naked eye. Still, the Court held that when the surveillance equipment used is generally available to the public, its use is not constitutionally proscribed.[68] Justice Powell, in his dissenting opinion in *Dow*, pointed out that the problem posed by the majority's analysis is that it "will not protect Fourth Amendment rights, but rather will permit their gradual decay as technology advances."[69]

Recent developments in the computer field have increased the threat to traditional privacy expectations.[70] Employers now have the ability to monitor the use of computers by their employees from the time they log on until the time they log off.[71] Software has been developed which allows employers to compare the efficiency of employees as they work,[72] or to relay subliminal messages to employees working at computer stations.[73] While the Fourth Amendment may currently pro-

67. *See id.* at 238.

68. *Id.* The Court described the camera used to take aerial photographs of Dow's plant as "a conventional, albeit precise, commercial camera commonly used in mapmaking." *Id.* Upon closer examination, however, it appears that the system used to get the photographs was quite sophisticated, far from being generally available to the public. The aircraft used, a twin engine Beechcraft, is described as able to "provide photographic stability, fast mobility and flight endurance required for precision photography." Dow Chemical Co. v. United States, 536 F. Supp. 1355, 1357 n.2 (E.D. Mich. 1982) (quoting Handbook on Aerial Surveys & Photogrammetry—Abrams Aerial Survey Corporation). The cost of the camera used was in excess of $22,000, and the camera itself is described as the "finest precision aerial camera available." *Id.* When the photographs were enlarged it became "possible to discern equipment, pipes, and power lines as small as 1/2 inch in diameter." *Id.*

69. *Dow*, 476 U.S. at 240 (Powell, J., dissenting). One example of the advances in surveillance technology is the Keyhole 12 satellite, scheduled for launch in 1988. From its 200 mile orbit, the satellite is expected to be able to take high-resolution photographs of objects as small as three inches. *See* King, *supra* note 1. Advances in optical technology have resulted in the development of miniature cameras which "could be concealed in anything from a briefcase, to a lamp, to a plant." OTA, *supra* note 41, at 63. Through the use of optical fibers, a camera lens could be placed in one area, and the recorder in another. This set up would allow surveillance of a private area without subjecting the listener/viewer to the risk of being discovered. *Id.*

70. *See* Reece, *Computer Monitoring and Privacy: Is the Orwellian Nightmare Here*, NAT'L L.J., Feb. 15, 1988, at 20.

71. *Id.*

72. *Id.*

73. *Id.*

tect public employees from the use of computer monitoring, the Court's reasoning in *Dow* suggests that this protection will deteriorate as information gathering technology becomes more widespread.

In order to prevent the decay of Fourth Amendment rights, the Court must accept that advances in surveillance technology allow governmental intrusions into individual privacy that are not justified by the government's need for the information. As technology has advanced, the level of reasonably expected privacy has decreased.[74] "Previously, one could take actions to ensure an expectation of privacy in a private place, *e.g.*, locking the doors and closing their curtains."[75] Because advances in surveillance technology have made these precautions meaningless, the expectation of the privacy they offer is no longer justifiable. Therefore, if the Court relies on a justifiable expectation of privacy as the measure of protection, that protection will diminish as the relevant technology becomes more widely accepted. The Court could halt the decline in individual privacy by adopting a minimum level of privacy beyond which any intrusion, regardless of the technology used, would be unreasonable. For example, this minimum might be "locking the doors and closing the curtains,"[76] or any other standard, so long as it remained constant in the face of advancing technology.

B. STORING INFORMATION

Of the three stages of conflict, the storage of personal information has the least intrusive effect on an individual's privacy.[77] Currently, there are three primary methods used to manipulate and analyze personal information maintained in government data files: computer matching, computer assisted front-end verification, and computer profiling. Computer matching is a process whereby two or more data bases are compared to determine whether the individual appears on more than one. Used properly, this information can be used to detect fraud, waste and abuse.[78] Computer-assisted, front-end, verification allows an agency to check the information given to them by an individual, for accuracy and completeness, by comparing similar information contained in computerized data files. This method is used to determine eligibility for government assistance programs.[79] Computer Profiling refers to the

74. *See* OTA, *supra* note 41, at 62.

75. *Id.*

76. *Id.*

77. The mere fact that personal information is stored poses no more of a serious threat to an individual's privacy than if the information had stayed with him. This is less true of aesthetic privacy because the idea that the information is outside the individual's control is itself cause for concern. *See supra* text accompanying notes 25-26.

78. *See Government Data Bases and Privacy*, THE FUTURIST, Sept.-Oct. 1986, at 54, 55.

79. *Id.*

use of computer data files to create profiles of persons who have certain characteristics. This method of manipulating personal data can be used, for example, to identify an individual who exhibits characteristics common to tax evaders.[80]

In order for these methods to operate effectively, the computer data files must contain accurate and up-to-date information—the more information the better. As is often the case, however, when large amounts of information are being handled, the potential for both intentional and accidental misuse exists. For example, Massachusetts uses a computer matching system to determine eligibility for welfare aid. In one case, the welfare department threatened to cut benefits to a woman when the computer turned up an $11,000 bank account she had allegedly failed to declare. It turned out that the account belonged to someone with a similar social security number.[81] As the use of new technology increases, so does the potential for misuse.

The primary privacy concern, regarding the storage of information, is a potential chilling effect on the individual's exercise of his independent judgment that may result from the knowledge that personal information is being stored. This concern was addressed by the United States Supreme Court in the case of *Whalen v. Roe*.[82] In *Whalen*, the Court was presented with the question of whether the State of New York could keep a centralized computer record of the names and addresses of all persons who had obtained certain drugs pursuant to a doctor's prescription.[83] The concern expressed by the plaintiffs was that some people might decline the use of needed medication because of the knowledge that the information might be readily available in a computer file.[84] The Court found that, while the storage of the information presented an added burden to the individual's decision-making process, it was insufficient to constitute an invasion of a constitutionally protected right of privacy.[85] The decision in *Whalen* implies that only a complete foreclosure of an individual's ability to make independent judgments will constitute an actionable infringement on privacy. Although this analysis may have been valid when the Court decided *Whalen*, advances in computer technology have subsequently increased,

80. *Id.*

81. Field, *supra* note 12, at 85.

82. 429 U.S. 589 (1977). *See also* NAACP v. Alabama, *ex rel* Patterson, 357 U.S. 449 (1958); Thornburgh v. American College of Obstetricians and Gynecologists, 476 U.S. 747 (1986).

83. *Whalen*, 429 U.S. at 591.

84. The Court acknowledged that, not only was there a threat that medication might be refused because of a concern for privacy, but that needed medication had in fact been declined. *Id.* at 603.

85. *Id.* at 602-04.

and will continue to increase, this burden on privacy.[86]

In order to minimize the danger posed by the threat of misuse, one of three things must happen: the Court must define broader limits of protection,[87] Congress must adopt storage notification requirements,[88] or Congress must provide for greater oversight of the current system.[89] One of the methods of protection currently being considered is the development of an official Board to oversee computer matching of federal data files.[90] While such a system would impair governmental efficiency, it would go a long way toward providing peace of mind to those whose actions would be chilled by the knowledge that certain personal information is being stored by the government.

C. DISTRIBUTING INFORMATION

Finally, the most serious threat to informational privacy comes from the distribution and use of personal information. While gathering information threatens physical privacy because of its intrusive nature,[91] the individual's informational privacy is not threatened until that information is used for a purpose different than that intended by the individual, or is made known to someone with interests contrary to the individual's. This is especially true of strategic information, where the concern for privacy stems from the individual's need for exclusive use of the information.[92] Thus, it is not surprising that most of the legislation protecting personal information tends to focus on this area.[93] Of this legislation, The Privacy Act of 1974[94] applies most directly to the issue of governmental use and distribution of personal information. The Act provides two rights: first, information cannot be disclosed without the individual's consent,[95] and second, the individual must be given access to any of the collected information.[96]

---

86. *Id.* "Advances in computer technology are making it easy to do what was impossible not long ago: cross-match information almost at the touch of a button to create portraits of individuals—and even to try to predict their behavior." Field, *supra* note 12, at 84.

87. *See supra* text accompanying notes 74-76.

88. *See infra* text accompanying notes 98-102.

89. *See* Field, *supra* note 12, at 86.

90. *Id.*

91. *See supra* notes 54-76 and accompanying text.

92. *See supra* notes 27-29 and accompanying text.

93. *See* Privacy Act of 1974, 5 U.S.C. § 552a (1982); Freedom of Information Act, 5 U.S.C. § 552 (1982); *see also* Fair Credit Reporting Act, 15 U.S.C. § 1681i (1982); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232 (1982); Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 (1982).

94. 5 U.S.C. § 552a (1982).

95. *Id.* § 552a(b).

96. *Id.* § 552a(d).

Facially, these rights provide a good measure of security against misuse of personal information; however, this armor is slightly tarnished. For example, the Privacy Act does not apply to records kept by the Central Intelligence Agency,[97] the Secret Service,[98] any agency whose principal function pertains to law enforcement,[99] for statistical purposes,[100] or to federal testing results.[101] Furthermore, the Privacy Act's requirement of consent prior to disclosure is subject to twelve exceptions, each of which provides a potential floodgate for the release of personal information. The Privacy Act does not require the consent of the individual when the information is disclosed: (1) to officers of the governmental agency in performance of their duty; (2) pursuant to a statutory requirement; (3) for routine use by a collecting agency; (4) to the Census Bureau; (5) for purposes of statistical research; (6) to the National Archives; (7) to be used in a criminal or civil trial; (8) in order to protect the health or the safety of another; (9) to Congress; (10) to the Comptroller General; (11) pursuant to a court order; (12) under certain circumstances, to a consumer reporting agency.[102]

While each of these exceptions may conceivably promote a governmental interest,[103] they allow for distribution of personal information well beyond what is justified by the government's interest when weighed against the individual's privacy interest. An example of the overbroad distribution allowed by the Privacy Act is when an individual, perhaps motivated by a sense of civic duty, voluntarily gives personal information to the government, and that information is released to someone whom the individual would not have given the information. In this type of situation, the private nature of the information changes as the use of the information changes.[104] To that extent, the Privacy Act fails to provide protection from the use of personal information for purposes other than those intended by the individual.

In order to minimize the potential damage caused by the misuse of personal information, the government should adopt measures to insure that the individual is notified prior to the release of personal informa-

97. *Id.* § 552a(j)(1).
98. *Id.* § 552a(k)(3).
99. *Id.* § 552a(j)(2).
100. *Id.* § 552a(k)(4).
101. *Id.* § 552a(k)(6).
102. *Id.* § 552a(b)(1-12).
103. The exceptions to the Privacy Act's consent requirement may be justified as promoting the governmental interests of formulating policy or fighting crime. *See supra* notes 43-52 and accompanying text.
104. The change in the value is especially evident where the information is released to a consumer reporting agency. In this situation, the government's efficiency interest is questionable at best. *See* Dow v. General Services Admin., 544 F. Supp. 530 (D.C. Md. 1982).

tion. Predisclosure notification would permit the government to continue to use the information as currently allowed by the Privacy Act, while giving the individual advance warning of potential misuse so that he can protect himself from any injurious effects.[105] Notification should be mandatory unless the government's need for the information concerns national security or the prevention of crime.[106] However, prior to allowing an exception to the notification requirement, an independent determination that the government's need for the information is actually justified by interests in national security or crime fighting should be made. This determination would be similar to the warrant requirement under the Fourth Amendment. An independent authority, such as an agency head, a judge, or a commission, must verify that there is a justifiable need for not notifying the individual.

The right of access permitted by the Privacy Act provides a measure of security only to the extent that the information may be checked by the individual to insure that it is accurate.[107] It provides no protection, however, against the chilling effect caused by the storage of the information.[108] When the individual is not sure that information about him is being kept, he may hesitate to take advantage of the right of access for fear that, if there is no file, one will be started. This doubt could be alleviated by adopting procedures which provide notification to the individual whenever personal information is distributed. Since the individual has no need to check the accuracy of information until it is actually used, notification would help alleviate the chilling effect caused by fears of misuse. This would result because an individual who is not notified would know that either no file exists or that, if one does exist, it is not being used.

V. CONCLUSION

The current legal structure, even though it permits the erosion of personal privacy as technology advances, does provide an adequate foundation upon which to establish the needed protections. In order to protect the individual against the threat from new invasive technologies, the courts must adopt a minimum standard of reasonably expected

105. Executive Order 12600 is a step in the right direction. The order requires that predisclosure notification be given whenever confidential commercial information has been requested. Exec. Order No. 12600, 3 C.F.R. 235 (1988). Unfortunately, the order does not provide any right enforceable under law, but is only intended to improve the internal management of the government. *Id.* § 10.

106. Requiring notification in this area would substantially frustrate governmental efficiency by allowing potential criminals to cover their tracks after learning of an investigation.

107. 5 U.S.C. § 552a(d)(2) (1982).

108. *See supra* notes 82-85 and accompanying text.

privacy. This minimum standard can be based upon the Fourth Amendment's guarantee of protection against unreasonable searches and seizures. It should allow government to continue its police and national security protection at its current level, while guaranteeing that if an individual takes certain steps to assure his privacy it will be respected.

Protection against the chilling effect that stored information has on independent judgment can be provided by the government's adoption of a commission to oversee the methods used for storage and to insure against their misuse. This oversight would allow the government to store personal information while providing the individual with a greater degree of confidence and security. Finally, the individual can be protected from injury caused by the release of incorrect information, or the release of information to a party with interests adverse to those of the individual, by providing predisclosure notification to the individual whenever personal information is released. The predisclosure requirement would allow government to continue to use the information to promote efficiency, while giving the individual notice of potential misuses. Provisions for this requirement could be made simply by amending the Privacy Act to include predisclosure notification, or by eliminating the exceptions to the Act's current notification requirements.

The adoption of these measures would significantly help protect personal privacy in the face of advancing technology, while only minimally affecting governmental efficiency.