Florida State University Law Review

Volume 20 | Issue 3 Article 1

1993

Access to Government-Held Information in the Computer Age: Applying Legal Doctrine to Emerging Technology

Matthew D. Bunker
1@1.com

Sigman L. Spilchal
2@2.com

Bill Chamberlin
11@11.com

Linda M. Perry
22@22.com

FLORIDA STATE UNIVERSITY
LAW REVIEW

ACCESS TO GOVERNMENT-HELD INFORMATION IN THE COMPUTER AGE: APPLYING LEGAL DOCTRINE TO EMERGING TECHNOLOGY

Matthew D. Bunker, Sigman L. Splichal,
Bill Chamberlin, & Linda M. Perry

VOLUME 20 WINTER 1993 NUMBER 3

Recommended citation: Matthew D. Bunker et al., *Access to Government-Held Information in the Computer Age: Applying Legal Doctrine to Emerging Technology*, 20 FLA. ST. U. L. REV. 543 (1993).

ACCESS TO GOVERNMENT-HELD INFORMATION IN THE COMPUTER AGE: APPLYING LEGAL DOCTRINE TO EMERGING TECHNOLOGY

MATTHEW D. BUNKER,* SIGMAN L. SPLICHAL,**
BILL F. CHAMBERLIN,*** AND LINDA M. PERRY****

I. INTRODUCTION

IN a democratic system based on popular sovereignty, citizens have an interest in the workings of their government. The basic data of those government operations are official records and documents. The federal government,[1] the fifty states, and the District of Columbia[2] have shown their commitment to the concept of public access to government-held information. All have statutes that allow varying degrees of access to government records.[3] Florida, a leader in the tradition of open government, enacted a public records law[4] that provided a model for a nationwide effort that resulted in similar legislation in many states.[5]

The fundamental concept of open government often conflicts with government's desire to keep information secret, either to preserve pri-

---

* B.S., 1979; M.S., 1989, Kansas State University; J.D., 1985, University of Kansas; Ph.D, Candidate 1993, University of Florida.

** Assistant Professor of Communications, University of Miami; B.S., 1970; M.A., 1976; Ph.D., Candidate 1993, University of Florida.

*** Joseph L. Brechner Eminent Scholar of Mass Communication; Director, Brechner Center for Freedom of Information, University of Florida; B.A., 1967, University of Washington; M.A., 1968, University of Wisconsin; Ph.D., 1977, University of Washington.

**** B.S., 1987; M.A., 1989; Ph.D., Candidate 1993, University of Florida.

The authors would like to thank the following individuals who provided significant research assistance in the preparation of this Article: Michael Nyenhuis, Morgan Gaynor, and David Switalski. Expenses for this project were funded in part by the Brechner Center for Freedom of Information, College of Journalism and Communications, University of Florida.

1. *See* Freedom of Information Act, 5 U.S.C. § 552 (1988).

2. *See* REPORTERS COMM. FOR FREEDOM OF THE PRESS, TAPPING OFFICIALS' SECRETS, A STATE OPEN GOVERNMENT COMPENDIUM (1989) (reproducing, with annotations, the various freedom of information acts and public records laws) [hereinafter "TAPPING OFFICIALS' SECRETS"].

3. *Id.*

4. FLA. STAT. ch. 119 (1991). The Public Records Law was enacted in 1909 and was one of the first in the nation. Ch. 5942, Laws of Fla. (1909).

5. FLORIDA JT. LEGIS. INFO. TECH'Y RESOURCE COMM., FLORIDA'S INFORMATION POLICY: PROBLEMS AND ISSUES IN THE INFORMATION AGE 28 (1989) [hereinafter FLORIDA'S INFORMATION POLICY].

vacy, to maintain national security, or for one of many other purposes, some more valid than others. This has resulted in a substantial body of case law that has grown out of efforts to balance these competing interests.[6]

The use of computers to maintain public records has complicated the situation.[7] Many open records statutes were written when government information consisted of paper records stored in file cabinets. The use of computers to create, manipulate, store, and disseminate these records is changing how—and even whether—governments provide public access to their records.

This Article will examine the constitutional and statutory bases for access to government information. It will explore some of the practical obstacles to obtaining access to government records held in computers. The Article will then describe the legal issues specific to computerized government records and will discuss how courts at all levels have dealt with those issues. Next, the Article will examine the tension between access to records and concerns about personal privacy. Although privacy concerns are implicated in many contexts in this Article, specific discussion will be reserved until the final substantive section. In conclusion, the Article will offer guidelines the authors believe will help ensure access to computerized records. Throughout, the focus will be on access both at the federal level and in Florida.

---

6. The conflict between access and privacy is discussed at length, *infra* notes 286-388 and accompanying text.

7. The issue of access to computerized records has been addressed by a number of commentators, including Eric M. Freedman, *Freedom of Information and the First Amendment in a Bureaucratic Age*, 49 BROOK. L. REV. 835 (1983); Patti A. Goldman, *The Freedom of Information Act Needs No Amendment To Ensure Access to Electronic Records*, 7 GOV'T INFO. Q. 389 (1990); Jamie A. Grodsky, *The Freedom of Information Act in the Electronic Age: The Statute Is Not User Friendly*, 31 JURIMETRICS J. 17 (1990); Patrick L. "Booter" Imhof & Edwin A. Levine, *Impact of the Information Age on Access and Dissemination of Government Information in Florida*, 14 FLA. ST. U. L. REV. 635 (1986); Megan A. Kendall, *Current Development*, AFSCME v. County of Cook*: Access to Information Beyond Reach as Computer Tape Lengthens Bureaucratic Red Tape*, 3 SOFTWARE L.J. 755 (1990); Leo T. Sorokin, *The Computerization of Government Information: Does It Circumvent Public Access Under the Freedom of Information Act and the Depository Library Program?*, 24 COLUM. J.L. & SOC. PROBS. 267 (1990); Sol Villasana, *The People's Right To Know in the Age of Electronic Information*, BARRISTER, Fall 1990, at 61. *See also* Jerry Berman, *The Right To Know: Public Access to Electronic Public Information*, 3 SOFTWARE L.J. 491 (1989); Henry Perritt, Jr., *Electronic Acquisition and Release of Federal Agency Information: Analysis of Recommendations Adopted by the Administrative Conference of the United States*, 41 ADMIN. L. REV. 253 (1989); Sandra D. Scott, Computer Technology v. Laws on Access (unpublished paper presented to the Association for Education in Journalism and Mass Communication, annual convention, Boston, Mass., Aug. 1991); Sigman L. Splichal & Bill F. Chamberlin, The Fight for Access to Government Records Round Two: Enter the Computer (unpublished paper presented to the International Communication Association, annual meeting, Miami, Fla., May 1992) (on file with authors).

II. ACCESS TO RECORDS: FUNDAMENTAL PRINCIPLES

Access to government-held information is grounded in the American political ideal of self-government. The Framers of the *United States Constitution* said self-governing people should be well-informed about the workings of government to make intelligent political choices.[8] In a discussion of the First Amendment, James Madison said: "The right of freely examining public characters and measures, and of free communication thereon, is the only effectual guardian of every other right. . . ."[9] Thomas Jefferson's belief in the importance of an informed electorate, and a press that is free to inform it, is well documented. Jefferson said that because the informed "opinion of the people" is the basis of government,[10] he would prefer "newspapers without a government" over "government without newspapers."[11]

The Framers, despite their commitment to self-government, did not give much guidance as to how the press was to go about informing the people—or as to how the people were to go about informing themselves—about the operations of government. Nonetheless, the Framers did provide some mechanisms for holding representatives accountable to the people. There are constitutional mandates for access to government information, although they are narrow and specific. For example, the Constitution requires the legislative and executive branches to report certain information about their operations.[12] Each house is required to keep and publish a "Journal of its Proceedings."[13] However, each house may determine for itself what might "require Secrecy" and, as a result, be kept off the record.[14] In

---

8. Only narrow traditions of openness existed in the early years of the Republic. *See generally* Edward L. Barrett, Jr., *Freedom of the Press—American Style*, LEGAL INSTITUTIONS TODAY: ENGLISH AND AMERICAN APPROACHES COMPARED 214, 238-39 (Harry W. Jones ed., 1977). As Congress opened its doors to the public and the press in the 1780s and 1790s, both houses wrote rules under which they might operate behind closed doors if the need arose. *See* Introduction *in* JOURNALS OF CONGRESS, 1775-1788; LEWIS DESCHLER, CONSTITUTION, JEFFERSON'S MANUAL, AND RULES OF THE HOUSE OF REPRESENTATIVES, H.R. DOC. NO. 564, 82d CONG., 2d SESS. (1953).

9. WRITINGS OF JAMES MADISON 398 (1806), *reprinted in* Note, *Access to Official Information: A Neglected Constitutional Right*, 27 IND. L.J. 209, 212 (1952).

10. *See Letter from Jefferson to Edward Carrington, Jan. 16, 1787, in* THE PAPERS OF THOMAS JEFFERSON 48-49 [hereinafter PAPERS OF JEFFERSON].

11. *Id.* But Jefferson also believed that the guarantee for a free press should not protect the press from liability for publishing false facts. *Letter from Jefferson to Madison, July 31, 1788, in* PAPERS OF JEFFERSON, *supra* note 10, at 13:442-43. See also LEONARD W. LEVY, EMERGENCE OF A FREE PRESS 250-81 (1985), for a discussion of Jefferson's belief in state prosecutions for the press's seditious libels.

12. *See, e.g.*, U.S. CONST. art. I, § 5, cl. 3; *id.* § 9, cl. 7.

13. *Id.* § 5, cl. 3.

14. *Id.*

addition, Congress is required to publish "from time to time" a "regular Statement and Account of the Receipts and Expenditures of all public Money. . . ."[15] The President is required to report to Congress "Information on the State of the Union."[16]

Except for these narrow exceptions for specific reports, the Constitution does not directly mandate public access to government information.[17] The United States Supreme Court has not explicitly found, except in criminal trials,[18] an implied constitutional right of access to government proceedings or records. Although the First Amendment does not directly mention access, some have suggested it mandates access to government information in some circumstances.[19]

A. *The First Amendment*

The First Amendment says "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."[20]

The First Amendment is often recognized as continuing a fundamental personal right of conscience and expression.[21] Indeed, the clauses protecting the fundamental rights of individuals are enumerated first. The First Amendment is viewed as "the repository of . . . self-governing powers,"[22] as it provides a peaceful means for political and social change through public discussion.

---

15. *Id.* § 9, cl. 7. *But see* United States v. Richardson, 418 U.S. 166 (1974) (federal taxpayer did not have standing to claim Congress had failed to require detailed reports of Central Intelligence Agency expenditures). In his opinion for the Court, Chief Justice Burger suggested that taxpayers could never have standing and that "the subject matter is committed to the surveillance of Congress, and ultimately to the political process." *Id.* at 179.

16. U.S. CONST. art. II, § 3.

17. See *infra* notes 52-73 and accompanying text discussing cases asserting a right to access of government information.

18. See Richmond Newspapers v. Virginia, 448 U.S. 555, 563-75 (1980), for a short summary of the Anglo-American history of the right to attend criminal trials.

19. *See infra* notes 70-73 and accompanying text.

20. U.S. CONST. amend I.

21. *See generally* LEVY, *supra* note 11; Vincent Blasi, *The Checking Value in First Amendment Theory*, 1977 AM. B. FOUND. RES. J. 523; *Justice Black and First Amendment "Absolutes": A Public Interview*, 37 N.Y.U. L. REV. 549 (1962) (transcript of interview conducted by Professor Edmond Cahn).

22. William J. Brennan, Jr., *The Supreme Court and the Meiklejohn Interpretation of the First Amendment*, 79 HARV. L. REV. 1, 11 (1965).

1. Self-Government

The United States Supreme Court has recognized that the primary function of the First Amendment is to protect the freedoms necessary for self-government. Justice Louis Brandeis in 1927 is said to have given "the principle its classic formulation":[23]

> Those who won our independence believed . . . that public discussion is a political duty; and that this should be a fundamental principle of the American government. . . . Believing in the power of reason as applied through public discussion, they eschewed silence coerced by law—the argument of force in its worst form. Recognizing the occasional tyrannies of governing majorities, they amended the Constitution so that free speech and assembly should be guaranteed.[24]

In 1931 a majority of the Court said the First Amendment provides "the opportunity for free political discussion to the end that government may be responsive to the will of the people and that changes may be obtained by lawful means . . . ."[25] Justice William J. Brennan summarized the principle succinctly in his opinion for the Court in *Garrison v. Louisiana*,[26] saying that "speech concerning public affairs is more than self-expression; it is the essence of self-government."[27]

The Court has extended considerable First Amendment protection to discussion of public affairs by individuals and the press.[28] Yet the Court has seemed reluctant to recognize a concomitant right to gov-

---

23. As characterized by Justice Brennan in his opinion for a unanimous Court in New York Times v. Sullivan, 376 U.S. 254, 270 (1964).

24. Whitney v. California, 274 U.S. 357, 375-76 (1927) (Brandeis, J., concurring) (footnote omitted).

25. Stromberg v. California, 283 U.S. 359, 369 (1931). See also Cohen v. California, 403 U.S. 15, 24 (1971), where the Court held:

> The constitutional right of free expression . . . is designed and intended to remove governmental restraints from the arena of public discussion, putting the decision as to what views shall be voiced largely into the hands of each of us, in the hope that use of such freedom will ultimately produce a more capable citizenry and more perfect polity and in the belief that no other approach would comport with the premise of individual dignity and choice upon which our political system rests.

In addition, the Court held in Roth v. United States, 354 U.S. 476, 484 (1957), that the First Amendment is designed to "assure unfettered interchange of ideas for the bringing about of political and social changes desired by the people."

26. 379 U.S. 64 (1964) (overturning criminal libel conviction for criticizing the official conduct of state judges in Louisiana).

27. *Id.* at 74-75.

28. *See, e.g.*, Nebraska Press Ass'n v. Stuart, 427 U.S. 539 (1976); New York Times v. United States, 403 U.S. 713 (1971); New York Times v. Sullivan, 376 U.S. 254 (1964); Near v. Minnesota, 283 U.S. 697 (1931).

ernment-held information that the public has a duty to discuss.[29] First Amendment scholars, as well as some Supreme Court justices and federal judges, have articulated theories that might support such a right.

Political philosopher Alexander Meiklejohn said the First Amendment's protection is concerned with "a public power, a governmental responsibility."[30] In the Meiklejohnian view, the First Amendment gives absolute protection to expression on self-government issues because citizens need information about their government to vote intelligently.[31]

One way citizens inform themselves about their government is through their surrogate, the press. Professor Vincent Blasi has said that the First Amendment provides a "checking value" on abuse of official power in government.[32] According to Blasi, the First Amendment protects the press in its watchdog role—reporting on the actions of public officials to keep government responsive and accountable. The press gives citizens the information they need "about what government officials are doing," such as "the official actions revealed in the Pentagon Papers."[33]

The Supreme Court has acknowledged that information itself is important to public discussion,[34] but has not articulated a right of access to that information.[35] The Court, however, has recognized a right of the public to receive information that is already in the hands of the media and others.[36]

2. *A Right To Receive Information*

In 1936, the Supreme Court first identified a right to receive information in *Grosjean v. American Press Co.*[37] The Louisiana Legislature had imposed a "license tax" on the gross advertising receipts of large newspapers. The Court held that the tax was unconstitutional because "it abridges the freedom of the press."[38] A free press is "a vital source of public information," and "informed public opinion is

---

29. *See infra* notes 52-57 and accompanying text.

30. Alexander Meiklejohn, *The First Amendment Is An Absolute*, 1961 SUP. CT. REV. 245, 255.

31. ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT 6 (1948).

32. Blasi, *supra* note 21, at 528.

33. *Id.* at 553.

34. *See, e.g.*, New York Times v. Sullivan, 376 U.S. 254 (1964).

35. *See infra* text accompanying notes 52-73.

36. *See, e.g.*, First Nat'l Bank of Boston v. Bellotti, 435 U.S. 765 (1978).

37. 297 U.S. 233 (1936). *See also* Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, 425 U.S. 748, 756-57 (1976); Kleindienst v. Mandel, 408 U.S. 753, 762-65 (1972); Martin v. City of Struthers, 319 U.S. 141, 143 (1943).

38. *Grosjean*, 297 U.S. at 251.

the most potent of all restraints upon misgovernment."[39] Thus, the tax would infringe on "the natural right" of the people to "acquire information about their common interests."[40]

The Court has reiterated, in a variety of contexts, the idea that "the Constitution protects the right to receive information and ideas."[41] Many consider *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council*[42] the seminal "right to receive" case. In that 1976 decision, the Court struck down a Virginia statute forbidding pharmacists from advertising the prices of prescription drugs.[43] Justice Blackmun, writing for the majority, said the free flow of information about commercial matters was necessary to assure informed public decision-making.[44] The protection of the First Amendment, Blackmun reasoned, extends not only to the speaker, but to the recipient of the communication.[45] Although *Virginia State Board* dealt with commercial speech, the majority opinion made it clear that the constitutional protection for receipt of information would apply with even more force when more directly related to self-government and public policy.[46]

In 1982 the Supreme Court emphasized the connection between self-government and the right to receive information in *Board of Education v. Pico*.[47] That case involved a school board-ordered removal of books from secondary school libraries after the board characterized the books as "anti-American, anti-Christian, anti-Semtic [sic], and just plain filthy . . . ."[48] Justice Brennan, writing for a three-justice plurality, emphasized the First Amendment's role in assuring wide-

---

39. *Id.* at 250. However, the Court also has found that "the press does not have a monopoly on either the First Amendment or the ability to enlighten," *Bellotti*, 435 U.S. at 782 (1978), and the right of the press is no greater than the right of the public. *See generally* Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980); Houchins v. KQED Inc., 438 U.S. 1 (1978); Saxbe v. Washington Post Co., 417 U.S. 843 (1974); Pell v. Procunier, 417 U.S. 817 (1974); Branzburg v. Hayes, 408 U.S. 665 (1972).

40. *Grosjean*, 297 U.S. at 243.

41. In addition to cases discussed in the text, see Stanley v. Georgia, 394 U.S. 557, 564 (1969) (relying on the right to free access to ideas and privacy rights in the home to hold that states may not make the private possession of obscene material by an adult a crime). *See also* Kleindienst v. Mandel, 408 U.S. 753 (1972) (finding the right to receive information and ideas insufficient to overturn a 1952 law making Communists ineligible to receive visas); Lamont v. Postmaster Gen., 381 U.S. 301 (1965) (relying on a right to "receive information and ideas" to invalidate a 1962 law under which the post office screened foreign mail and detained "communist propaganda").

42. 425 U.S. 748 (1976).

43. *Id.* at 773.

44. *Id.* at 765.

45. *Id.* at 756.

46. *Id.* at 765 n.19.

47. 457 U.S. 853 (1982).

48. *Id.* at 857.

spread dissemination of ideas and information.[49] "[T]he State may not, consistently with the spirit of the First Amendment, contract the spectrum of available knowledge."[50] Moreover, the right to receive, according to Justice Brennan, is a "necessary predicate" to citizen participation in government and the exercise of other constitutional rights.[51]

The First Amendment right to receive information has been closely tied to effective self-government in a number of cases. It thus suggests some constitutional justification for access to government records. Although the right to receive has not been extended to government records, the same concerns that drive its application by the Court in other areas could logically serve as grounds to require some form of access to government information.

3. *A Limited Right of Access to Government-Held Information*

The First Amendment has been interpreted by the Court to protect the right to publish information about public issues that comes into the media's possession.[52] Except for judicial proceedings and records, however, the Court has not articulated a constitutional right of access to information that the government produces and holds.

The Court first confronted the issue of a First Amendment right of access to government-controlled information[53] in the 1974 companion cases of *Pell v. Procunier*[54] and *Saxbe v. Washington Post Co.*[55] In both cases, the Court upheld regulations prohibiting press interviews with prison inmates. In rejecting the First Amendment claims of the press, the Court said the media could be denied access to prisoners because the public also was denied access in order to control the prison populations.[56] Justice Potter Stewart, in his opinion for the *Pell* Court, said the First Amendment prohibits government interference with the press. It "does not, however, require government to accord

---

49. *Id.* at 866.

50. *Id.* (citing Griswold v. Connecticut, 381 U.S. 479, 482 (1965)).

51. *Id.* at 867.

52. *See, e.g.*, cases cited *supra* note 28.

53. The Court considered newsgathering issues in 1972 in Branzburg v. Hayes, 408 U.S. 665 (1972), a case involving reporters' claims that requiring them to appear and testify before grand juries about their confidential news sources would burden newsgathering. It rejected a qualified privilege not to testify. *Id.* The Court recognized that newsgathering has some First Amendment protection. *Id.* at 681. However, it rejected the claim that the press has a constitutional right of special access to information not available to the public generally. *Id.* at 684.

54. 417 U.S. 817 (1974).

55. 417 U.S. 843 (1974).

56. *Saxbe*, 417 U.S. at 846-47; *Pell*, 417 U.S. 817.

the press special access to information not shared by members of the public generally."[57]

In one limited domain, the Court has recognized a constitutional right of access to information. In *Richmond Newspapers, Inc. v. Virginia*[58] the Court held in a seven-to-one opinion that the First Amendment requires that a criminal trial "must be open to the public," absent an overriding interest.[59] Chief Justice Burger's plurality opinion, joined only by Justices White and Stevens, based this implicit right on the fact that criminal trials historically have been open to the public,[60] and that openness is necessary to the effective functioning of the criminal justice system.[61]

Richmond Newspapers sets out a number of benefits that result from open trials. Openness "gave assurance that the proceedings were conducted fairly to all concerned, and it discouraged perjury, the misconduct of participants, and decisions based on secret bias or partiality."[62] Moreover, open trials, particularly in the case of especially heinous crimes, had a "significant community therapeutic value" by providing a catharsis for an area outraged by a crime.[63]

Following *Richmond*, the Supreme Court expanded the First Amendment right of access to include jury voir dire[64] and preliminary hearings.[65] In the 1986 case concerning preliminary hearings, *Press Enterprise Co. v. Superior Court [Press-Enterprise II]*, the Court explicitly adopted the two-step inquiry suggested in *Richmond* for determining if a First Amendment right of access exists.[66] The first question was "whether the place and process have historically been open to the press and the general public."[67] Second, the Court asked "whether public access plays a significant positive role in the functioning of the particular process in question."[68] This inquiry, sometimes called the

---

57. *Pell*, 417 U.S. at 834.

58. 448 U.S. 555 (1980). Richmond Newspapers appealed an order closing a murder trial that was being tried for the fourth time after two mistrials, including one due to pretrial publicity, and a conviction reversal based on improperly admitted evidence. The trial was concluded and the defendant acquitted before the appeal reached the Court. *Id.* at 559-63.

59. *Id.* at 581 (Justice Powell did not participate in the case).

60. *Id.* at 563-75.

61. *Id.* at 569-77.

62. *Id.* at 569.

63. *Id.* at 571.

64. Press-Enterprise Co. v. Superior Court of Cal. ("Press-Enterprise I"), 464 U.S. 501 (1984).

65. Press-Enterprise Co. v. Superior Court of Cal. ("Press-Enterprise II"), 478 U.S. 1 (1986).

66. *Id.*

67. *Id.* at 8.

68. *Id.*

functional test, asks whether access enhances the governmental process, for example, by contributing to either perceived or actual fairness in a proceeding.[69]

The *Richmond* line of cases provides weak support for a First Amendment right of access to government records. Those cases dealt only with proceedings in criminal courts and not with records held by other government agencies. Moreover, the first prong of the *Press-Enterprise II* test for First Amendment access—a tradition of openness—is often arguably lacking when it comes to government records. However, some courts following *Richmond* and its progeny have suggested that the positive value of openness—the functional prong—may be sufficient to justify a First Amendment right of access.[70] That right of access may exist independently of any tradition of openness. For example, the Second Circuit in *Application of the Herald Co.* found the functional justification sufficient to declare a First Amendment right of access to pretrial suppression hearings.[71] The court reasoned that although pretrial suppression hearings did not have a tradition of openness, the functional justification was sufficient when "public observation serves important public purposes," such as scrutiny of the criminal justice system.[72] Moreover, the Second Circuit found that a majority of Supreme Court justices in *Richmond* and its progeny had accepted the functional justification, standing alone, as a sufficient ground to support constitutional access rights.[73]

If the functional justification can serve as an independent basis for inferring First Amendment access rights, that principle could well be extended to a right of access to government records in general. However, at present, whether records are available is dependent upon statutory law. It is to that statutory realm that we now turn.

B. A Statutory Approach to Access

1. The Federal Government

A gradual trend in our nation's history of increasing access to information held by the government was countered in the 1940s by secrecy concerns of World War II and Cold War tensions.[74] Although the

---

69. *Id.* at 9.

70. *See generally* Application of the Herald Co., 734 F.2d 93 (2d Cir. 1984).

71. *Id.*

72. *Id.* at 97.

73. *Id.*

74. Barrett, *supra* note 8, at 238; Comment, *The Right of the Press To Gather Information After* Branzburg *and* Pell, 124 U. PA. L. REV. 166, 167-68 (1975).

1946 Federal Administrative Procedures Act (APA)[75] recognized the public nature of government records, the APA also gave the executive branch broad discretion in the disclosure of government records.[76] Section 3 of the APA allowed agencies to determine what information "requiring secrecy in the public interest" should be exempted from disclosure, and whether the person requesting the record was "properly and directly concerned" with the information.[77] The APA lacked a remedy for wrongfully withholding information. Federal agencies and the courts came to use the APA "more as a withholding statute than a disclosure statute."[78]

Press organizations and other advocates of open government looked to Congress to increase access to federal government documents. Media lawyer Harold L. Cross,[79] in *The People's Right To Know*,[80] wrote that "Congress is the primary source for relief. . . . The time is ripe for an end to ineffectual sputtering about executive refusals of access to official records and for Congress to begin exercising effectually its function to legislate freedom of information for itself, the public, and the press."[81] Over the next ten years, U.S. Representative John Moss of California chaired committee hearings in a push toward opening the federal government's records to the public. The work of Cross and the Moss Committee culminated in 1966 legislation replacing section 3 of the APA. This legislation is known as the Freedom of Information Act (FOIA).[82]

Although the FOIA does not have a preamble stating its guiding principle, the Senate Report on the bill states "a general philosophy of full agency disclosure."[83] Interpreting the FOIA, the Supreme

---

75. 5 U.S.C. § 1002 (1946).

76. *Id.*

77. *Id.*

78. Steven Helle, *The News-Gathering/Publication Dichotomy and Government Expression*, 1982 DUKE L.J. 1, 58-59; Paul A. Ruben, Note, *Applying the Freedom of Information Act's Privacy Exemption to Requests for Lists of Names and Addresses*, 58 FORDHAM L. REV. 1033, 1035 (1990).

79. Cross was general counsel for the *New York Herald Tribune*. He prepared the original draft of Maine's Freedom of Access law in 1951. Gordon Scott, *Tapping Officials' Secrets in Maine*, *in* TAPPING OFFICIALS' SECRETS, *supra* note 2.

80. *See* HAROLD L. CROSS, THE PEOPLE'S RIGHT TO KNOW: LEGAL ACCESS TO PUBLIC RECORDS AND PROCEEDINGS (1953) (tracing the growth of the concept of free information over the centuries and the response in this country by courts and legislators).

81. *Id.* at 246.

82. 5 U.S.C. § 552 (1988).

83. The term "agency" includes "any executive department, military department, Government corporation, Government controlled corporation or other establishment in the executive branch of the federal government, . . . or any independent regulatory agency." 5 U.S.C. § 552(e). The Act does not apply to the records of Congress or the federal courts. See 5 U.S.C. § 551(1) for a new definition of agency.

Court has stated that "[t]he basic purpose of the FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed."[84]

The FOIA was an effort by Congress to balance society's interest in open government with other important interests, "such as the public's interests in the effective and efficient operations of government, . . . and in the preservation of the confidentiality of sensitive personal, commercial, and governmental information."[85] All records not specifically exempted must be made "promptly available to any person."[86] Moreover, the FOIA requires federal agencies to state their reasons for withholding documents.[87] Under the FOIA, nine categories of government records may be exempted from disclosure: (1) those relating to national security (granting broad discretion to the president to establish classification criteria); (2) agency rules and practices; (3) statutory exemptions (such as tax returns and census records); (4) confidential business information (such as financial data and trade secrets that might cause competitive harm); (5) interagency or intra-agency memoranda (working documents historically exempted by the common law); (6) personnel or medical files (that "would constitute a clearly unwarranted invasion of personal privacy"); (7) law enforcement investigations; (8) banking reports; and (9) information (maps) about oil and gas wells.[88]

The FOIA does not define "record,"[89] nor does it address the medium in which public records are maintained; it does not mention

---

84. NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978).

85. U.S. DEP'T OF JUSTICE, GUIDE TO THE FREEDOM OF INFORMATION ACT 343 (1992). *See also* H.R. Rep. No. 1497, 89th Cong., 2d Sess. 3-4 (1966); S. Rep. No. 813, 89th Cong., 2d Sess. (1965).

86. 5 U.S.C. § 552(a)(3). The statute provides:

> Except with respect to the records [mandated to be] made available under paragraphs (1) and (2) of this subsection, each agency, upon any request for records which (A) reasonably describes such records and (B) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.

Id.

87. *Id.* § 552(a)(6)(A)(i).

88. *Id.* § 552(b)(1)-(9).

89. The Supreme Court, in Forsham v. Harris, 445 U.S. 169, 177 (1980), said an agency must physically possess documents before they are records (exempting reports prepared and possessed by private consultants). In Kissinger v. Reporters Committee for Freedom of the Press, 445 U.S. 136 (1980), the Court said the FOIA does not require an agency to retrieve records that have been removed from the agency. In 1991, Senator Patrick Leahy introduced a bill that would define "records," for purposes of the FOIA, to include electronic information. S. 1940, 102nd Cong., 1st Sess. (1991). The bill would also require agencies to provide records in electronic formats.

computerized records. However, the Computer Security Act of 1987[90] prohibits agencies from withholding computerized records from the public if the records would be available under the FOIA as paper documents.[91] Eight years before the passage of the Computer Security Act, the Ninth Circuit reached a similar result in *Long v. Internal Revenue Service*.[92]

The *Long* court overturned a district court ruling and held that a computer tape was a public record, subject to disclosure.[93] The court wrote: "In view of the common, widespread use of computers by government agencies for information storage and processing, any interpretation of the FOIA which limits its application to conventional written documents contradicts the 'general philosophy of full agency disclosure' which Congress intended to establish."[94]

2. *State Freedom of Information Laws*

Because the FOIA pertains only to federal records, access to records produced and held by states, counties, or municipalities is established by state law. All fifty states and the District of Columbia have statutes providing public access to government records.[95] The comprehensiveness of these open records statutes varies significantly. Some states, such as Louisiana,[96] North Dakota,[97] New Hampshire,[98] and Florida,[99] have written open records principles into their constitutions. Other states, such as Wisconsin, Massachusetts, and Montana, have had open records statutes for many years.[100] Wisconsin's very first statutes, enacted in 1849, protected both open meetings and open records.[101]

---

90. Act of Jan. 8, 1988, Pub. L. No. 100-235, 101 Stat. 1724 (1988).
91. *Id.*
92. 596 F.2d 362 (9th Cir.), *cert. denied*, 446 U.S. 917 (1980).
93. *Id.*
94. *Id.* at 365 (quoting S. Rep. No. 813, 89th Cong., 1st Sess. 3 (1965)).
95. *See* TAPPING OFFICIALS' SECRETS, *supra* note 2.
96. LA. CONST. art. XII, § 3.
97. N.D. CONST. art. XI, § 6.
98. N.H. CONST., pt. 1, art. 8.
99. Florida voters approved a public records constitutional amendment in November 1992. *See* FLA. CONST. art I, § 24. The amendment won 83.1% approval. *Nov. 3, 1992, General Election Results, Florida Dep't. of State, Div. of Elections* (unofficial). *See also* Kara M. Tollett, Comment, *The Sunshine Amendment of 1992: An Analysis of the Constitutional Guarantee of Access to Public Records*, 20 FLA. ST. U. L. REV. 525 (1992).
100. Wisconsin has had an open records law for 153 years; Massachusetts, 133 years; Montana, 98 years; Florida, 83 years.
101. WIS. STAT. ch. 10, §§ 29, 37, 137 (1849). The original statute requiring constitutional officers to open their records "has survived virtually unchanged." Robert Christensen, *Tapping Official Secrets in Wisconsin* 1, *in* TAPPING OFFICIALS' SECRETS, *supra* note 2.

Most states depended on the discretion of agencies, or on the common law, to provide public access to government records until they were inspired by the federal FOIA to codify the concept of open government. The common law had varied among states, with most courts requiring a person requesting a record to have a legitimate interest in, and a useful purpose for, the requested record.[102] However, the courts in some states, such as Michigan, had granted broad common law rights of access.[103]

Most states' open records laws have preambles that identify the guiding principle: government accountability. Many states tie their statement of intent to American democratic theory.[104] Illinois, for example, links the right of access with enabling "people to fulfill their duties of discussing public issues fully and freely" and making "informed political judgments . . . ."[105] Hawaiian legislators said that opening government to public scrutiny "is the only viable and reasonable method of protecting the public's interest."[106] A Delaware statute declares that "[i]t is vital that citizens have easy access to public records in order that the society remain free and democratic."[107]

The open records statutes of most states grant a right or an entitlement to inspect and copy government records to "every person" or to "any person."[108] Some states grant the right of access specifically to "every citizen."[109]

Most states apply their open records laws to executive branch agencies, counties, and municipalities. A few states, such as North Dakota and Kentucky, apply the law broadly to entities that receive public funding.[110] Many states require some degree of access to records in the state legislature.[111] Most states rely on common law principles to maintain access to the records of the judiciary.[112]

---

102. *See* Cross, *supra* note 80, at 26-29.

103. Herschel Fink & Darlene Darnell, *Tapping Officials' Secrets in Michigan*, TAPPING OFFICIALS' SECRETS, *supra* note 2 (citing Burton v. Tuite, 44 N.W. 282, 293 (1889) ("I do not think that any common law . . . would deny to the people thereof [the] right of free access to, and public inspection of, public records.")).

104. *See, e.g.*, IND. CODE ANN. § 5-14-3-1 (Burns 1987).

105. ILL. REV. STAT. ch. 116, para. 201 (1987).

106. Haw. HB 2002, § 2 (1975).

107. DEL. CODE ANN. tit. 29, § 10001 (1991).

108. *See* TAPPING OFFICIALS' SECRETS, *supra* note 2.

109. ALA. CODE § 36.12 (1992); N.M. STAT. ANN. § 14.2 (Michie 1992); VA. CODE ANN. § 15.1 (Michie 1992).

110. Some states specify the minimum necessary, such as Kentucky, which sets 25% of the entity's total budget as the amount of public funds received that subjects a public agency to its open records law. KY. REV. STAT. ANN. § 61.870 (1) (h) (Baldwin 1992).

111. Including Hawaii, Louisiana, Maine, Mississippi, Nevada, New Hampshire, New Jersey, North Carolina, North Dakota, Ohio, Utah, West Virginia. HAW. REV. STAT. § 92F.2

Computers are only beginning to have an effect on these public records laws. Illinois[113] is one of the few states that has recognized the impact of computers on public records. The state requires public agencies to furnish lists of records they maintain and a description of how to obtain computerized records "in a form comprehensible to persons lacking knowledge of computer language or printout format."[114]

3. *The Right To Know in Florida*

Florida has had a tradition of open government since 1909.[115] Its public records law statement of intent says: "It is the policy of this state that all state, county, and municipal records shall at all times be open for a personal inspection by any person."[116] The Florida public records law defines public records to include "all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings or other material, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency."[117]

All records are available for inspection by the public unless there is a specific statutory exemption.[118] Those denied access to the records may institute a civil action, which takes priority over other pending cases, to compel the agency to allow access.[119] Agencies and officials that violate the Act are subject to both noncriminal and criminal sanctions, as well as assessment of a prevailing requester's attorneys' fees.[120]

The case law growing out of Florida's public records law[121] has reinforced its broad scope[122] and articulated its underlying philosophy.

(1992); LA. REV. STAT. ANN. § 44.8 (West 1991); ME. REV. STAT. ANN. tit. I, § 401 (West 1991); MISS. CODE ANN. § 25.61 (1991); NEV. REV. STAT. § 239.010 (1991); N.C. GEN. STAT. § 132.1 (1992); N.D. CENT. CODE § 44.04 (1991); OHIO REV. CODE ANN. § 149.43 (Baldwin 1992); UTAH CODE ANN. § 63.2 (1992); W. VA. CODE § 4.3 (1992).

112. States with statutory mandates of access to judicial records include Nevada, North Carolina, Ohio, Utah, and Wyoming. NEV. REV. STAT. ANN. § 3.280 (Michie 1991); N.C. GEN. STAT. § 7A-109 (1992); OHIO REV. CODE ANN. § 1901.31 (Baldwin 1992); UTAH CODE ANN. § 63-2-301 (1992); WYO. STAT. § 16-4-203 (1992).

113. ILL ANN. STAT. ch. 116, para. 205 (Smith-Hurd 1987).

114. *Id.*

115. *See generally* ch. 5943, Laws of Florida (1909).

116. FLA. STAT. § 119.01(1) (1991).

117. *Id.* § 119.011(1).

118. Wait v. Florida Power & Light Co., 372 So. 2d 420, 424 (Fla. 1979).

119. FLA STAT. § 119.11(1) (1991).

120. *Id.* § 119.10 (penalties); *id.* § 119.12 (attorneys' fees).

121. *Id.* ch. 119 (open records).

122. OFFICE OF THE ATT'Y GEN., GOVERNMENT-IN-THE-SUNSHINE MANUAL, vol. 15 (1993).

For example, in 1985 the Second District Court of Appeal in *Lorei v. Smith*[123] said:

> The legislative objective underlying the creation of [the public records law] was to insure to the people of Florida the right to freely gain access to governmental records. . . . The breadth of such [a] right is virtually unfettered, save for the statutory exemptions designed to achieve a balance between an informed public and the ability of government to maintain secrecy in the public interest. . . . When the demand for disclosure competes with a public interest, asserted to be protected by statutory exemption, the judiciary's role is to insure that the governmental claim does not defeat the right to disclosure.[124]

Florida courts have thus been active in protecting the right of access. The Fifth District Court of Appeal found in *Fritz v. Norflor*[125] that the law requires compliance by every person who has custody of public records.[126] In *News Press Publishing Co. v. Gadd*,[127] the Second District Court of Appeal held that all documents falling within the scope of the public records law are subject to disclosure unless specifically exempted by legislation.[128] That court also found the motivation of the seeker is irrelevant; the only viable issue is whether the documents sought are public records.[129]

The Fourth District Court of Appeal in 1982 considered *Seigle v. Barry*,[130] the first Florida case involving computerized records. In *Seigle* economists retained by a bargaining unit for employees of the Broward County School Board sought access to some of the board's public records maintained on a computer.[131] The court said that "information stored on a computer is as much a public record as a written page in a book or a tabulation in a file stored in a filing cabinet."[132] The court also said that "all of the information in the computer, not merely that which a particular program accesses,

123. 464 So. 2d 1330 (Fla. 2d DCA), *rev. denied*, 475 So. 2d 695 (Fla. 1985).
124. *Id.* at 1332.
125. 386 So. 2d 899 (Fla. 5th DCA 1980).
126. *Id.* at 900.
127. 388 So. 2d 276 (Fla. 2d DCA 1980).
128. *Id.* at 278.
129. *Id.*
130. 422 So. 2d 63 (Fla. 4th DCA 1982), *rev. denied*, 431 So. 2d 988 (Fla. 1983).
131. *Id.* at 64. The board had agreed to allow access to the computer records, including the computer tapes, but refused to use a specially designed program to provide the information in a printout format the economists preferred. *Id.* at 65.
132. *Id.*

should be available for examination and copying in keeping with the public policy underlying the right-to-know statutes."[133]

III. PUBLIC ACCESS TO COMPUTERIZED GOVERNMENT RECORDS: THE STATE OF THE PRACTICE

A. Computers in Government

One of the chief obstacles to accessing government information in the computer age has been the low priority placed on public access in the design of government computer systems. Over the past decade or more, government computer use has increased dramatically. In just a few years, some agencies have gone from filing paper records on seemingly endless rows of shelves in huge storage rooms to keeping most of those records in computers. It has been a monumental task simply to ensure that an agency's employees have access to the records. Employee access has thus often been the priority, frequently relegating public access to an afterthought.

Governments use computers in large part for convenience and cost savings. As years have passed and governments have grown, so has the amount of records governments keep. In many cases it has become impractical, if not impossible, to continue to handle paper records. It takes too much space and too many employees to keep track of paper records. At the same time, the cost of basic computer technology has plummeted, making computers affordable to even the smallest governmental units.[134]

1. Federal Agencies

On the federal level, use of computers has grown phenomenally in the past decade. The number of large computers—known as mainframes—in use by federal agencies climbed from about 22,000 in 1986 to nearly 48,000 at the beginning of 1990.[135] Those computers were worth an estimated $10.5 billion.[136] Use of smaller microcomputers,

---

133. *Id.* The court ruled that agencies may provide access to computer records through programs normally used to maintain the public records, but were not obligated to provide records in the format demanded by the requester. *Id.* at 66. Access by a specially designed program may be permitted at the discretion of the record holder, and courts may determine when special programs are necessary for full disclosure. *Id.* at 66-67.

134. Kenneth L. Kraemer et al., *Trends in Municipal Information Systems 1975-1985*, 18 BASELINE DATA REPORT, at 2.

135. GENERAL SERVS. ADMIN., FEDERAL INFORMATION RESOURCE MANAGEMENT, MICROCOMPUTER SURVEY REPORT (Sept. 1988).

136. *Id.*

often known as personal computers, grew from about 490,000 in 1987 to more than one million in 1989.[137]

2. State and Local Agencies

Growth on the state and local levels has been just as dramatic. Even the smallest municipal governments may now use computers to store at least some of their records.[138] Ninety-seven percent of the nation's cities were using computers by 1985, an increase of more than ninety percent from a decade earlier.[139]

In Florida, a 1989 survey by the Florida Department of State found that eighty-three percent of responding agencies said at least twenty-five percent of their records were computerized.[140] Thirty-four percent said more than seventy-five percent of their records were computerized.[141]

B. Forms of Access

The various computer technologies have clouded the issue of how best to provide the public access to government records. With paper records, the issue was clear: Anyone who wanted to examine a record could sit down with the record and review it at no cost. The record usually could be photocopied for a nominal fee.[142] Electronically held information, however, can be produced in a variety of formats—a fact that has complicated the issue.

The electronic equivalent of viewing a paper record is either a computer printout or a public access computer terminal. The information kept in a computer can be printed, just like a paper record. Public terminals, on the other hand, allow a user to view the electronic record on a video screen—through security measures that will be described later—without the ability to alter it.[143]

However, computers offer more possibilities for access. The information a user requests can be made available on a magnetic tape or

---

137. GENERAL SERVS. ADMIN., FEDERAL EQUIPMENT DATA CENTER, AUTOMATIC DATA PROCESSING EQUIPMENT IN THE U.S. GOVERNMENT (Apr. 1990).

138. Jeffrey Brudney, *Computers and Smaller Local Government*, 12 PUB. PRODUCTIVITY REV. 179, 184 (1988).

139. Kraemer, *supra* note 134, at 2.

140. FLORIDA DEP'T OF STATE, INFORMATION TECHNOLOGY AND PUBLIC RECORDS: EMERGING ISSUES 42 (1991) [hereinafter EMERGING ISSUES].

141. *Id.*

142. *See, e.g.*, FLA. STAT. § 119.07(1)(a) (1991).

143. Interview with Richard M. Saig, computer systems officer, Computer Systems Division, Jacksonville, Fla. (Mar. 5, 1990) [hereinafter Saig Interview]. For a discussion of security measures, see *infra* text accompanying note 169.

computer disk. This can be a great advantage to those seeking a large volume of records. For instance, a real estate company might be interested in property tax records for hundreds of homes in a county. The county could print the information on paper for the real estate company to enter into its own computer. Or, the county could provide the information in its electronic format. The real estate company could then electronically load the information into its computer, saving time and money. However, there often is a formidable technical challenge if the two computer systems are not compatible.

At least one survey has shown that government agencies still rely most heavily on paper formats when providing access. In the Florida Department of State survey of records custodians in 1989,[144] most of the agencies responding—eighty-three percent—reported they would provide a computer printout to members of the public who asked to examine or inspect a computerized record.[145] Sixty percent of the agencies reported providing an on-site public access computer.[146]

If a member of the public asked for a copy of a computerized record, most agencies—eighty-four percent—said they would provide a computer printout.[147] Thirty-seven percent said they would provide a computer tape, while nineteen percent would provide a diskette when asked.[148] Only twenty percent said they offered some type of remote access via telephone lines to their computers for examining or copying records.[149]

Another issue is an agency's willingness to alter computer programs to produce requested information. For instance, a journalist might want to search a courthouse computer database to determine whether a certain judge has been tough or lenient in sentencing drunk drivers. But rather than reviewing every drunk driving case, the journalist may want to sort the cases by the judge's name. So the journalist might ask the records custodian to modify the database management system or applications program to allow the search. Some users believe that to take full advantage of the new electronic information technology, agencies should provide this type of reprogramming. Some records custodians, however, have argued that such searches create "new" records, something not required under most freedom of information laws. In addition, custodians have said, the cost and the time it takes to reprogram are prohibitive.[150]

---

144. *See* EMERGING ISSUES, *supra* note 140.
145. *Id.* at 44.
146. *Id.*
147. *Id.* at 45.
148. *Id.*
149. *Id.* at 44.
150. Interviews with Lynwood Roberts, tax collector, Jacksonville, Fla.; Lonnie E. Paulk,

C. Examples of Public Access Systems

Peter Hernon and Charles McClure, in their 1987 critique of federal information policies, found that agencies used extensive resources to design and develop electronic information systems.[151] Although many agencies paid inadequate attention to preparing indices to the information and making other provisions to allow easy public access,[152] there are exceptions at both the federal and state levels.

The first large federal electronic information system designed for public access was the Security and Exchange Commission's $35 million Electronic Data Gathering and Retrieval system, or EDGAR.[153] With EDGAR, the SEC collects, processes, and disseminates more than nine million pages of securities filings each year via computer.[154] Previously, all of the documents were printed and filed on paper. EDGAR benefits the SEC by simplifying the internal processing of prospectuses, registrations, and other filings. But EDGAR also benefits the users of SEC information by making the documents available by computer at remote locations.

A private contractor operates the system for the SEC.[155] Because the information is public, neither the SEC nor the contractor is allowed to exert any form of copyright or ownership over the data kept in EDGAR. The contractor generates revenue by charging a fee to users who access EDGAR to examine or retrieve public documents or information.[156]

The Environmental Protection Agency (EPA) also has established an innovative public access program. The agency's list of companies that emit any of more than 350 toxic pollutants is now available through an electronic database,[157] the Toxic Release Inventory. It is accessible to anyone with a microcomputer and a telephone modem through the National Library of Medicine's Toxicology Data Net-

---

deputy assistant tax collector, Jacksonville; Kim Stribling, electronic data processing methods coordinator for the tax collector's office, Jacksonville (Mar. 7, 1990).

151. PETER HERNON & CHARLES MCCLURE, FEDERAL INFORMATION POLICIES IN THE 1980'S: CONFLICTS AND ISSUES 168 (1987).

152. *Id.*

153. Robert M. Gellman, *Authorizing EDGAR: Information Policy in Theory and Practice*, 5 GOV'T INFO. Q. 201-06 (1988). In 1992, EDGAR began to automatically accept electronic document filings—a significant improvement of the system's capabilities. Kurt Eichenwald, *The S.E.C. Goes Electronic as Edgar Starts Running*, N.Y. TIMES, July 16, 1990, at C4.

154. Gellman, *supra* note 153, at 201.

155. *Id.* at 203.

156. *Id.*

157. ENVIRONMENTAL HEALTH CTR., NATIONAL SAFETY COUNCIL, CHEMICALS, THE PRESS AND THE PUBLIC (undated).

work, called TOXNET. There is an hourly fee to access the database.[158]

Numerous examples of public access programs can be found at the state level. For example, Michigan's "Browse" system allows the public to monitor the progress of a legislative bill remotely by patching into a state database through computers in homes or offices.[159] In Minnesota, a nonprofit youth services program can access, via a computer in its office, certain information about its clients held in databases by the state's welfare office.[160] Also, insurance companies have similar access to driver's license records, and certain law firms have limited access to information on criminal cases kept on computer by law enforcement agencies.[161]

In Florida the Secretary of State provides similar dial-up access to its Division of Corporation's records, which include records for all active and inactive corporations registered with the state.[162] The state contracts with a private information company, CompuServe Inc., to make the records available electronically. CompuServe packages the records in a form attractive to users and charges a subscription fee to anyone who wants access. The Department of Highway Safety and Motor Vehicles also provides remote access to selected driver's license and motor vehicle records through CompuServe.[163] All of these Florida records may still be reviewed by the public without cost at the appropriate agency, unless there is specific statutory authority for a fee.[164]

However, such examples are unusual. Far more common are agencies that, for a variety of reasons, frustrate access to government information held in computers.

D. Obstacles to Access

The U.S. Office of Technology Assessment has identified seven factors as major impediments to the development of efficient systems of public access to computerized government records on the state and

158. *Id.*

159. U.S. OFFICE OF TECH'Y ASSESSMENT, INNOVATIVE USE OF INFORMATION TECHNOLOGY FACILITATING PUBLIC ACCESS TO AGENCY DECISIONMAKING: AN ASSESSMENT OF THE EXPERIENCE IN STATE AND LOCAL GOVERNMENTS 14-34 (1985).

160. *Id.*

161. *Id.*

162. FLORIDA'S INFORMATION POLICY, *supra* note 5, at 77.

163. *Id.*

164. *See, e.g.*, FLA. STAT. § 119.07(1)(a) (1991).

local level. These factors are (1) state laws that do not place a priority on access; (2) vulnerability of systems to security breaches from either loss of electronic data as a result of technological problems or unauthorized access to the data; (3) threats to the confidentiality of some information kept on computer; (4) cost of hardware and software needed to provide access; (5) ability of available software to provide requested information; (6) lack of citizen awareness and interest; and (7) varied technology, making it difficult to standardize computer systems and access programs.[165]

These factors have the effect of slowing down, or even halting, access programs. In California, for instance, a report on the need for a public access policy recommended that any such policy be developed over the course of several years, rather than months.[166] The report cited the need to "retrofit large and varied systems and/or employ developing new technology to resolve the conflicting goals of providing public access and yet safeguarding confidential information and the physical data itself."[167] The California report identified security and cost as perhaps two of the most difficult issues to overcome.

The security of electronically held information has been a major concern at all levels of government. A 1990 report from the State University System of Florida on computer security makes this point: "The value of state data and software, in terms of restoration costs and losses due to unauthorized disclosure, far exceeds the value of its associated hardware. For that reason, information processed by computers must be recognized as a major state asset and be protected accordingly."[168]

Protection of electronic information takes two forms: protection from loss due to failure of the computer system and protection from unauthorized access. Protecting electronic records from a computer failure is akin to protecting paper records from a fire. To accomplish this, many agencies "back up" electronically stored information onto computer tapes daily.[169] In effect, this provides a spare copy of the data.

To protect against unauthorized access, particularly in light of privacy or national security concerns, agencies frequently employ a series of codes and passwords. These allow only certain users access to specific parts of a database, giving some people the ability to read a rec-

---

165. U.S. OFFICE OF TECH'Y ASSESSMENT, *supra* note 159, at 31.

166. *Id.* at 21-23.

167. *Id.*

168. OFFICE OF RESOURCE MGMNT., STATE UNIV. SYS. OF FLA., STATE OF FLORIDA INFORMATION RESOURCE SECURITY STANDARDS AND GUIDELINES (1990).

169. Saig Interview, *supra* note 143.

ord, some the ability to read and retrieve, and some the ability to read, retrieve, and manipulate. The codes prompt the computer to display only certain information menus and function options the user is allowed to access. The most sensitive information will be accessible by the fewest number of users. If used correctly, user codes and passwords can be an effective means of control.

Cost is another potential impediment to access. While computers save in personnel costs, they still cost governments a great deal of money. The federal government, as mentioned, has more than $10 billion of mainframe computers.[170] The cost of computer equipment is often used in arguments about whether and how much the public should pay for access to the information stored in them.

During the Reagan Administration, these issues of cost, privacy, and security were arguments used to curtail access. In 1985 the Office of Management and Budget released a circular to provide a "general policy framework for the management of federal information resources."[171] The circular's general thrust was to minimize the federal government's role in disseminating computerized information. Instead, the private sector was encouraged to take raw computer data from the government and make it accessible to the public for a fee. In one sense, public access was sacrificed in the process: the cost of subscribing to private information vendors, while it might be reasonable for businesses, may be beyond the reach of the average citizen.

However, the U.S. House Committee on Government Operations took the opposite approach. The Committee viewed modern information technology as a means to expand the nature and scope of public access to government information and encouraged federal agencies to do so.[172] Computers, because of the volume of information they store and the speed at which they can retrieve it, can allow more efficient and complete access to governmental information.

To provide effective access for those seeking information about government, agencies must plan for access, which in general they have not done. In 1984 the U.S. Office of Technology Assessment found that computer technology has been used primarily as a means to collect, store, organize, and retrieve public information for internal use.[173] "Minimal concern is given during the design and implementa-

170. *See supra* note 136 and accompanying text.

171. OFFICE OF MGMNT. AND BUDGET, CIRCULAR NO. A-130, MANAGEMENT OF FEDERAL INFORMATION RESOURCES (1985).

172. Gellman, *supra* note 153, at 200-01.

173. U.S. OFFICE OF TECH'Y ASSESSMENT, FEDERAL GOVERNMENT PROVISION OF PUBLIC INFORMATION: ISSUES RELATED TO PUBLIC ACCESS, TECHNOLOGY, AND LAWS/REGULATIONS xii (1984).

tion of the federal information systems to enhancing user access to public information," the report concluded.[174]

However, the U.S. House Committee on Government Operations in 1986 called on agencies to use modern technology to improve the range and quality of public access to agency records.[175] "As technology permits an agency to upgrade its own ability to access, copy, and manipulate data, an agency should make reasonable attempts to allow public users of agency information to share the benefits of automation," the committee said.[176]

IV. Legal Issues in Computerized Access

Any practical discussion of access to government-held records should begin with a definition of what constitutes a "public record." This section will look at how "public record" has been defined by the federal courts under the FOIA, how various states have defined the term, and in particular how Florida defines to what information citizens have access. This section will then look at how these definitions have evolved in recent years as paper records yield to the onslaught of computer technology.

A. The Freedom of Information Act of 1966

In 1966—when the computer was a behemoth of wires and circuits and still somewhat of a novelty within the federal bureaucracy—Congress passed the Freedom of Information Act (FOIA). The legislation affirmed the belief that the business of government should be the people's business.[177] It opened the records of scores of administrative agencies to public scrutiny, subject only to nine exemptions.[178] The requirements of the FOIA did not apply to Congress itself.[179] Interestingly, the term "record" was not specifically defined in the original FOIA.[180]

This oversight was rectified in 1980 by the U.S. Supreme Court in *Forsham v. Harris*.[181] That case involved a FOIA request for data developed and held by a private group of physicians and scientists studying diabetic treatment under a grant from the Department of Health,

174. *Id.*
175. H.R. Rep. No. 560, 99th Cong., 1st Sess. 11 (1986).
176. *Id.*
177. 5 U.S.C. § 552 (1988).
178. *Id.* § 552(b)(1)-(9).
179. *Id.* § 552(a).
180. *See generally id.* § 552.
181. 445 U.S. 169, 176 (1980).

Education, and Welfare (HEW). The Court rejected the request, reasoning that the information was not in the immediate control of HEW and therefore was not an "agency record" under the FOIA.[182] Borrowing from the Federal Records Disposal Act,[183] the Court defined public record as "all books, papers, maps, photographs, *machine[-]readable materials or other documentary materials, regardless of physical form or characteristic*, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business."[184]

In *Forsham* the Court said records sought under the FOIA must be in the control of an agency, and that the Act did not require an agency to acquire records or create new ones.[185] The Court's broad definition of the *form* of public records did sweep virtually any kind of nonexempt information in the control of an agency into the ambit of the FOIA—including information stored in agency computers. It did not, however, include physical objects.

The Supreme Court recently established a two-part test to determine whether government-held information qualified as an "agency record" under the FOIA. In *Department of Justice v. Tax Analysts* the Court said that a record must have been created or obtained by an agency and that the record must be under the agency's control at the time of the FOIA request.[186]

The Supreme Court's definition of public records clearly includes information held in government computers. Courts, however, have given agencies discretion over how computerized information is made available to the public and have said that agencies do not have to use their information technologies to dramatically reconfigure data or create new documents to satisfy FOIA requests. The Supreme Court's definition of "public record" provided expansive wording similar to various state public records statutes, as the following section demonstrates.

B. State Definitions of Public Records

Every state has adopted some form of statute addressing the public's right of access to government information.[187] Many recent sta-

182. *Id.* at 177.
183. 44 U.S.C. § 3301 (1976).
184. *Forsham*, 445 U.S. at 183 (emphasis added).
185. *Id.* at 183-85.
186. 492 U.S. 136 (1989).
187. *See* Burt A. Braverman & Wesley R. Hepler, *A Practical Review of State Open Records Laws*, 49 GEO. WASH. L. REV. 720 (1981).

tutes define public records broadly, similar to the definition offered in *Forsham*. Kentucky, for instance, defines public records as "all books, papers, maps, photographs, cards, tapes, disks, diskettes, recordings or other documentary material regardless of physical form or characteristic, which are prepared, owned, used, in the possession of or retained by a public agency."[188]

A few states, such as New Mexico and Arizona, provide no binding definition of what constitutes a public record for purposes of public inspection. New Mexico allows the "public record" status of information to be decided judicially on a case-by-case basis.[189] Of the fifty states and the District of Columbia, most define "public record" without regard for physical form or characteristic. Such definitions make computer-held government information at least theoretically accessible to the public. Some state access statutes explicitly define computer-held information as a public record.[190]

Among the access questions facing states are: Are computerized public records subject to the same degree of access as records in their traditional forms? Who decides the form in which computerized records are made available to the public? Is a computer tape itself a public record and subject to copying, or can agencies meet their statutory obligations by providing paper copies of information? Are computer programs themselves, as distinct from the information stored in computers, public records?

In a pair of often-cited cases from the early 1970s, courts held that computer tapes of paper records were public records. In 1971 the New Mexico Supreme Court said that a master computer tape of voter registration affidavits was as much a public record as the affidavits themselves.[191] Likewise, the New Hampshire Supreme Court held in 1973 that a computer tape of field cards used to prepare property tax assessments was itself a public record.[192] The court said that a researcher was entitled to a copy of the tape, made at his own expense.[193]

---

188. KY. REV. STAT. § 61.870(2) (Baldwin 1992).

189. *See* Newsome v. Alarid, 568 P.2d 1236, 1240-41 (N.M. 1977).

190. Statutes in 13 states specifically mention computers: Arkansas, Connecticut, Florida, Illinois, Kansas, Kentucky, Maryland, Minnesota, Nebraska, North Carolina, South Carolina, Utah, and Wisconsin. ARK. CODE ANN. § 25-19-105 (Michie 1992); CONN. GEN. STAT. § 1-19a (1990); FLA. STAT. § 119.07 (1991); ILL. REV. STAT. ch. 116, para. 205 (1992); KAN. STAT. ANN. § 88-152 (1991); KY. REV. STAT. ANN. § 61.975 (Baldwin 1992); MD. CODE ANN. STATE GOV'T § 10-611(f) (1984); MINN. STAT. § 138.17 (1992); NEB. REV. STAT. § 81-1117.04 (1991); N.C. GEN. STAT. § 132-1 (1992); S.C. CODE ANN. § 30-9-75 (Law. Co-op. 1991); UTAH CODE ANN. § 63-2-103 (1992); WIS. STAT. § 19.32 (1990).

191. Ortiz v. Jaramillo, 483 P.2d 500 (N.M. 1971).

192. Menge v. City of Manchester, 311 A.2d 116 (N.H. 1973).

193. *Id.* at 119.

Additionally, the Illinois Supreme Court decided in 1990 that Cook County was required by the Illinois Freedom of Information Act to provide a computer tape of employee records to a union, absent a statutory exemption.[194] "Under the Illinois Act, having received a proper request to inspect or copy a public record, the public body must either comply or state why it cannot comply," the court wrote.[195]

Not all state courts regard computer records as necessarily open to scrutiny of any kind. The New Jersey Supreme Court has ruled that computerized records are not necessarily public records. In *North Jersey Newspapers Co. v. Passaic County Board of Chosen Freeholders*,[196] the court denied a request for telephone records and asserted that the state legislature did not intend that "all detailed information a modern computer-based system can generate constitutes [public records]."[197]

States have recently begun to address the issue of whether agency-developed computer programs—the digital instructions that tell computers how to sort and organize data—are public records.[198] A New Jersey Superior Court held that a computer spread-sheet program developed by a consultant to the state Department of Health to analyze hospital data was not a public record.[199] In a similar vein the Ohio Supreme Court has said that a computer program developed by a private enterprise to process state public records is not a public record.[200] The court reasoned that the agency could provide the records in paper form and that the software required for use of the record on magnetic tape was thus not necessary under the state public records statute.[201] The court said a requester was free to negotiate a price with the private contractor to obtain the computer program.[202]

---

194. AFSCME v. County of Cook, 555 N.E.2d 361, 365-66 (Ill. 1990).

195. *Id.* at 366.

196. 601 A.2d 693 (N.J. 1992).

197. *Id.* at 696.

198. PUBLIC RECORDS DIV., OFFICE OF THE MASS. SECRETARY OF STATE, 2 REPORT OF THE FIRST NATIONAL CONFERENCE ON ISSUES CONCERNING COMPUTERIZED PUBLIC RECORDS 9 (Boston, Mass., App., Sept. 1986). Five states specifically exempt computer software from their public records law: Minnesota, Kansas, Oklahoma, Oregon, and Virginia. MINN. STAT. § 13.03 (5) (1992); KAN. STAT. ANN. § 45.221 (a) (16) (1991); OKLA. STAT. tit. 51, § 24A.10 (B) (3) (1991); OR. REV. STAT. § 268.357 (1) (1991); VA. CODE ANN. § 2.1 - 342 (A) (24) (Michie 1992); Utah and Florida exempt software when computer programs would compromise agency data or security. FLA. STAT. § 119.07 (1991); UTAH CODE ANN. § 63-2-103 (1992).

199. Asbury Park Press, Inc. v. New Jersey, 558 A.2d 1363 (1989) (spread-sheet was not required by law to be kept on file and thus was not a public record).

200. State *ex. rel.* Recodate Co. v. Buchanan, 546 N.E.2d 203 (Ohio 1989).

201. *Id.* at 205.

202. *Id.*

In the absence of statutes and case law specifically defining computer records, agencies have frequently turned to their state attorneys general for guidance. As the following discussion illustrates, agency queries have asked whether computer-held records were public records, whether computer tapes were themselves public records, whether computer tapes were public records when the same information existed in another format, and whether computer programs were public records.

The advent of computer technology has sometimes rendered state and local agencies' understanding of public record laws obsolete. The laws, written when most records were paper, often prove ambiguous when agency personnel are confronted with requests for information in nontraditional forms. For example, in 1978 the Maryland Attorney General's Office was asked whether the state Public Information Law was intended to apply to information on computer tapes. The opinion said there was "no rational basis to distinguish a computer tape from a sound recording, film, paper or other type of document containing information."[203] In 1979 the South Carolina Attorney General's Office issued an opinion advising an agency that the mere fact that records were held in a computer did not affect their status as public records.[204]

The Connecticut Attorney General's Office advised that information compiled by computer from documents received by a state agency during the conduct of state business was itself a public record.[205] In 1980 the Tennessee Attorney General's Office said that records stored in computers, but not printed out, were public records if they otherwise would be.[206] That same year, the Tennessee Attorney General distinguished between computer records that reflected the final form of a public record and preliminary drafts that assisted in the creation of such a document.[207] The Florida Attorney General reached a similar conclusion.[208]

Another issue raised by computerization is the question of the status of computer programs developed by state and local agencies. A

---

203. 63 Op. Md. Att'y Gen. 659 (1978).

204. 79 Op. S.C. Att'y Gen. 134 (1979). *See also* Op. Wash. Att'y Gen. No. 18 (July 23, 1981) (public records include records on computer magnetic tape, disk-readable records, and other machine-readable media); Ops. Tex. Att'y Gen. No. 401 (1983), No. 352 (1982) (information does not fall outside state records act merely because it is stored on magnetic tapes or disks); Op. Neb. Att'y Gen. No. 128 (1983) (information that is a public record in its original form remains so when maintained in computer files).

205. 83 Op. Conn. Att'y Gen. 87 (1983).

206. 80 Op. Tenn. Att'y Gen. 125 (1980).

207. *Id.* at 288.

208. 1985 FLA. ATT'Y GEN. ANN. REP. 87.

1970 Wisconsin Attorney General opinion said an agency could sell a computer program as surplus, so long as the program was not developed for resale purposes.[209] Two county-developed computer programs used by a county appraiser's office were public records, according to a 1987 Oregon Attorney General opinion.[210]

C. *Computerized Records in Florida*

Florida's public records law provides an expansive definition of "public records." It defines public records as "all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings or other material, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency."[211] The Florida Supreme Court further expanded this definition interpreting public records to include "any material prepared in connection with official agency business which is intended to perpetuate, communicate, or formalize knowledge of some type."[212]

While the statute's definition of public record refers to government information "regardless of physical form or characteristic," it makes no specific mention of computerized information.[213] In 1982, however, the Florida Fourth District Court of Appeal ruled in *Seigle v. Barry* that all data held in state computers—not just that which is accessible by a particular program—are public records.[214]

The Florida Attorney General followed *Seigle* when the Florida Game and Fresh Water Fish Commission asked about public access to computer tapes of names and addresses of subscribers to a Commission publication. The Attorney General advised that, absent a statute exempting such records, the computer tapes were public records within the meaning of the public records law.[215]

The state's definition of public records does not encompass rough drafts or notes to be used in preparing some other documentary material.[216] Computer counterparts to such rough drafts and notes are not

---

209. 59 Op. Wisc. Att'y Gen. 145 (1970).

210. 21 Op. Or. Att'y Gen. 26 (1987).

211. FLA. STAT. § 119.011(1) (1991).

212. Shevin v. Byron, Harless, Schaffer, Reid & Assocs., Inc., 379 So. 2d 633, 640 (Fla. 1980).

213. Section 119.07(1)(b), however, does mention computers with respect to fees for the "extensive" use of information technology resources. *See also* FLA. STAT. § 119.085 (1991).

214. Seigle v. Barry, 422 So. 2d 63, 65 (Fla. 4th DCA 1982), *rev. denied*, 431 So. 2d 988 (Fla. 1983).

215. 1985 FLA. ATT'Y GEN. ANN. REP. 3.

216. *Id.* at 87.

public records, the Attorney General's office said in response to a query from the Florida Secretary of State.[217] The Secretary asked whether machine-readable intermediate files—computer files often created for only seconds during the document-construction process—were public records that must be maintained. The opinion concluded that the files were not public records because they "are not intended to perpetuate or formalize knowledge of some type but rather constitute mere precursors of government records."[218]

Another issue with computer-record implications involves whether a county must provide access to copies of government records stored outside a county when original documents are available at the county courthouse. The Santa Rosa County Attorney asked the Attorney General whether the county had to transport microfilmed records stored outside the county back to the courthouse to comply with a public records request. The Attorney General, citing *Seigle*,[219] noted that the requester could not determine the format in which the records are disclosed. The opinion said, however, that by storing and maintaining the records at a private storage facility, the county had designated the storage company as the custodian of the copies of the public records, and as such the company was subject to the copying and inspection provisions of Florida's public records law.[220] The implication, when copies of government computer records are stored by a third party in a centralized location, is that such records are equally accessible under the state's public records law.

Another significant access issue is whether a computer program itself—the software that collects, stores, retrieves, and processes information—is a public record. In 1990 the Florida Legislature amended the public records law to allow agencies to copyright and sell copies of agency-developed data processing software at market prices.[221] However, the amendment requires agencies to make available software "solely for application to data or information maintained or generated by the agency that created the [software]" under the public records law fee structure.[222] Presumably, copyrighted agency software should not, under the amendment, inhibit access.

---

217. *Id.*

218. *Id.*

219. Seigle v. Barry, 422 So. 2d 63 (Fla. 4th DCA 1982), *rev. denied*, 431 So. 2d 988 (Fla. 1983).

220. 1988 FLA. ATT'Y GEN. ANN. REP. 26.

221. FLA. STAT. § 119.083 (1991). Bills pending in the Legislature as this Article went to press would repeal this statute and include agency-created software within the definition of "public record" in § 119.01. Fla. SB 562 (1993); Fla. HB 1683 (1993). Both bills had been approved by committees as this Article went to press and were pending before the Senate and the House.

222. FLA. STAT. § 119.083(3) (1991).

The Attorney General has also broadly interpreted access laws to prevent computerized communication among government officials from limiting access. In 1989 the Attorney General advised that computer messages among public officials who conduct public business are the same as public meetings and create public records subject to the open records law.[223] In one opinion, the Attorney General advised the Hillsborough County Attorney that if county commissioners linked their offices on a computer network, they could not use the technology to conduct meetings.[224] The use of the computers by commissioners to communicate among themselves on issues pending before the body appears to be subject to the open meetings law, the opinion said. It added that any related information transmitted by or held in the county commission's computer system was a public record.[225]

A second opinion involved the Palm Beach County School Board's decision to put computer terminals, linked to the school board's offices, in board members' homes.[226] The Attorney General's office advised that correspondence among public officials about public business was a public record. An assistant state attorney commented, "'[t]he definition of a public record is intended to include just about anything—not just paper documents.'"[227]

In summary, computerized government information in Florida is clearly a public record. The Attorney General's office has said that computer tapes themselves are public records and has suggested that computerized copies of public records, even if held by third parties, are as public as the original records.

D. Novel Questions About Computer Access

While the courts leave little doubt that information in government computers constitutes a public record, a number of conflicts have arisen over public access to such records. As the court in *Yeager v. DEA* suggested, these cases present novel and important questions concerning the interpretation of the Freedom of Information Act as it

223. 1989 FLA. ATT'Y GEN. ANN. REP. 39.

224. *Id.*

225. *Id.*

226. *Computer Messages Are Public Records*, BRECHNER REP. (Brechner Ctr. for Freedom of Info., Univ. of Fla.), Mar. 1989, at 3.

227. *Id.* For an intriguing twist on this issue at the federal level, see Armstrong v. Executive Office of the President, No. 89-142, 1993 U.S. Dist. LEXIS 95 (D.C. Cir. Jan. 6, 1993), where the court held electronic messages of the outgoing Bush administration could not be fully reproduced on paper and, thus, were records themselves which could not be erased under the Federal Records Act.

applies to agency records stored in computers.[228] The questions being raised include:

—Does the retrieval of data from an agency computer constitute creation of a new record, which the FOIA does not require?

—Do agencies have to create programs to satisfy requests for data not already processed for agency use?

—To what extent must an agency segregate exempt and non-exempt data in a computer to fulfill an FOIA request?

—To what extent must agencies invest in new computer technologies to enhance public access?

—Should the agency or the requester determine the physical form in which a public record will be made available?

1. Duty To Create a New Record

It is well-established that agencies do not have to create records to meet FOIA requests.[229] In the case of paper records, agencies are not required to gather information from various sources to create new documents or to analyze or summarize information in their files. However, what constitutes "creation" of a record when the capabilities of the computers are considered is less clear.

In *Yeager*, for example, a requester sought information that, as it existed in the agency's computer for agency use, was shielded from disclosure under an FOIA exemption.[230] The requester argued that the FOIA imposed a duty on the agency to use computers to edit the data in such a way to make it disclosable.[231] The court rejected this reasoning and concluded that agencies were not required to create a new record by restructuring data in order to satisfy an FOIA request.[232]

In *Long v. IRS* the U.S. Court of Appeals for the Ninth Circuit reached a different conclusion in a similar situation.[233] The Internal Revenue Service argued that providing a computer tape with some information deleted constituted creation of a new record, which the FOIA did not require. The court rejected the IRS's argument. The court said that using agency computers to delete identifying information to protect personal privacy was permissible and that the resulting "record" was not a new record for FOIA purposes.[234]

---

228. 678 F.2d 315, 317, 326-27 (D.C. Cir. 1982).

229. *See generally* Kissinger v. Reporters Comm. for Freedom of the Press, 445 U.S. 136, 153 (1980); NLRB v. Sears Roebuck & Co., 421 U.S. 132, 162 (1975).

230. 678 F.2d at 318.

231. *Id.* at 318-19.

232. *Id.* at 327.

233. 596 F.2d 362 (9th Cir. 1979).

234. *Id.* at 365-66.

Many state courts, mirroring the federal courts, do not require agencies to create new records to satisfy requests for copies of public records. Several state courts, however, have said that removing identifying information or scrambling data to protect identities does not constitute creation of new records. A New York court, for example, held in 1980 that a school district must release test scores after using its computer to delete names and to scramble the order of the names to ensure anonymity.[235] The resulting information was not a new record for access purposes, the court said. The Illinois Supreme Court used similar reasoning in 1989 when it held that a school district was not creating a new record by providing computer compilations of achievement test scores with names removed and the order of the scores scrambled.[236]

In Florida, the Fourth District Court of Appeal declared in *Seigle v. Barry* that the state's public records law does not obligate a custodian to produce a new record by manipulating data contained in existing records.[237] The court stated that "[i]f the health department maintains a chronological list of dog-bite incidents with rabies implications [a] plaintiff, bitten by a suspect dog, may not require the health department to reorder that list and furnish a record of incidents segregated by geographical areas."[238]

2. *Creation of Computer Programs To Meet FOIA Requests*

An issue related to the question of whether generating a document from a computer is "creating" a record is whether agencies must develop computer programs in order to compile or organize information to meet FOIA requests. A federal district court in Pennsylvania said that creation of a special computer program to satisfy a public records request exceeded the U.S. Department of Treasury's obligations to provide records under the FOIA.[239] *Clarke v. U.S. Department of Treasury*[240] arose when an individual asked the Treasury Department for names and addresses of all registered institutional owners of certain bonds, along with the dollar amount, maturity date, and ownership of each bond.[241] The Treasury Department refused the request on the grounds the information as requested did not already exist as an agency record.

---

235. Kryston v. Board of Educ., 430 N.Y.S.2d 688 (N.Y. App. Div. 1980).
236. Bowie v. Evanston Community Consol. Sch. Dist., 538 N.E.2d 557 (Ill. 1989).
237. 422 So. 2d 63 (Fla. 4th DCA 1982), *rev. denied*, 431 So. 2d 988 (Fla. 1983).
238. *Id.* at 65.
239. Clarke v. U.S. Dep't of Treasury, No. 84 Civ. 1873 (E.D. Pa. Jan. 28, 1986).
240. *Id.*
241. *Id.*

The requester argued that the information was neither privileged nor confidential and that a computer program could be written to extract the pertinent information. However, the court said that "[w]hile an agency may be required to produce records that do exist, it is not required to make them."[242] The court also noted that the Treasury Department's own regulations provide that "[t]here is no requirement that records be created or data processed in a format other than required for government purposes" in order to comply with a request.[243]

The issue of computer programming was alluded to in a 1989 case in which a federal district court in California said the Immigration and Naturalization Service had a duty to use its computer to search for records in response to FOIA requests.[244] In *Mayock v. Immigration and Naturalization Service* the court said requests for "all records" under the FOIA should generally be interpreted by the INS to include computer searches of relevant electronic databases.[245] The *Mayock* court, however, did not define "search" or suggest to what extent an agency should program its computers beyond programming already used by the agency.

3. *Segregation of Computerized Data*

Another situation that has posed difficulties for computerized access arises when information disclosable under the FOIA is combined with exempt information in government files. In such instances, the FOIA requires agencies to provide "[a] reasonably segregable portion of a record . . . after deletion of the portions which are exempt . . . ."[246] The notion of what steps agencies should reasonably take to provide access was developed when deleting exempt material consisted of manually blacking out the information on each document.

Based on several cases involving written documents, federal courts have established four criteria to determine whether nonexempt mate-

---

242. *Id.* (citing Kissinger v. Reporters Comm. for Freedom of the Press, 445 U.S. 136, 152 (1980).)

243. *Id.* (citing 31 C.F.R. § 1.5(a) (1984)). *See* American Friends Serv. Comm. v. Department of Defense, No. 83-4916, slip. op. at 13 (E.D. Pa. Aug. 4, 1988), *cited in* FOIA UPDATE, Spring/Summer 1990, at 20. The same federal court that decided *Clarke* later broached the question of whether an agency should develop a "new computer software program" to process agency data. The court, however, never answered this question. *See also* Gurrier v. Hernandez, 566 N.Y.S.2d 406, 407 (N.Y. App. Div. 1991) (agency not required to create statistical information from database, despite requester's claim such creation would be a "very simple matter"); State *ex rel.* Scanlon v. Deters, 544 N.E.2d 680 (Ohio 1989) (agency not required to produce compilation of data that does not presently exist or which computer is not programmed to produce).

244. Mayock v. Immigration and Naturalization Serv., 714 F. Supp. 1558 (N.D. Cal. 1989), *rev'd on other grounds*, 938 F.2d 1006 (9th Cir. 1991).

245. *Id.*

246. 5 U.S.C. §552(b) (1988).

rial is reasonably segregable from exempt material. First, agencies need not segregate—and thus may deny access—when the process results in an unintelligible document.[247] Second, agencies can refuse to segregate when disclosable material is so inextricably intertwined with nondisclosable information that segregation is not feasible and would place an inordinate burden on the agency.[248] Third, disclosure would not be required when disclosable material is largely interspersed with nondisclosable information,[249] once again resulting in a document that does not meaningfully represent the record as a whole. The fourth and final instance occurs when disclosure of nonexempt information would be revealing and endanger the confidentiality of the exempt information within the record.[250]

When records are stored in computers, the issue of segregability becomes more complex. In some cases, deletion of exempt information can be accomplished with the push of a button. Ease of segregation, however, is dependent on how the agency computer system has been designed. It may be easier to formulate a query to segregate nonexempt information on newer databases, such as relational databases, than it is with some older hierarchical mainframe databases.[251] Nonetheless, agencies have been reluctant to recognize that computers can make it easier for them to segregate data, balking at the idea of deleting exempt material to facilitate disclosure.

Two circuits of the U.S. Court of Appeals have attempted to deal with the question of segregability of information held in government computers, with different results.[252] In 1979 the Ninth Circuit said that "editing" identifying information on individual taxpayers to satisfy an FOIA request was within the scope of the agency's duty to reasonably segregate exempt and non-exempt data to satisfy an FOIA request.[253] In *Long v. IRS* the court said it did not believe the "mere deletion of names, addresses, and social security numbers results in the agency's creating a whole new record."[254] The court, however, was

247. *See* Lead Indus. Ass'n v. OSHA, 610 F.2d 70, 86 (2d Cir. 1979).

248. *See* Mead Data Central, Inc. v. Department of the Air Force, 566 F.2d 242, 260 (D.C. Cir. 1977).

249. *See Lead Industry*, 610 F.2d at 70; *see also* Sterling Drug, Inc. v. Harris, 488 F. Supp. 1019 (S.D.N.Y. 1980).

250. *See Lead Industry*, 610 F.2d at 70; *see also* Briton v. Department of State, 476 F. Supp. 535, 541-42 (D.D.C. 1979), *aff'd*, 636 F.2d 600 (D.C. Cir. 1980), *cert. denied*, 452 U.S. 905 (1981).

251. *See generally* Steven Guengerich & Sandra Rotenberg, *Strategic Thinking in Picking a DBMS*, NETWORK WORLD, Oct. 14, 1991, at 55.

252. Yeager v. DEA, 678 F.2d 315 (D.C. Cir. 1982); Long v. IRS, 596 F.2d 362 (9th Cir. 1979).

253. *Long*, 596 F.2d 362.

254. *Id.* at 366.

not clear about whether an agency should create a new computer program to achieve such redaction.

Two years later, in *Yeager v. DEA*, the D.C. Circuit reached a different conclusion when it considered "the extent to which an agency is required to employ its computer capabilities in fulfilling its duty to segregate and release nonexempt material."[255] The case began with a request for several entire DEA computer files on narcotics violations—data normally shielded by a FOIA exemption. The requester asked that the DEA "collapse" the records. Collapsing, a relatively complex process, involves using a computer to eliminate identifying information, leaving only nonsensitive, disclosable aggregate data. Collapsing data, for example, might involve taking specific information, such as a date, and expressing it in more general terms, such as a ten-year span.[256] The court refused to require the agency to collapse the data, maintaining the FOIA "does not contemplate imposing a greater segregation duty upon agencies that choose to store records in computers than upon agencies that employ manual retrieval systems."[257] In other words, the court said that even though an agency's computers can perform tasks to make data lawfully disclosable, the agency's only duty is to perform tasks analogous to segregating information in paper format.

The *Yeager* court concluded that "the FOIA does not mandate that the DEA use its computer capabilities to 'compact' or 'collapse' information as part of its duty to disclose reasonably segregable information."[258] However, the court did suggest that computers provide agencies with more flexibility to meet FOIA requests, and that agencies should be encouraged to perform services they are not required to provide.[259]

4. *Use of New Technology*

While the *Yeager* court encouraged agencies to use their computer capabilities to voluntarily go beyond the letter of the law to satisfy FOIA requests,[260] the extent to which federal agencies have an obligation to invest in costly new technologies in order to enhance public access remains limited. In 1986 a federal court in Florida held that the United States Customs Service was not obligated to invest in costly

255. 678 F.2d at 320.
256. *Id.* at 319 n.9.
257. *Id.* at 322.
258. *Id.* at 327.
259. *Id.* at 326-27.
260. *Id.*

technology to provide computer terminals for public access.[261] In *Martin & Merrell, Inc. v. United States Customs Service* a customs broker seeking certain liquidation entries on file with the Customs Service argued that the Service's Miami division should install on-site computer terminals so that persons seeking information about liquidation dates could access the data without the inconvenience of having to file FOIA requests.[262] In rejecting the broker's argument, the court stated: "The [FOIA] in no way contemplates that agencies . . . should invest in the most sophisticated and expensive form of technology."[263]

5. *Form of Record Disclosure*

Although the FOIA itself never defined exactly what comprised a "record" within the scope of the FOIA, it is reasonable to conclude that the Act envisioned record requests being met by supplying paper documents. But as the computer became the rule rather than the exception in government record-keeping, it became less obvious what constituted an adequate response to a record request when records are potentially available in non-paper form. Records can take the form not only of paper documents, but also of magnetic computer tapes, floppy disks, and other computer-readable formats. With records available in multiple forms, requesters might find one more useful than another. For example, a computer tape of a database that can be electronically analyzed is often much more useful than a bulky computer printout of the same material.

With multiple options available for providing public access, a question arises: Who should determine the form in which a public record is released—the agency holding the record or the party seeking it? In an influential decision, a federal district court concluded that the agency should ultimately decide the form in which a record is provided.[264]

In *Dismukes v. Department of the Interior* a District of Columbia district court held in 1984 that an agency could make information available in a form the agency deemed most useful to the typical requester.[265] The requesting party in this case sought the names and addresses of participants in an Interior Department oil and natural gas leasing lottery, and wanted the records on computer tapes. The Inte-

261. Martin & Merrell, Inc. v. United States Customs Serv., 657 F. Supp. 733, 734 (S.D. Fla. 1986).
262. *Id.*
263. *Id.*
264. Dismukes v. Department of the Interior, 603 F. Supp. 760, 761-63 (D.D.C. 1984).
265. *Id.*

rior Department stored the information on both computer tapes and microfiche files but chose to make it available only in the latter form. The Department argued that it routinely made such information available on microfiche because that was the form requesters generally preferred. The court backed the agency, but cautioned that the form in which the agency chose to provide a record could neither "unreasonably hamper" the requester nor reduce the usefulness of the information.[266] The court followed *Dismukes* in 1988 when it decided *National Security Archives v. CIA*.[267] In that case, the court stated that the Central Intelligence Agency did not have to provide records in electronic database format after it had already provided a computer printout of the records in response to an FOIA request.[268] Again, in *Coalition for Alternatives in Nutrition & Health Care, Inc. v. FDA*, the same court followed *Dismukes* by deciding that the agency could determine the form in which records are made available under the FOIA.[269]

While federal courts have held that an agency may determine the form in which a record will be released under the FOIA, some state courts have shown more flexibility.[270] For example, in 1973 the New Hampshire Supreme Court held that a computer tape of field cards used to prepare property tax assessments was itself a public record.[271] Reasoning that the computer tape was as much a public record as the paper documents, the court held that a researcher seeking the assessment data was entitled to a copy of the tape made at his own expense.[272] In another state decision, a New York court concluded that

---

266. *Id.* at 762; *cf.* Timken Co. v. United States, 659 F. Supp. 239, 242 (Ct. Int'l Trade 1987) (holding that computer printouts of requested files were unresponsive to an FOIA request because the printed files were not as useful to the requester as the information on computer tape).

267. National Sec. Archives v. CIA, Civ. No. 88-119 (D.D.C. July 26, 1988).

268. *Id.*

269. Coalition for Alternatives in Nutrition & Health Care, Inc. v. FDA, No. 90 Civ. 1025 (D.D.C. Jan. 4, 1991). *See also* Hahn v. IRS, No. 90 Civ. 2782 (D.D.C. Jan. 10, 1992) (holding IRS need not provide records in form "comprehensible to a layperson"). *Cf.* Army Times Publishing Co. v. Department of the Army, 684 F. Supp. 720 (D.D.C. 1988) (holding Army required to provide computer tapes; however, issue was not format but existence of FOIA exemption).

270. For an example of a state court following the federal courts' holdings that agencies may determine the form of a response, see Seigle v. Barry, 422 So. 2d 63 (Fla. 4th DCA 1982), *rev. denied*, 431 So. 2d 988 (Fla. 1983).

271. Menge v. City of Manchester, 311 A.2d 116, 119 (N.H. 1973); *see also* Blaylock v. Staley, 732 S.W.2d 152, 153 (Ark. 1987) (suggesting, in dicta, that requester could obtain magnetic tape rather than paper copy if no undue burden on agency); *but see* Tax Data Corp. v. Hutt, 826 P. 2d 353 (Colo. Ct. App. 1991) (holding that paper printout constitutes reasonable access; no requirement that the agency allow requester "hands-on" use of computer terminal); Chapin v. Freedom of Info. Comm'n, 577 A.2d 300, 301 (Conn. App. Ct. 1990) (holding state law allows agency to provide only paper copy of requested information; need not provide computer disk).

272. *Menge*, 311 A.2d at 119.

the intent of a state public records law to provide maximum access could not be frustrated by the format in which information is provided.[273] The court held that a New York City agency must provide computer tapes of its records to a commercial publisher rather than printouts of the information.[274] The court reasoned that requiring the requester to search manually through more than a million pages of printouts undermined the principle of maximum access.[275] The court also noted that the cost of providing computer tapes was less than providing printouts.[276]

VI. COMPUTERS AND THE PRIVACY EQUATION

A. Privacy in Peril

The tension between personal privacy and government's need to gather and analyze personal information is long-standing. Governments have an interest in keeping complete, accurate information on individuals. This information allows them to spend tax revenues prudently and to check for fraud and waste by program beneficiaries. For example, finding welfare recipients who receive more than their share of benefits saves tax dollars and prevents cheaters from living well at the expense of the needy and the taxpayers.

The public, and particularly the media, have always had an interest in having access to records of government. Access to such records allows citizens to monitor their government and discourages clandestine abuses. The retention of massive files on such people as the Reverend Martin Luther King, Jr. is an example of the undesirable activity possible when government records are outside the public's reach.[277]

While the public has a right to know about the activities of government, individuals on whom the government keeps records also have an interest in preventing disclosure of embarrassing or sensitive information. Release of such information might harm reputations, cost jobs, or result in other forms of discrimination or sanctions. For example, disclosure that an individual is HIV positive, or actually has AIDS, might have such results.

Before computers dominated government record-keeping, the best protections for personal privacy were practical barriers. The expense

273. Brownstone Publishers, Inc. v. New York City Dep't of Bldgs., 560 N.Y.S.2d 642 (N.Y. App. Div. 1990).

274. *Id.* at 643.

275. *Id.*

276. *Id.*

277. DAVID GARROW, THE FBI AND MARTIN LUTHER KING, JR. (1981).

in gathering large numbers of paper records was often costly and time-consuming, and analysis of such material was tedious. Computers, however, have compressed the gathering and sorting functions and have made records, once tucked obscurely in file cabinets at distant locations, available with relative ease.[278] The U.S. Supreme Court has noted that such efficiency robs individuals of their "practical obscurity" and prevents them from putting past mistakes behind them and moving on to productive lives.[279]

The sheer volume of computer data available has eroded personal privacy by making more information about individuals available. Potentially damaging information, now stored more widely and kept longer, is available for use and misuse as never before. This information explosion is due partly to the drastic reduction of space needed for record-keeping. Computer storage media such as magnetic tapes and floppy disks can store what once took rows of file cabinets. This abundance of storage space has freed agencies to gather more and more information and to keep it longer. The ease of storing information at a lower cost has made it easier to keep records than to dispose of them. David F. Linowes, author of *Privacy in America*,[280] compares surplus information to atomic waste because scientists "have not yet given us the practical means for safely disposing of either."[281] As a result of the ease with which it can be stored, personal information is now often kept long after it has become outdated and inaccurate; as individuals go through life and their circumstances change, information often becomes obsolete or irrelevant.[282]

While the volume of personal information has increased dramatically, computers have made obtaining access to specific information much easier. Government agencies have developed computer programs that allow them to retrieve information quickly[283] without having to sift through indices or records. Frequently, information can be obtained with a few simple keystrokes at a computer terminal.

As faster computers are developed, searching files will only get easier. Computer searches that are now time-consuming and costly will become virtually instantaneous. Practical access will become easier and the threat to privacy potentially greater.

---

278. *See generally* DAVID F. LINOWES, PRIVACY IN AMERICA: IS YOUR PRIVATE LIFE IN THE PUBLIC EYE? (1989).

279. Justice Dep't v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 780 (1989).

280. LINOWES, *supra* note 278.

281. *Id.* at 14.

282. *Id.* at 12 (giving examples of problems created by obsolete or inaccurate data).

283. *See generally* FLORIDA'S INFORMATION POLICY, *supra* note 5, at 83-96.

Because of the ease of computer access and data sharing among numerous agencies, the de facto protection of "practical obscurity" has disappeared.[284] Individuals can no longer rely on the scattered, hard-to-find nature of information about themselves to create an expectation of privacy. Concerns about the erosion of privacy have led many commentators to raise the specter of George Orwell's "Big Brother" as more and more personal information finds its way into government computers.[285] Legislatures have responded to this concern with statutes designed to ensure personal privacy.

B. Federal Privacy Laws

1. The Privacy Act

The Privacy Act of 1974[286] was passed to regulate how government used personal information and was inspired by fears of "the impact of computer data banks on individual privacy"[287] that grew out of the debate over a proposal for a National Data Center to pool government information. The Privacy Act forbids disclosure of information without an individual's consent[288] and grants the individual access to all collected information.[289]

The Act also allows individuals to request that records about them be corrected if they contain inaccuracies.[290] If an agency denies a correction request, the individual can bring a civil action against the agency.[291] Courts then may order an agency to amend the individual's record.[292] The Privacy Act, however, contains several agency exemptions, including the Central Intelligence Agency, the Secret Service, and law enforcement agencies.[293]

Another exemption applies to information disclosed for "routine use" by a collecting agency.[294] Agencies have often cited this exception

284. *See* Justice Dep't v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 780 (1989).

285. *See* John Shattuck, *In the Shadow of 1984: National Identification Systems, Computer Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991 (1984); Toby Solomon, *Personal Privacy and the 1984 Syndrome*, 7 W. NEW ENG. L. REV. 753 (1985).

286. 5 U.S.C. § 552a (1988).

287. H.R. REP. No. 1416, 93rd Cong., 2d Sess. 7 (1974).

288. 5 U.S.C. § 552a(b).

289. *Id.* § 552a(d).

290. *Id.* § 552a(d)(2).

291. *Id.* § 552a(d)(3).

292. *Id.* § 552a(g)(2)(a).

293. *Id.* § 552a(j)(1), (j)(2), (k)(3).

294. *Id.* § 552a(b)(3).

to avoid the individual consent requirement by defining routine use expansively.[295] An agency might, for example, define routine use as release to academic researchers. One information technology expert said of the exemption: "You could drive a truck through it."[296]

Another problem with the Privacy Act is that it was enacted when government records were maintained primarily on paper.[297] New computer technologies allow agencies to store and manipulate data in ways not covered by the Act, effectively limiting the Act's protection.[298] Thus, the Privacy Act's attempt to protect informational privacy as "a personal and fundamental right protected by the Constitution"[299] has to some extent been undermined.

2. *The Freedom of Information Act*

Although the FOIA[300] establishes a "general philosophy of full agency disclosure"[301] to government records, the Act contains an exemption designed to protect individuals from unnecessary disclosure of personal information in government files.[302] That exemption allows agencies to withhold information in personnel, medical, and similar files when disclosure would constitute "a clearly unwarranted invasion of personal privacy."[303]

Because computer record compilations may contain summaries of widely scattered, hard-to-retrieve data, they may be exempt from disclosure under the exception. For example, in *Justice Department v. Reporters Committee for Freedom of the Press*,[304] an exemption for law enforcement records was held to apply to computerized summaries of arrest records.

C. *The Supreme Court and Informational Privacy*

Although a right of privacy is not explicitly mentioned in the *United States Constitution*, the U.S. Supreme Court has recognized a limited

---

295. Interview with Edwin Levine, Staff Director, Fla. Jt. Legis. Info. Tech'y Resource Comm. (Mar. 2, 1990) [hereinafter Levine Interview]; *see also* Todd Coles, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957, 959 (1991).

296. Levine Interview, *supra* note 295.

297. *See* FLORIDA'S INFORMATION POLICY, *supra* note 5, at 123.

298. *Id.* at 124.

299. Privacy Act of 1974, Pub. L. No. 93-579, § 2(a)(4), 88 Stat. 1897. *See also* H.R. REP. No. 1416, 93rd Cong., 1st Sess. 9 (1974).

300. 5 U.S.C. § 552 (1988).

301. S. REP. No. 813, 89th Cong., 1st Sess. 3 (1965).

302. 5 U.S.C. § 552(b)(6).

303. *Id.*

304. 489 U.S. 749 (1989).

right to private decision making. For example, the Court has held there is a constitutional right to privacy in the use of contraceptives[305] and in the decision to have an abortion.[306]

Those cases recognized a right to decisional privacy. Decisional privacy is the individual interest in making deeply personal decisions free from governmental interference.[307] Computer privacy cases, on the other hand, involve informational privacy. Informational privacy is the individual's interest in controlling the flow of information about him- or herself.[308] Because decisional privacy and informational privacy are distinct interests, decisional privacy cases do not necessarily provide guidance for informational privacy issues.

One of the first major opinions addressing informational privacy was the 1967 case of *Katz v. United States*.[309] In *Katz* the Court held that people have a reasonable expectation of privacy in their telephone conversations. The Court found that the Fourth Amendment's protection against unreasonable searches and seizures extended to intangible items such as Katz's phone conversation.[310] *Katz* demonstrated the Court's willingness to extend zones of privacy beyond the "persons, houses, papers and effects" explicitly mentioned in the Fourth Amendment.[311] However, the Court limited its holding to the conversation at issue and did not declare a generalized right to informational privacy.[312]

The Supreme Court did not address informational privacy again until 1976 in *Paul v. Davis*.[313] In *Paul* the Court refused to expand the right to privacy to prohibit a state from publicizing an arrest.[314] The plaintiff in that case had been included in a flyer listing "active shoplifters" that was distributed to local merchants by police.[315] Writing for the majority, Justice Rehnquist found no informational privacy right in the Constitution.[316] Justice Rehnquist pointed out that the Court's "right of privacy" cases had dealt with substantive restrictions on such activities as procreation and contraception.[317] "None of

305. *See* Griswold v. Connecticut, 381 U.S. 479 (1965); *see also* Eisenstadt v. Baird, 405 U.S. 438 (1972).
306. *See* Roe v. Wade, 410 U.S. 113 (1973).
307. *See id.* at 154-55.
308. Whalen v. Roe, 429 U.S. 589, 599 n.25 (1977).
309. 389 U.S. 347 (1967).
310. *Id.* at 353.
311. U.S. CONST. amend. IV.
312. *Katz*, 389 U.S. at 349-50.
313. 424 U.S. 693 (1976).
314. *Id.*
315. *Id.* at 694-95.
316. *Id.* at 713-14.
317. *Id.* at 713.

our substantive privacy decisions hold this or anything like this, and we decline to enlarge them in this manner," Rehnquist wrote.[318]

In *United States v. Miller*,[319] decided shortly after *Paul*, the Court again declined to declare a right of informational privacy. In *Miller* the issue was whether a subpoena of an individual's bank records violated the Fourth Amendment by intruding into a constitutionally protected zone of privacy.[320] Bank records, the Supreme Court held, did not carry a legitimate expectation of privacy. Justice Powell reasoned that since the records "contain only information voluntarily conveyed to the banks and exposed to their employees"[321] in the ordinary course of business, the owner forfeited any constitutional expectation of privacy in their contents.[322]

The Court did discuss an "individual interest in avoiding disclosure of personal matters" in the 1977 case of *Whalen v. Roe*.[323] In *Whalen* physicians and patients challenged a state statute creating a database of information on prescriptions issued for certain drugs.[324] The Court upheld the statute, but alluded to a privacy interest in preventing disclosure of personal matters.[325] However, the Court did not say when that interest might allow an individual to refuse to disclose information or to block access to records.[326] The assertion of a privacy interest stands alone in the opinion, and the Court did not clarify the nature of the privacy interest.

In another 1977 case, *Nixon v. Administrator of General Services*,[327] the Supreme Court alluded again to the existence of an informational privacy interest. In that case the Court was confronted with a constitutional privacy challenge to a statute allowing the Administrator of General Services to take control of the papers of former President Richard Nixon.[328] The *Nixon* Court acknowledged the existence of "the individual interest in avoiding disclosure of personal matters . . . ."[329] The Court, after considering Nixon's privacy inter-

318. *Id.*
319. 425 U.S. 435 (1976).
320. *Id.*
321. *Id.* at 442.
322. *Id.*
323. 429 U.S. 589, 599 (1977).
324. *Id.* at 593.
325. *Id.*
326. *See generally* Glenn C. Smith, *We've Got Your Number! (Is It Constitutional To Give It Out?): Caller Identification Technology and the Right to Informational Privacy*, 37 UCLA L. REV. 145, 172-75 (1989); Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133 (1991).
327. 433 U.S. 425 (1977).
328. *Id.*
329. *Id.* at 457.

est, concluded the statute was constitutional.[330] The *Nixon* Court declined to define the constitutional privacy interest. Moreover, as in *Whalen*, that interest was not part of the Court's holding.

In summary, the Court declined in *Paul* and *Miller* to recognize a right to informational privacy. Later, in *Whalen* and *Nixon*, while recognizing an informational privacy "interest," the Court did not define the extent of the protected interest. Taken together, these cases suggest there is as yet no firm constitutional right to informational privacy.

D. Access and Privacy Cases

The Supreme Court has been more expansive in recognizing privacy interests in access cases where the privacy interests are derived from statutory language. In *Department of the Air Force v. Rose*, for example, the Court held that information still could be exempt from disclosure under the FOIA even though it had once been public.[331] Summaries of disciplinary proceedings against Air Force cadets might still be exempt under the FOIA's exception for "clearly unwarranted" invasions of personal privacy[332] even though they had once been posted on Air Force Academy bulletin boards, the Court held. Justice Brennan wrote: "Despite the summaries' distribution within the Academy, many of this group with earlier access to summaries may never have identified a particular cadet, or may have wholly forgotten his encounter with Academy discipline. And the risk to the privacy interest of a former cadet . . . cannot be rejected as trivial."[333]

The Court also recognized a statutory privacy exemption in the 1989 case of *Justice Department v. Reporters Committee for Freedom of the Press*.[334] In *Reporters Committee*, members of the media sought criminal record compilations ("rap sheets") of an organized crime figure from the FBI's computer banks.[335]

Writing for the majority, Justice Stevens held that the rap sheets fell under FOIA exemption seven for law enforcement information constituting an "unwarranted invasion of privacy" and denied the disclosure request.[336] "[B]oth the common law and the literal under-

330. *Id.* at 465.
331. 425 U.S. 352 (1976).
332. 5 U.S.C. § 552(b)(6).
333. *Rose*, 425 U.S. at 380-81.
334. 489 U.S. 749 (1989).
335. *Id.* at 757.
336. *Id.* at 780. *See also* 5 U.S.C. § 552(b)(7).

standings of privacy encompass the individual's control of information concerning his or her person,"[337] Justice Stevens wrote. He buttressed his conclusion by citing *Whalen* and the Privacy Act.[338]

Justice Stevens distinguished computerized record summaries and the individual records the summaries contained:

> Recognition of [an informational] privacy interest supports the distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole. . . . Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.[339]

Justice Stevens acknowledged that all the crime figures' arrests were or may have been public records. He cited *Rose* for the proposition that individual privacy interests may not disappear just because information requested was once public.[340] "The substantial character of [an informational privacy] interest is affected by the fact that in today's society the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains the age of 80, when the FBI's rap sheets are discarded," Stevens wrote.[341]

Reporters Committee is a significant case on access and privacy in the computer age. Although the actual holding is based on the FOIA exemption for law enforcement records, the language that distinguishes individual records and computer compilations could easily apply in other contexts.

The FOIA law-enforcement exemption that Justice Stevens used to deny the disclosure request requires balancing the individual privacy interest in non-disclosure against the public interest in the release of the records.[342] In *Reporters Committee* the crime figure whose rap sheets were sought allegedly had ties to a corrupt congressman. The rap sheets might have shed light on the crime figure's dealings with the congressman, if any, or yielded other information of public interest. It is difficult, then, to see why the Supreme Court used *Reporters Committee* to declare that rap sheets were categorically exempt from disclosure.

---

337. *Reporters Committee*, 489 U.S. at 763.

338. *Id.* at 766-71 (citing Whalen v. Roe, 429 U.S. 589 (1977) and the Privacy Act, 5 U.S.C. § 552a (1988)).

339. *Id.* at 764.

340. *Id.* at 767-69.

341. *Id.* at 771.

342. *Id.* at 762.

Privacy advocates have reason to be concerned about the computerization of records. At the same time, however, access advocates have reason to be concerned about results like that in *Reporters Committee*. Courts may act reasonably to protect privacy, but they also may use computerization of records as a broad shibboleth to limit public record disclosure laws. Whether *Reporters Committee* fosters sensible treatment of computerized records or is used to thwart the FOIA's general policy of disclosure remains to be seen.

E. State Cases on Computer Access and Privacy

Because the Supreme Court has not declared a constitutional right to informational privacy, most general privacy law is left to the states. Some states have explicit constitutional provisions protecting a person's right to privacy.[343] Interpretations of these provisions vary. Many have been advanced in search-and-seizure cases, but some also have been invoked in informational privacy cases.

As in *Rose* and *Reporters Committee*, the privacy exemptions have been used in some states to decide computer privacy cases. An issue that most commonly arises in state computer cases is whether computer records pose a greater threat to privacy than other forms of records. Courts have reached mixed conclusions.

As early as 1972, shortly after commentaries warning about the threat of computerized records began to appear, the Colorado Supreme Court acknowledged the threat in *Davidson v. Dill*.[344] In *Davidson* a lower court dismissed the plaintiff's effort to expunge arrest records under a common-law invasion of privacy claim.[345]

In reversing the lower court, the court noted the impact of computers on privacy:

> Recent years have witnessed a substantial upsurge in the number of cases and commentaries dealing with the problem before this Court. In no small part, this phenomenon is due to the advent of the computer age—an event which has drastically increased the power of industry and government to collect data—and the growing concern for the individual's loss of privacy as a natural by-product of our modern technology.[346]

---

343. *See, e.g.*, ALASKA CONST. art. I, § 22; ARIZ. CONST. art. II, § 8; CAL. CONST. art. I, § 1; FLA. CONST. art. I, § 23; HAW. CONST. art I, § 6; ILL. CONST. art. I, § 6; LA. CONST. art. I, § 5; MONT. CONST. art. II, § 10.

344. 503 P.2d 157 (Colo. 1972).

345. *Id.* at 158.

346. *Id.*

The court also mentioned that arrest files were traded with other police data centers, including those of the FBI. After concluding that retention of the files could collide with the emerging right of privacy,[347] the court remanded the case.[348]

Davidson demonstrates that state courts have not waited for federal guidance in the treatment of computerized records. If anything, some state courts recognized the potential for privacy invasion created by computerization before Congress and the U.S. Supreme Court did.

In 1982 in *Kestenbaum v. Michigan State University*,[349] the Michigan Supreme Court held disclosure of a computerized record would constitute a "clearly unwarranted invasion of . . . privacy" under the Michigan counterpart to the federal FOIA.[350] The litigation in *Kestenbaum* began when a student brought suit to compel release of a duplicate computer tape containing the names and addresses of Michigan State University students.[351] The tape was used to produce the university's directory.[352]

The court rejected the disclosure request even though the names of the students ultimately would appear in the student directory. "Form, not just content, affects the nature of information," the court wrote. "Seemingly benign data in an intrusive form takes on quite different characteristics than if it were merely printed."[353] Students did not know when they registered "that an efficient and intrusive computer mailing system already was available to anyone for a nominal sum," the court said.[354]

In *Kestenbaum* the court might have been concerned that the computer tape would make it easy for the plaintiff to contact the students in bothersome ways. For example, it might have been used to automatically produce a mailing list.[355] But the opinion never explained how the computer tape would have been different from a copy of the student directory. On the facts, then, it seems a weak case for nondisclosure.

---

347. *Id.* at 160.

348. *Id.* After *Davidson*, the Colorado Legislature passed the Criminal Justice Records Act, which provided that records could be sealed and not reopened except by court order. COLO. REV. STAT. § 24-72-803 (1992). Thus the possibility of having records destroyed is no longer likely in Colorado. *Davidson* is discussed not for its result, but for its concern about computerized records.

349. 327 N.W.2d 783 (Mich. 1982).

350. *Id.* at 785.

351. *Id.* at 783.

352. *Id.*

353. *Id.* at 789.

354. *Id.* at 790.

355. Kestenbaum was the president of a registered student political organization. *Id.* at 783.

Two years later, the Michigan Court of Appeals denied a records request for a computer tape held by the Detroit police on the same grounds. In *Mullin v. Detroit Police Department* the plaintiff sought a computer tape containing the names and addresses of people involved in Detroit traffic accidents since 1980.[356] The information was in the public record in the form of 70,000 individual accident reports.[357]

The appeals court said "this case falls squarely within *Kestenbaum*" and held disclosure would be a "clearly unwarranted invasion of privacy."[358] The case was actually a stronger one for nondisclosure than *Kestenbaum*, the court reasoned, because the accident reports contained embarrassing facts such as the names of people arrested.[359] Thus, the appeals court adopted *Kestenbaum*'s distinction between the privacy implications of computerized and paper records.

Courts have also used privacy to block release of driver's license records. In the 1988 Massachusetts case of *Doe v. Registrar of Motor Vehicles*, an appeals court vacated a lower court decision allowing disclosure of such records.[360] The appeals court put the burden on the records custodian to show the information was not "personal data" under the state's Fair Information Practices Act.[361] The court stated:

> Even if the items here at issue are not considered "intimate details of highly personal nature," the aggregate effect on the privacy of the total number of people whose data are disseminated weighs against disclosure. . . . There is a negative public interest in placing the private affairs of so many individuals in computer banks available for public scrutiny.[362]

These cases demonstrate that some state courts have recognized that the volume of data and retrieval speed unique to computer records creates novel privacy problems. However, many courts have not followed this reasoning. Many courts have simply found that computer records are public records just as paper records and have allowed access to computer records to the same extent as paper.

In *Webb v. City of Shreveport* a Louisiana appeals court granted a request for a computer tape containing names and addresses of public

---

356. 348 N.W.2d 708, 710 (Mich. Ct. App. 1984).
357. *Id.* at 712.
358. *Id.*
359. *Id.*
360. 528 N.E.2d 880, 888-89 (Mass. App. Ct. 1988).
361. *Id.*
362. *Id.* at 886. For a decision barring disclosure of driver's license information on state constitutional invasion of privacy grounds, see Perkey v. Department of Motor Vehicles, 721 P.2d 50 (Cal. 1986).

employees in Shreveport.[363] The records were available as public records in other forms. Thus, there was no reasonable expectation of privacy in the names and addresses[364] that would violate the *Louisiana Constitution*'s privacy provision.[365] The court did not explicitly consider whether the computer tapes had a special privacy-invasive character.[366]

The New York case of *Szikszay v. Buelow* gave computer records similar treatment.[367] In *Szikszay* the plaintiff sought county computer tapes containing the names and addresses of the owners of each parcel of land in Cattaraugus County.[368] An Erie County court held the tapes were subject to disclosure under the New York Freedom of Information Law.[369] The court held there was no unwarranted invasion of privacy under the state records law and thus the records were public.[370] A distinction between computerized and paper records was explicitly rejected. "The form of the records and petitioner's purpose in seeking them do not alter their public character or petitioner's concomitant right to inspect and copy," the court wrote.[371]

A 1982 Kansas case also treated computerized records like those in any other form. In *State ex rel. Stephan v. Harder* the Kansas Supreme Court was asked to consider whether denial of access to abortion records was proper.[372] The records contained the names of physicians who were paid public funds to perform abortions.[373] The computer tapes were required to be maintained and kept by law as Kansas public records law provided,[374] and thus were public records, the court held.[375] The court also ruled that severing confidential portions of the records did not make them "new records" under the law because the record custodians were under an implied duty to delete the confidential information.[376] Finally, the court held that any privacy

363. 371 So. 2d 316, 317 (La. Ct. App. 1979).
364. *Id.* at 319.
365. "Every person shall be secure in his person, property, communications, houses, papers and effects against unreasonable searches, seizures or invasions of privacy." LA. CONST. art. I, § 5.
366. 371 So. 2d at 318.
367. 436 N.Y.S.2d 558 (N.Y. Sup. Ct. 1981).
368. *Id.* at 559.
369. *Id.* at 563.
370. *Id.* (quoting N.Y. PUB. OFF. LAW §§ 87 subd. 2(b), 89 subd. 2(b)(iii) (McKinney 1988)).
371. *Id.*
372. 641 P.2d 366 (Kan. 1982).
373. *Id.* at 368.
374. *Id.* (citing KAN. STAT. ANN. § 45-201 (1982)).
375. *Id.* at 372.
376. *Id.* at 374.

concerns were outweighed by the public's right to know about the workings of government.[377]

F. Privacy and Computer Access in Florida

Florida's public records law[378] is one of the broadest in the nation. It has possibly the strongest presumption favoring disclosure of government records of any state. The Florida Supreme Court has ruled that only "those records that are provided by statutory law to be confidential or which are expressly exempted by general or special law" are exempt from disclosure.[379] Generally, Florida courts have subordinated privacy interests to public access by giving the records act the broadest possible expression.[380]

Florida's constitution contains a provision specifically protecting individual privacy.[381] In 1980 Florida voters adopted a provision that reads: "Every natural person has the right to be let alone and free from governmental intrusion into his private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law."[382] On the strength of the last sentence, the Florida Supreme Court has held the privacy provision does not bar disclosure of public records.[383]

In 1980 the Florida Supreme Court decided a case that seemed to foreclose any implicit state or federal constitutional privacy interest that might prevent access to records. In *Shevin v. Byron, Harless, Schaffer, Reid & Associates, Inc.*, the court confronted a claim that papers prepared by a consultant assisting in a personnel search were not subject to disclosure on federal and state constitutional privacy grounds.[384] The *Shevin* court rejected these arguments, holding that the federal informational privacy interest was not sufficiently developed by the U.S. Supreme Court.[385] The Florida court also concluded that there was "no support in the language of any provision of the Florida Constitution or in the judicial decisions of this state" for a state informational privacy right to override access to records.[386]

---

377. *Id.* at 376.
378. *See* FLA. STAT. ch. 119 (1991).
379. Wait v. Florida Power & Light Co., 372 So. 2d. 420, 422 (Fla. 1979).
380. Lorei v. Smith, 464 So. 2d 1330 (Fla. 2d DCA), *rev. denied*, 475 So. 2d 695 (Fla. 1985).
381. FLA. CONST. art. I, § 23.
382. *Id.*
383. Forsberg v. Housing Auth. of Miami Beach, 455 So. 2d 373, 374 (Fla. 1984).
384. 379 So. 2d 633 (Fla. 1980).
385. *Id.* at 637-38.
386. *Id.* at 639.

However, in a 1992 non-computer case, the Florida Supreme Court suggested that there may be privacy interests of third parties that could limit access to records, at least in criminal discovery proceedings. The court in *Post Newsweek Stations v. Doe* affirmed a lower court ruling that barred an attempt by third parties to have the records disclosed.[387] The court, in dicta, did not rule out the possibility of closing public records generated in criminal discovery based on privacy concerns.[388]

VII. CONCLUSION

Computers present perhaps the greatest opportunity since the printing press to make vast quantities of information available to the average person. This information explosion includes records of government—records that allow citizens to actively supervise the performance of both elected officials and bureaucrats. Ironically, the very mechanism that could provide such enhanced access to information is in some cases being used to limit access.

Agencies that are required to provide access to their records have sometimes used the new technology to avoid disclosure. Agencies may not design systems with access in mind, only to claim later that information is unavailable because "our computer can't do that." Agencies have also frequently balked at providing information in the format most useful to the requester.

Judicial reaction to computerized records has been mixed. While some courts have held that computerized records are no less public records than those on paper, other courts, perhaps evincing some fear of the new technology, have reacted less favorably. For example, some courts have been reluctant to allow requesters to choose a particular format for receiving information, even if information in the desired form would be relatively simple for the agency to produce. Perhaps the greatest battle for those seeking access to computerized records is over requests that may be perceived to invade individual privacy. This issue, to which there are no easy answers, will likely continue to haunt access advocates.

However, many other issues are currently being debated in the courts and legislatures, including in the state of Florida. Many policies affecting computer records are likely to be adopted in the near future. For example, the Florida Bureau of Archives and Records Management, a division of the Department of State, recently adopted rules

387. 17 Fla. Law Weekly 715 (Fla. Nov. 25, 1992).
388. *Id.* at 717.

for public records that must be kept for more than ten years. The rules require that state agencies obtain computer systems that adequately provide public access to records and provide requesters with information in the form they choose, if it is available.[389] Agencies also are required to define the contents of their long-term computerized records and shall not ordinarily enter into a contract or obligation that "impairs the right of the public under state law to inspect or copy the agency's nonexempt public records."[390] The bureau has begun a rulemaking proceeding to consider access provisions for other computerized records.

In addition, a subcommittee of Florida's Growth Management Data Network Coordinating Council, established by the Office of the Governor to manage the sharing of computer data related to growth management among the state's agencies, has issued a report with several recommendations for access to computerized records.[391] The recommendations include amending the state's public records statute to require government agencies to design computer systems that facilitate access and creating a Public Records Council within the Department of State to address public access policy.[392] Even further, however, the Florida Legislature was considering in the spring of 1993 legislation that would allow government agencies to impose fees for copies of some computer records to subsidize the development and maintenance of sophisticated computer systems.

As a preliminary step toward framing the debate on computer-access ideas, the authors of this Article suggest a set of computer-access criteria. All the recommendations are based on the underlying assumption that access should not be restricted simply because records are in a computer. On the contrary, the principles that have guided federal and state access laws demand that government use the computer to enhance the people's right to know. The authors compiled the following thirteen recommendations after discussions with reporters, computer technicians, lawyers interested in freedom of information, legislative staff, and government records managers. Some of them parallel recommendations made by such organizations as the American Library Association[393] and the American Bar Association.[394] Many

389. FLA. ADMIN. CODE ANN. r. 1B-26.003(6)(f)(3) (1992).

390. *Id.*

391. OFFICE OF THE GOV., REPORT OF THE FINDINGS OF THE GROWTH MANAGEMENT DATA NETWORK COORDINATING COUNCIL'S SUBCOMMITTEE ON FLORIDA'S PUBLIC RECORDS LAW (Dec. 1992).

392. *Id.* at 53, 55-56.

393. Principles of Public Information Policy, 55 Fed. Reg. 12751 (1990).

394. AMERICAN BAR ASS'N, PUBLIC ACCESS TO GOVERNMENT ELECTRONIC INFORMATION UN-

of the ideas are based on current state and federal access laws. Some of the ideas, to the best of the authors' knowledge, are original.

The authors recommend:

1. Federal, state, and local governments must promote public access needs when agencies install or upgrade computer systems. Public access can be built into a system at the design stage at little additional cost. If public access is built into a system, records custodians cannot deny access based on the cost of reprogramming the computer. When public access is built in up front, access to computerized records is actually cheaper than searches for corresponding paper files.

2. All information in government-owned and operated computers is a public record, absent specific statutory exemptions. Defining the scope of public access should remain the prerogative of elected representatives after open discussion in the public arena. Access exemptions should not be declared ad hoc by government agencies or by the courts.

3. Any government agency that uses computerized records should make nonexempt information available to the public through user-friendly computer terminals. In the long run, providing access to the public records will be cheaper if self-service terminals are provided. Easy-to-follow instructions for public terminals should be available. Database security is a legitimate concern, but systems can be designed so the public can only read, and not alter, the information.

4. Government agencies using computerized records should make available to the public a catalog of nonexempt public information stored in computers. Effective organization and indexing required by such cataloging will increase agency efficiency as well as enhance public understanding of government.

5. Content-based exemptions for withholding computer records should be the same as for paper files. In general, information that was public record in paper files ought to be public record in computer files. The public policy issues do not substantially change. Any reasons for exempting computerized records based on content must be thoroughly documented and must not be based on unsubstantiated fears of technology.

6. Information in computers not specifically exempted by statute should not be withheld on the grounds that it is mixed with exempt

---

DER THE FREEDOM OF INFORMATION ACT (Feb. 1990); *see also* Sandra D. Scott, Computer Technology v. Laws on Access (unpublished paper, presented to the Association for Education in Journalism and Mass Communication annual convention, Boston, Mass., Aug. 1991); FLORIDA SOC'Y OF NEWSPAPER EDITORS, GUIDELINES FOR THE PROTECTION OF ACCESS TO COMPUTERIZED RECORDS, *reprinted in Guidelines Developed for Access to Government Computer Data*, BRECHNER REP. (Brechner Ctr. for Freedom of Info., Univ. of Fla.), Sept. 1992, at 4.

information. If public access is built into government computer systems, deleting exempt information is far easier using a properly designed computer than by reading and editing paper documents. Segregating materials by computer would save the government significant amounts of employee time.

7. Computerized information created or used by a government official as part of his or her official duties must be available to the public unless specifically exempted by statute. Only drafts of documents that are incomplete or not intended for dissemination should be exempt from disclosure.

8. Information in government computers cannot be withheld on the ground that the information is not available in paper form or because no official has used or seen the information. Producing a printed document from computer data or copying that information onto a magnetic tape is not "creating a record" in the sense the term is applied to paper records. The government was not expected to create paper documents to satisfy record requests because of the potential burden on agencies. However, information in a computer already exists as a government record. To deny public access to computerized information the government is using would create a vast new exemption to public records laws—an exemption that could subvert the very purpose of access laws.

9. Computer software made and used by government is a matter of public record. For example, the software that determines how income tax data are manipulated is as important as other records of tax-collecting agencies.

10. Agencies must release computerized information in the form requested when they are capable of doing so. Currently, many agencies give requesters paper printouts that are more expensive to produce than providing records on disk or magnetic tape. Requesters receiving paper records often have to input the data into digital form, a step that is unnecessary, time-consuming, and extremely costly. Government should facilitate the use of information, rather than frustrate it, whenever possible. Until the time comes when access is routinely built into government computers, agencies should, for example, copy data in their computers onto tapes or disks provided by the requesters, at cost. In addition, agencies should be encouraged to make computerized information available through remote access.

11. The public may only be charged the actual cost of reproducing government-held computerized information unless extensive employee and computer time is required. At no time should government charge more than the actual cost of materials, labor, and computer time.

12. Costs of government documents should not be a barrier to access, even when government records are provided by private information providers. Government needs to ensure that the costs of government records available only through commercial vendors are kept reasonable. The costs of government information available only through commercial vendors is already a problem, and will only get worse. The average citizen may be priced out of the information market if steps are not taken to prevent escalating costs.

13. Governments should ensure that all records are maintained in a form that can be accessed through available technology. Documents in archives may have to be transferred to a contemporary format if there is a risk that the technology required to read them could become obsolete. Governments are already reporting that documents in archives cannot be accessed because machines no longer exist to read them. This problem will grow with constantly changing computer technology.

Access to computerized information presents different problems than those associated with access to paper files. If would-be requesters do not begin to demand the same level of access to computer files they now have to paper files, hard-won privileges of access may vanish. Most of the protections listed above, in one form or another, need to find their way into access law.