

UIC John Marshall Journal of Information Technology & Privacy Law

Volume 5
Issue 1 *Computer/Law Journal - Summer 1984*

Article 3

Summer 1984

Fair Administration of the Freedom of Information Act After the Computer Revolution, 5 Computer L.J. 51 (1984)

John M. Graham

Follow this and additional works at: <https://repository.law.uic.edu/jitpl>



Part of the [Computer Law Commons](#), [Internet Law Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

John M. Graham, Fair Administration of the Freedom of Information Act After the Computer Revolution, 5 Computer L.J. 51 (1984)

<https://repository.law.uic.edu/jitpl/vol5/iss1/3>

This Comments is brought to you for free and open access by UIC Law Open Access Repository. It has been accepted for inclusion in UIC John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of UIC Law Open Access Repository. For more information, please contact repository@jmls.edu.

NOTES

FAIR ADMINISTRATION OF THE FREEDOM OF INFORMATION ACT AFTER THE COMPUTER REVOLUTION†

I. INTRODUCTION

We live in an information-dependent society. Such dependence is pervasive in the business as well as the political world. Before a responsible person makes a decision, he gathers all the information he can. This includes political decisions. The rights to vote and to speak out against the government cannot be effectively exercised without sufficient knowledge of relevant government operations.¹ Congress recognized this fact when it said that “[a] democratic society requires an informed, intelligent electorate, and the intelligence of the electorate varies as the quantity and quality of its information varies.”²

“[T]o permit access to official information long shielded unnecessarily from public view,”³ Congress enacted the Freedom of Information Act⁴ (FOIA or Act) in 1966. The FOIA requires federal agencies to make their records “promptly available to any person”⁵ unless the record is clearly exempted from disclosure by one of the nine carefully drawn exemptions.⁶ Taken together, the general pol-

† Awarded National First Place in the COMPUTER/LAW JOURNAL'S First Annual Computer Law Writing Contest.

1. See H.R. REP. NO. 1497, 89th Cong., 2d Sess. 2, 12, *reprinted in* 1966 U.S. CODE CONG. & AD. NEWS 2418, 2419, 2429.

2. *Id.* at 12, 1966 U.S. CODE CONG. & AD. NEWS at 2429.

3. *EPA v. Mink*, 410 U.S. 73, 79-80 (1973).

4. Pub. L. No. 89-487, 80 Stat. 250 (1966) (codified as amended at 5 U.S.C. § 552 (1982)). Congress felt the FOIA was needed to preclude “statutory excuse[s] for withholding Government records from public view.” H.R. REP. NO. 1497, *supra* note 1, at 3, 1966 U.S. CODE CONG. & AD. NEWS at 2420.

5. 5 U.S.C. § 552(a)(3) (1982).

6. 5 U.S.C. § 552(b)(1)-(9) (1982). In general, the exemptions cover areas in which a need for either governmental secrecy or personal privacy might arise.

icy of full disclosure and the nine exemptions represent a delicate balance between the public's need to know and the government's need to keep information confidential.⁷

Courts have generally weighted the balance in favor of disclosure by requiring that the exemptions be construed narrowly.⁸ They have concluded as well that courts may not exercise equitable discretion to justify governmental withholding of information where a proper agency record⁹ does not fit into one of the enumerated exemptions.¹⁰

Today, the computer threatens to shift this balance. Computers have been termed "information processors"¹¹ because they can efficiently store, search for, interpret, and retrieve vast amounts of information. Because computers have revolutionized the way that information is processed, they will certainly affect the application of laws that deal with the dissemination of information. Congress, however, did not consider the revolutionary effect of computers on information gathering, storage, retrieval, and dissemination when it formulated the FOIA.¹²

7. H.R. REP. NO. 1497, *supra* note 1, at 6, 1966 U.S. CODE CONG. & AD. NEWS at 2423.

8. *See, e.g.*, Department of the Air Force v. Rose, 425 U.S. 352, 361 (1976); Vaughn v. Rosen, 484 F.2d 820, 823 (D.C. Cir. 1973), *cert. denied*, 415 U.S. 977 (1973).

9. The Act requires disclosure only of "agency records." 5 U.S.C. § 552(a). The definition of an agency record, which is not present in the Act, has been manipulated by agencies to justify withholding material not otherwise exempt. *See, e.g.*, SDC Dev. Corp. v. Matthews, 542 F.2d 1116 (9th Cir. 1976), where the plaintiff requested medical records already available to the public, but at a fee that included the high costs of development and maintenance of the medical records system. Had the FOIA required release, the requester would have had to pay only the nominal costs of searching for and copying the records. Effectively, this would have shut down the record system in question, since it was maintained only because of the fees charged. The court held that the records were not agency records within the meaning of the Act. The court based its rationale on two points. First, the records did not reflect the structure, operation, or decision-making functions of the agency. *Id.* at 1119. Second, Congress had specifically authorized the agency to charge fees that represented the costs of development and maintenance. *Id.* at 1120. For a general discussion of what a record is, see Note, "Agency Records" Under the Freedom of Information Act: An Analysis of *Forsham v. Califano*, 13 GA. L. REV. 1040 (1979) [hereinafter cited as *Agency Records*]; Note, *What is a Record? Two Approaches to the Freedom of Information Act's Threshold Requirement*, 1978 B.Y.U.L. REV. 408 [hereinafter cited as *What is a Record?*].

10. *See, e.g.*, Soucie v. David, 448 F.2d 1067 (D.C. Cir. 1971). Most courts and commentators agree that the power of equitable discretion, or balancing the equities, is forbidden by the language of the FOIA. *But see What is a Record?*, *supra* note 9, at 427-33 (discusses equitable discretion).

11. *See, e.g.*, D. BENDER, COMPUTER LAW: EVIDENCE AND PROCEDURE § 3.01, at 3-2 n.3 (1982).

12. The only reference to computers found in the legislative history of the FOIA

This Note will explore the affect computers may have on the application of the Freedom of Information Act and suggest amendments to the Act that take into account the full power of information processors. It will begin by examining the structure and application of the Act, focusing on the areas relevant to computer stored records. It will then discuss the case of *Yeager v. DEA*,¹³ the only federal case to date that discusses fully how computers fit into the Act despite declining to require the use of computer power to expand the release of information pursuant to the FOIA. Thereafter, the Note discusses other areas in which computers may affect the FOIA's application.

As computers become more and more prevalent, and as lawyers become more familiar with their uses, FOIA lawsuits will contain arguments based on computer related issues. While no single conclusion can be drawn about the overall effect the computer will have, Congress and the courts must be constantly aware of the rapidly changing impact of computers and adapt the FOIA and its application accordingly.

II. THE STRUCTURE OF THE FREEDOM OF INFORMATION ACT

The Freedom of Information Act created a balance between the public's right to know and the need for maintenance of confidentiality. Section 552(a) declares a broad policy of disclosure, while section 552(b) clearly delineates areas where the need for secrecy is deemed paramount. Three types of government information are made available to the public through section (a): (1) information relating to agency organization and procedure,¹⁴ (2) final opinions and statements of agency policy,¹⁵ and (3) any "agency records" for which a proper request has been made.¹⁶ It is this third category—

was in the Senate report that accompanied the 1974 amendments to the FOIA. The report considered the problem of search and copy fees for records stored on a computer, and required agencies to perform computerized searches that were "functionally analogous to [manual] searches." S. REP. NO. 854, 93d Cong., 2d Sess. 12 (1974).

13. 678 F.2d 315 (D.C. Cir. 1982).

14. 5 U.S.C. § 552(a)(1) (1982). This section requires that such information be published in the Federal Register.

15. 5 U.S.C. § 552(a)(2) (1982). This section requires that such information be available for public inspection and copying, and that identifying information about the available records be manually indexed to facilitate research on such records.

16. 5 U.S.C. § 552(a)(3) (1982). This section states:

Except with respect to the records 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

which lacks the clear boundaries of the first two—that has been at the center of most FOIA litigation.

The Act provides that if an agency record does not fall into one of the exemptions, it must be disclosed to any person¹⁷ properly requesting it.¹⁸ The threshold inquiry therefore concerns the definition of the terms “record” and “agency record.” The Act defines neither of these terms. Thus, an agency that convinces a court to use a definition that does not include the information requested can effectively justify withholding information.¹⁹

In *Nichols v. United States*,²⁰ the court looked to a dictionary definition in ruling that a record is “that which is written or transcribed to perpetuate knowledge.”²¹ Accordingly, there is a notion that anything that cannot be copied is not a record. In *Nichols*, for example, certain physical objects associated with the shooting of the late President Kennedy were not available through the Act.²² There

published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.

Id.

17. Rather than make information available only to persons properly and directly concerned with the information, the FOIA avoids any “need” test by making information generally available “to the public.” 5 U.S.C. § 552(a) (1982). See *EPA v. Mink*, 410 U.S. 73, 79 (1973).

18. A proper request must “reasonably describe the records.” 5 U.S.C. § 552(a)(3)(A) (1982). A reasonable description is one that would enable a professional employee familiar with the requested information to find the records. H.R. REP. NO. 876, 93d Cong., 2d Sess. 6 (1974), reprinted in 1974 U.S. CODE CONG. & AD. NEWS 6267, 6271. See J. O'REILLY, FEDERAL INFORMATION DISCLOSURE § 9.03 (1983 Supp.).

19. See, e.g., *Forsham v. Harris*, 445 U.S. 169 (1980) (records generated, owned, and possessed by a federal grantee are not agency records unless the grantor exercised day-to-day control over production of the records or had exercised its right to obtain custody of the records); *SDC Dev. Corp. v. Matthews*, 542 F.2d 1116 (9th Cir. 1976) (medical records that were available for sale at a price including substantial development fees are not FOIA records (nor agency records) and thus are not available to the public for the nominal search and copy fees guaranteed by the FOIA). See *supra* note 9 for a more complete description of this case. See also *Nichols v. United States*, 325 F. Supp. 130 (D. Kan. 1971) (gun and articles of clothing used in a murder were not records), *aff'd on other grounds*, 460 F.2d 671 (10th Cir. 1972), *cert. denied*, 409 U.S. 966 (1972).

20. 325 F. Supp. 130 (D. Kan., 1971), *aff'd on other grounds*, 460 F.2d 671 (10th Cir. 1972), *cert. denied*, 409 U.S. 966 (1972).

21. 325 F. Supp. at 135 (quoting Webster's New Collegiate Dictionary). See also Attorney General's Memorandum on the Public Information Section of the Administrative Procedure Act, reprinted in 20 AD. L. REV. 263 (1967) (stating that the search and duplication required in 5 U.S.C. § 552(a)(4) take “objects or articles such as structures, furniture, paintings, sculpture, three-dimensional models, vehicles, equipment, etc. . . .” out of the definition of records).

22. 325 F. Supp. at 135.

seems to be no doubt, however, that records stored by a computer are available through the Act,²³ although a question remains as to the form in which the information is to be distributed.

It is important to note that the Act distinguishes between mere information and information contained in a record. A requester must describe the record sought in a reasonable fashion.²⁴ Unless the information desired is contained in records that can be described clearly, a request may not be granted. In *Krohn v. Department of Justice*,²⁵ the plaintiff requested particular information about every case decided in certain federal courts pursuant to a certain rule. The court held that he had not made a proper request, because the information requested was not indexed, but appeared in many different places in some of the appropriate files.²⁶ The court concluded that the plaintiff had made a vague request for data, rather than a specific one for records.²⁷ Another court has held, however, that a request for information known to be contained in a particular portion of each of a series of records adequately described those records.²⁸

The definition of "agency record" also serves to complicate matters. A record must be sufficiently related to an agency in order for it to be subject to disclosure under the Act.²⁹ The Supreme Court has generally used property law notions to determine whether such a relationship exists between the record and the agency.³⁰ Thus, for a record to be an "agency record," the agency must either have actual possession of the record,³¹ or have exercised day-to-day control over its production.³² Mere supervision of the activities of a federal

23. *Long v. IRS*, 596 F.2d 362, 364-65 (9th Cir. 1979), *cert. denied*, 446 U.S. 917 (1980) (the term "records" includes computer tapes); *Yeager v. DEA*, 678 F.2d 315, 321 (D.C. Cir. 1982) (computer-stored records, no matter what the media, are still records within the ambit of the Act).

24. 5 U.S.C. § 552(a)(3) (1982).

25. 628 F.2d 195 (D.C. Cir. 1980).

26. *Id.* at 197-98.

27. *Id.* at 198. See also *Electronic Memories & Magnetics Corp. v. United States*, 431 F. Supp. 356 (C.D. Cal. 1977); *What is a Record?*, *supra* note 9, at 417 n.47.

28. *Disabled Officer's Ass'n v. Rumsfeld*, 428 F. Supp. 454, 456-57 (D.D.C. 1977), *aff'd*, 574 F.2d 636 (D.C. Cir. 1978).

29. 5 U.S.C. § 552(a) (1982).

30. *Forsham v. Harris*, 445 U.S. 169 (1979); *Kissinger v. Reporters Comm. for Freedom of the Press*, 445 U.S. 136 (1979) (records of which the agency no longer had custody were properly withheld).

31. *Forsham v. Harris*, 445 U.S. 169, 181 (1979). *But see* *Goland v. CIA*, 607 F.2d 339 (D.C. Cir. 1978) (congressional transcript marked "secret" given to the CIA for limited reference purposes is not an agency record even while in custody of the agency), *cert. denied*, 445 U.S. 927 (1980).

32. *Forsham v. Harris*, 445 U.S. 169, 182 (1979).

grantee, including on-site visits and review of periodic reports, is not enough of a relationship to the data generated, owned, and possessed by a private organization.³³ This is true even when federal policy is influenced by reports based on the raw data requested, and when the agency has an unexercised right to review or obtain permanent custody of the raw data.³⁴

Once information has been properly classified as an agency record, only one of the nine exemptions may justify nondisclosure. Although each of the nine exemptions may be affected in some general way by the use of computer stored records, only five will be discussed in detail.³⁵

Exemption 2 protects matters that are "related solely to the internal personnel rules and practices of an agency."³⁶ These matters have generally been defined as those that are trivial and could generate no legitimate outside interest,³⁷ such as rules governing use of parking facilities or statements of policy as to sick leave.³⁸ The Supreme Court has held that exemption 2 permits agencies to withhold "matters of some public interest . . . only when necessary to prevent the circumvention of agency regulations that might result from disclosure to the subjects of regulation of the procedural manuals and guidelines used by the agency in discharge of its regulatory function."³⁹ While computer programs clearly constitute records under the Act, one agency has tried to protect the codebook and data storage format under this exemption,⁴⁰ both of which are necessary to access information released in computerized form.

Exemption 4 protects "trade secrets and commercial or financial information obtained from a person and privileged or confidential."⁴¹ Such information is protected if it is the type of information not customarily disclosed to the public, and its disclosure would either impair the government's ability to gather necessary information or

33. *Id.* at 171.

34. *Id.*

35. The exemptions not discussed are 5 U.S.C. §§ 552(b)(1) (1982) (national security information), (b)(3) (information protected from disclosure by other statutes), (b)(8) (information related to financial institutions), and (b)(9) (geological and geophysical information).

36. 5 U.S.C. § 552(b)(2) (1982).

37. *See, e.g.*, Department of the Air Force v. Rose, 425 U.S. 352, 367 (1976) (records of disciplinary actions at the Air Force Academy did have "substantial potential for public interest outside the Government").

38. S. REP. NO. 813, 89th Cong., 1st Sess. 6 (1965).

39. Department of the Air Force v. Rose, 425 U.S. 332, 364 (1976).

40. Yeager v. DEA, 678 F.2d 315, 318 (D.C. Cir. 1982). *See infra* notes 132 and 135 and accompanying text.

41. 5 U.S.C. § 552(b)(4) (1982).

cause substantial harm to the competitive position of the person from whom the information was obtained.⁴² The exemption therefore excludes from disclosure such items as "business sales statistics, inventories, customer lists, scientific or manufacturing processes or developments, and negotiation positions or requirements in the case of labor-management mediations."⁴³ Exemption 4 could be used to protect a confidential computer program⁴⁴ that the government bought under a secrecy agreement. Since the exemption does not protect government-generated trade secrets, another exemption must be used to protect programs written by an agency.

Exemption 5⁴⁵ protects inter-agency or intra-agency memoranda or letters that would not be available through discovery to a party in litigation against that agency. The Supreme Court has held that, to meet the first criterion, the record must not affect individual rights or require particular actions or forbearance by a member of the public.⁴⁶ To meet the second criterion, the record must be privileged from civil discovery.⁴⁷ Not all such privileges have been incorporated into exemption 5, however. The Court recognized that if exemption 5 incorporated every civil discovery privilege, it could become the grounds for withholding more information than Congress intended. Therefore, the Court held that only those privileges mentioned in the legislative history should be incorporated into exemption 5.⁴⁸

In civil litigation, only an executive privilege for predecisional deliberations and a privilege for an attorney's work product had been recognized prior to 1979.⁴⁹ In *Federal Open Market Comm. v. Merrill*, the Court held that a qualified privilege for trade secrets and other confidential commercial information should be incorporated into exemption 5.⁵⁰ The Court relied on the House Report,

42. See, e.g., *Pacific Architects & Eng'r, Inc. v. Renegotiation Bd.*, 505 F.2d 383, 384 (D.C. Cir. 1974).

43. H.R. REP. NO. 1497, *supra* note 1, at 9, 1966 U.S. CODE CONG. & AD. NEWS at 2427.

44. Authors of valuable computer programs, may, under proper circumstances, consider their programs trade secrets to prevent their being copied. Patent protection is often unavailable to computer programs, and copyright protection, though available, is limited at best. See generally D. REMER, LEGAL CARE FOR YOUR SOFTWARE 5-9 (1982).

45. 5 U.S.C. § 552(b)(5) (1982).

46. *Federal Open Market Comm. v. Merrill*, 443 U.S. 340, 352-53 (1979).

47. *Id.*

48. *Id.* at 354-55. *But see id.* at 366 n.2 (Stevens, J., dissenting).

49. *Id.* at 353.

50. *Id.* at 357-60. The privilege is based on FED. R. CIV. P. 26(c)(7), which provides that "for good cause shown . . . a trade secret or other confidential research,

which stated that "a Government agency cannot always operate effectively if it is required to disclose documents or information which it has received or generated before it completes the process of awarding a contract."⁵¹ The privilege is qualified in that the agency must show an actual and present need to protect the information.⁵² The information sought to be protected in *Merrill* consisted of directives setting out the guidelines by which the federal government would participate in the open securities market for the coming month. The government's purpose in participating in the securities market was to help control the nation's money supply. Any premature announcement of a particular month's policy would have severely hampered that effort.⁵³ Thus, the court held that the directives were protected for the month in which they were in effect, but no longer.⁵⁴

One commentator has suggested that *Merrill* opens the way for agencies to protect scientific and technical information, since a need for such protection can be shown.⁵⁵ Presumably, such information would include computer programs. The commentator suggests that the government needs to recoup some of its high development costs through the sale of new technology, especially to foreign markets.⁵⁶ The government could not sell equipment at a price that included research and development costs if the blueprints for the equipment were made available to the public⁵⁷ at a nominal cost for searching and copying. So long as the government intends to sell a high technology item, exemption 5 should protect applicable technical information from disclosure.⁵⁸

Exemptions 6 and 7 protect individual privacy and continuing investigations. Exemption 6 covers all information that would, because of its personal nature, lead to a "clearly unwarranted invasion

development, or commercial information [need] not be disclosed or [need] be disclosed only in a designated way."

51. H.R. REP. NO. 1497, *supra* note 1, at 10, 1966 U.S. CODE CONG. & AD. NEWS at 2427. The Court felt that, although the support in the legislative history was not as clear for this privilege as for the other two, it was clear enough. 443 U.S. at 359.

52. 443 U.S. at 362-64.

53. *Id.* at 348-49. The court noted that "[o]pen market operations are the most important monetary policy instrument of the Federal Reserve System." *Id.*

54. *Id.* at 363-64.

55. Belazis, *The Government's Commercial Information Privilege: Technical Information and the FOIA's Exemption 5*, 33 AD. L. REV. 415 (1981).

56. *Id.* at 416-17.

57. Since the Act, 5 U.S.C. § 552(a)(3) (1982), requires disclosure to "any person," even foreign competitors in the high technology market would have access to government technical data.

58. Belazis, *supra* note 55, at 424.

of personal privacy.”⁵⁹ This includes both information that identifies a person directly (“hardcore identifiers” such as name, address, and social security number) and information that could be used to identify a person in an indirect manner (“softcore identifiers” such as occupation and geographical location). Exemption 7 covers all information that could jeopardize the government’s ability to enforce the laws of the United States.⁶⁰

Finally, the Act requires that “[a]ny reasonably segregable portion of a record shall be provided to any person . . . after deletion of the portions that are exempt under [section b].”⁶¹ The courts have determined that the high cost of segregation does not necessarily make such segregation unreasonable.⁶² The standard to be applied is whether the nonexempt material, after deletion, still conveys meaningful and nonmisleading information.⁶³ Thus, a request for redaction will generally be granted unless the nonexempt material constitutes very little of the document or is inseparably intertwined with exempt information.

III. YEAGER v. DEA

In *Yeager v. DEA*,⁶⁴ the plaintiff wanted the Drug Enforcement Administration (DEA) to use its computer power to manipulate the

59. 5 U.S.C. § 552(b)(6) (1982) protects “personnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.”

60. 5 U.S.C. § 552(b)(7) (1982) protects:

investigatory records compiled for law enforcement purposes, but only to the extent that the production of such records would (A) interfere with enforcement proceedings, (B) deprive a person of a right to a fair trial or an impartial adjudication, (C) constitute an unwarranted invasion of personal privacy, (D) disclose the identity of a confidential source and, in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, confidential information furnished only by the confidential source, (E) disclose investigative techniques and procedures, or (F) endanger the life or physical safety of law enforcement personnel.

This includes enforcement of all kinds of laws, labor and securities as well as criminal. H.R. REP. NO. 1497, *supra* note 1, at 9, 1966 U.S. CODE CONG. & AD. NEWS at 2428.

Exemption 7(C) covers an area similar to exemption 6, but the word “clearly” is eliminated from “unwarranted invasion of privacy.” Personal privacy is apparently considered more important when a criminal investigation is going on than when one is not.

61. 5 U.S.C. § 552(b) (1982).

62. *See Long v. IRS*, 596 F.2d 362, 367 (9th Cir. 1979) (court declines to reach issue of whether cost of segregation can be unreasonable as a matter of law, because the cost was not unreasonable in the instant case), *cert. denied*, 446 U.S. 917 (1980).

63. *Yeager v. DEA*, 678 F.2d 315, 322 (D.C. Cir. 1982).

64. 678 F.2d 315 (D.C. Cir. 1982).

requested records in such a way as to allow disclosure of clearly exempt data. This manipulation would not have been feasible if the data were stored manually.⁶⁵

Yeager requested that the DEA release to him the entire Narcotics And Dangerous Drugs Information System (NADDIS). NADDIS is a sophisticated computer data base program that processes vast amounts of information gathered by the DEA's agents, informants, and witnesses. Each NADDIS record contains standard information fields, which are filled in as information becomes available. These fields include the name, address, occupation, race, and sex of a suspect.⁶⁶ There is also a general "remarks" field for information that either supplements the other fields or does not fit into any one of them. Each field is labeled as either a hardcore identifier or a softcore identifier.⁶⁷

The DEA asserted that the information contained in NADDIS fell under exemption 7 because dissemination might jeopardize continuing investigations, and that the material could not be redacted reasonably.⁶⁸ Yeager agreed, but claimed that the DEA had a duty to use its computing power to make the information nonexempt. Yeager conceded that all the hardcore identifiers as well as the remarks field were exempt, but he still wanted release of certain softcore information.⁶⁹

Yeager wanted the DEA to use computer "disclosure-avoidance techniques" so that useful information could be released to him while confidentiality was maintained.⁷⁰ Disclosure-avoidance techniques were designed so that information could be released, but the danger of the information being traced back to any individual would be reduced. A common example of this technique is known as "compacting," or "collapsing." It involves putting specific information into more general, statistical categories.⁷¹ Thus, instead of list-

65. At the time the case was decided, the computer system in question contained over 1 million records, with more records being added at a rate of about 3,500 per week. 678 F.2d at 321 n.13. While it might be possible to redact that many records manually, it is difficult even to imagine manually manipulating that many records in any sophisticated manner. This may be why Congress provided mere segregation as "full protection for the purposes to be served by the exemption." S. REP. NO. 854, *supra* note 12, at 32.

66. 678 F.2d at 322 n.15.

67. *Id.*

68. *Id.* at 319-20.

69. *Id.* at 322.

70. *Id.* at 319.

71. The time required to compact data manually would be astronomical when applied to the number of records kept by most government agencies. It is possible that for this reason no one has ever made such a request of a manual system.

ing all the individual files of those who have been suspected of dealing in heroin, the released record may say only that ten individuals, living in the midwest, who are between the ages of twenty and forty, were suspected of drug dealings. In contrast, segregation would release exact copies of the individual files with all exempt data deleted.

The *Yeager* court held that agencies which store their records in computers do not have a greater duty to segregate than agencies employing manual systems.⁷² However, the court did suggest that the use of computers might be relevant in measuring the burden.⁷³ In coming to this conclusion, the court considered Yeager's assertion that a process such as compacting, which would release data from otherwise exempt records, was similar enough to segregation to be required by the Act, on the grounds that it would "delete" the quality that made the information exempt.⁷⁴ The court also considered the rule that an agency is not required to create records it does not have or to write explanatory memoranda to be released along with proper agency records.⁷⁵

The court concluded that compacting information is not deletion for purposes of the Act, and that asking an agency to compact information does not constitute asking that agency to create a new record.⁷⁶ Compacting changes only the form in which information exists.⁷⁷ The court held that, since changing the form of a record is not the same as redaction, the DEA was not required to use its computers to compact the data into a releasable form.⁷⁸

Although the court reached a correct result, its reasoning is flawed. The court correctly reasoned that compacting information is not redaction and therefore is not required by the Act, but it confused the issue by comparing a computer record system with a manual one. The court implied that since compaction is virtually impossible on a manual system of records it is not required on a computer system either. This reasoning leads to the conclusion that anything that would not be possible on a manual record system should not be required on a computer record system.

This conclusion may lead to unfortunate results in some instances. An agency may be required to perform a search that could

72. 678 F.2d at 322-33.

73. *Id.* at 322 n.17.

74. *Id.* at 322.

75. *Id.* at 321 (citing *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132 (1975)).

76. 678 F.2d at 321.

77. *Id.*

78. *Id.* at 323. The Act specifically requires only "deletion of the [exempt] portions of otherwise releasable records." 5 U.S.C. § 552(b) (1982) (emphasis added).

not be performed manually because the Act did not select a particular type of search. The Act does, however, select a special type of disclosure-avoidance technique—segregation—and thus the proper reason why compacting is not required of an agency that stores its records in a computer is that compaction is an alternate form of disclosure-avoidance technique.⁷⁹

The court also erred in holding that compaction does not require an agency to do more than change the form of its records.⁸⁰ If a record is to be distinguished from information in the abstract, that record must consist of not only the information it contains, but also the format of that information. Thus, the court's view would be correct only if the Act dealt with mere information. Compaction in that case would change only the form of that information by segregating the exempt knowledge. Compacting a record, however, actually changes the nature of that record, creating a new record that the agency did not choose to retain. Redaction, on the other hand, retains both nonexempt data and the format of the record in question. Its main purpose is to allow release of nonexempt portions of records that happened to be stored in the same record as exempt data.⁸¹

The *Yeager* case also examined other issues related to computer-stored data. The first issue involved technical information related to the NADDIS system files. Such information included the codebook⁸² and data storage formats⁸³ which *Yeager* would have needed to read the records had they been released on magnetic computer tape. The DEA argued that the codebook and data storage format related solely to the internal procedures of the agency and were thus covered by exemption 2. The district court held that any information necessary to obtain access to released records related to more than internal agency procedures.⁸⁴ The Ninth Circuit refused to rule on the issue. It felt that since the codebook and data storage

79. Another example of computer systems being treated differently from manual systems is the amounts charged for searching and copying. Some agencies charge for computer and programmer time. *See, e.g.*, 5 C.F.R. § 294.107 (Department of Agriculture charges \$5-\$9 an hour to perform a manual search but charges \$17 an hour for programming a computerized search; on top of this, computer time itself is billed at \$219.00 per quarter hour).

80. Recall that "[a] requester must take agency records as he finds them." *Yeager*, 678 F.2d at 323; *accord* *Marks v. Department of Justice*, 578 F.2d 261, 263 (D.C. Cir. 1978).

81. *Vaughn v. Rosen*, 484 F.2d 820, 825 (D.C. Cir. 1973), *cert. denied*, 415 U.S. 977 (1973).

82. *See infra* note 135 and accompanying text.

83. *See infra* note 132.

84. 678 F.2d at 318 (citing unpublished lower court opinion).

format information need be provided only with records released on magnetic tape, the question of the form of release had to be answered first.⁸⁵

Another issue raised in the DEA's argument is that a request for an entire record system does not reasonably describe the records requested because it is overbroad.⁸⁶ This issue is especially important in computer record systems because the computer has the power to rapidly manipulate a record system as large as NAD-DIS. Requesters may find it simpler to request an entire record system rather than to narrow their requests. In this way, they can search for desired records themselves rather than leave it to the possibly hostile agency. Prior to the *Yeager* opinion, at least one commentator felt that a request for an entire system would be deemed overbroad.⁸⁷ The *Yeager* court, however, relying on legislative history, found that a request is reasonable so long as the agency knows precisely which records have been requested.⁸⁸ This standard is consistent not only with the Act's policy of full disclosure, but also with the notion that one does not have to show a need when requesting records.⁸⁹ Any other standard of reasonableness would probably require some inquiry into the requester's purpose for seeking each record. This would create a judicial exemption for records that would otherwise have been disclosed.

The *Yeager* case is probably only the first in a series of attempts to adapt the FOIA to the computer revolution. The remainder of this Note will analyze areas where the computer will most likely affect the administration of the Act. In some areas, only Congress can deal with this impact adequately. It is up to the courts, however, to administer the present FOIA fairly in light of the computer revolution.

IV. ADAPTING THE FOIA TO COMPUTER SYSTEMS

The *Yeager* court concluded that the Freedom of Information Act in its present form did not require the use of disclosure-avoidance techniques, even though their use would have permitted the release of information otherwise unobtainable.⁹⁰ It noted also, however, that "[a]s agencies begin keeping more of their records in

85. *Id.* at 326.

86. *Id.* See 5 U.S.C. § 552(a)(3) (1982).

87. J. O'REILLY, *supra* note 18, at § 9.03.

88. 678 F.2d at 326, referring to S. REP. NO. 854, *supra* note 12, at 10 and H.R. REP. NO. 876, *supra* note 51, at 5-6, 1974 U.S. CODE CONG. & AD. NEWS at 6267.

89. See *supra* note 17.

90. 678 F.2d at 323.

computerized form, the need to contour the provisions of FOIA to the computer will become increasingly necessary and more dramatic.'⁹¹ This section will discuss areas of the FOIA that may need amendment in the next few years and will suggest possible adaptations to the computer revolution.

A. USE OF DISCLOSURE-AVOIDANCE TECHNIQUES

The FOIA requires an agency to release only those records it has chosen to retain or is required by law to retain.⁹² An agency need not change the form of a record even when doing so would make exempt information nonexempt.⁹³ Congress determined that segregation would be the sole method of dealing with exempt records.⁹⁴ Yet, if an agency were required to change the form of a record, more information would be disclosed. Such a requirement would be consonant with the congressional policy of maximum disclosure. As the amount of information released to the public is increased, however, the possibility that a sensitive item of information will be disclosed is increased also.⁹⁵

Sensitive disclosure takes place when three things occur. First, a person looking at the released information is able to identify the source of that information. Second, that person learns something new from the released information. Third, that new information should have been protected under an FOIA exemption.⁹⁶ A sensitive item may be disclosed even if the value of that item cannot be exactly determined.⁹⁷ It is necessary only that the item can be determined more precisely as the result of release.⁹⁸

Disclosure-avoidance techniques are used to reduce the possibility of sensitive disclosure. Segregation is one of the simplest examples. A disclosure-avoidance technique is subject to two kinds of errors. After its application, the information released may still dis-

91. *Id.* at 327 (quoting unpublished lower court opinion).

92. *Borom v. Crawford*, 651 F.2d 500, 502 (7th Cir. 1981).

93. *Yeager*, 678 F.2d at 322. The agency must, of course, edit out exempt data from records containing otherwise releasable information.

94. S. REP. NO. 854, *supra* note 12, at 32.

95. For the purposes of this Note, a "sensitive item" is information that could be legally withheld under one of the FOIA's exemptions.

96. OFFICE OF FED. STATISTICAL POLICY AND STANDARDS, U.S. DEP'T OF COMMERCE, STATISTICAL POLICY WORKING PAPER 2, REPORT ON STATISTICAL DISCLOSURE AND DISCLOSURE-AVOIDANCE TECHNIQUES 6 (1978) [hereinafter cited as WORKING PAPER]; D. DENNING, CRYPTOGRAPHY AND DATA SECURITY 336 (1982).

97. D. DENNING, *supra* note 96, at 338. In this case, the disclosure is termed approximate.

98. Thus, an approximate disclosure would occur when a formerly unknown value of a person's salary could be determined to be within \$2000 of \$20,000 per year.

close sensitive data, or the application of the technique may suppress nonsensitive data.⁹⁹ It is almost impossible to eliminate one of these errors without increasing the other one dramatically.

Yeager's request that the DEA apply disclosure-avoidance techniques to the records he wanted amounted to a request that the agency turn its raw data into statistical data.¹⁰⁰ Although it may seem to mask the underlying specific information, statistical data may still disclose a great deal of sensitive data.¹⁰¹ Thus, many sophisticated techniques have been developed to mask statistical data further.¹⁰² These techniques, however, are still subject to the two errors mentioned above. The appropriate technique depends on the data itself and the circumstances surrounding its release.¹⁰³ For example, if information similar to that being released is readily available elsewhere, extra care must be taken to ensure that no sensitive disclosure will take place when the two sets of information are compared. If the FOIA required application of disclosure-avoidance techniques, the questions of which ones to apply and in what order would remain.

In answering these questions, one must decide which of the two errors must be guarded against more strenuously. Congress chose to guard against the first error when formulating the Act.¹⁰⁴ This resulted in a statute that promotes disclosure rather than withholding of information. A different standard, however, should apply to statistical data generated by disclosure-avoidance techniques. First,

99. WORKING PAPER, *supra* note 96, at 33. For example, assume that a test grade is a sensitive item if it can be traced back to the individual test taker. Neither the average test score for the class, nor the average test score for the class divided into male and female categories, nor the number of males and females in the class, is sensitive. Thus, maximum disclosure would mandate release of all of these values. If, however, there is only one male in the class, his exact test score could be determined from the information. Therefore, less than maximum disclosure must take place if absolute privacy of grades is to be maintained. In that case, some non-sensitive data must be withheld.

100. See *Yeager*, 678 F.2d at 319 n.9. The technique of "compacting" described in the opinion would produce "macrostatistics." See WORKING PAPER, *supra* note 96, at 8.

101. See WORKING PAPER, *supra* note 96, at 1, 6. "The problem is that statistics contain vestiges of the original information. By correlating different statistics, a clever user may be able to deduce confidential information about some individual." D. DENNING, *supra* note 96, at 331.

102. See WORKING PAPER, *supra* note 96, at 11-31, 43.

103. *Id.* at 41-43. The circumstances surrounding disclosure will usually include the identity of the requester, the amount of information on the same subject available for correlation, and the age of the information. *Id.* at 25-28.

104. One of Congress' stated purposes in passing the Act was "to establish a general philosophy of full agency disclosure unless information is exempted under clearly delineated statutory language." S. REP. NO. 813, *supra* note 38 at 3.

the information upon which the statistical data is based will already have been declared exempt.¹⁰⁵ Since it is impossible to have statistical data that is absolutely untraceable to its source, the data resulting from application of disclosure-avoidance techniques is particularly suspect. Second, because it is in a much more obscure form, it is harder to determine whether statistical data is exempt than whether raw data is exempt.¹⁰⁶

Given a FOIA directive mandating agencies to err on the side of disclosure,¹⁰⁷ an agency would have to search continually for the proper combination of techniques by which the data released would meet the minimum standards of protection and still be of use to the requester.¹⁰⁸ Such a requirement would place too great a burden on that agency in terms of time and money, and create a danger that a given agency would be tempted to risk unacceptable disclosure.

As alternatives, one might allow the requester to specify the techniques he would find acceptable or allow the agency to ask the requester about his intended use of the data. The first would probably place an unmanageable burden on federal agencies. A primary fear of agencies in statistical disclosure is that the requester will have outside information with which to compare the statistical data.¹⁰⁹ Agencies would have to ensure constantly that the requester did not have some ulterior motive when specifying his preferred techniques. They would have to ensure that a requester could not identify sensitive data, even with outside information. In other words, to make this alternative manageable, an agency would have to protect against releasing too much information as opposed to too little.

105. This section does not consider requests that an agency use its computer power to compile statistical information from nonexempt data. An agency should not be required to do something that an individual can do for himself.

106. The difficulty in determining whether disclosure has taken place from released statistics may explain why statutes dealing with statistical release normally prohibit any disclosure that *may* identify a source of information. See WORKING PAPER, *supra* note 96, at 6. These statutes stand in sharp contrast to the FOIA's broad policy of release.

107. See, e.g., *Department of the Air Force v. Rose*, 425 U.S. 352, 360-61 (1975).

108. For example, an agency might have determined that compacting information into geographical categories by state would sufficiently protect the underlying information. If, however, the requester wished to make a study using the data broken down into major metropolitan areas, the agency's format would be useless to him. Since metropolitan areas may span more than one state, the reverse would be true as well. Under the standard in question, the burden would be on the agency to ensure that use of the new categories would not produce an unacceptably high probability of sensitive disclosure.

109. Outside information is information not contained in the released records themselves. See WORKING PAPER, *supra* note 96, at 17, 26-27.

The second alternative would require an inquiry into the requester's motive. Congress deemed this possibility unacceptable when enacting the FOIA.¹¹⁰ One reason the Act was drafted was to prevent agencies from hiding their mistakes inside a veil of secrecy.¹¹¹ Allowing an inquiry into motive might put an agency on guard when that motive is contrary to the agency's interests, and hamper the outflow of information. It might also allow an agency to purposely make data unusable to the requester while still showing a good faith effort.

Assuming that a standard requiring an agency to err on the side of withholding too much information is desirable, one must still determine the best means of achieving this goal. The easiest answer might be to allow an agency to use whatever techniques it considers necessary to ensure that no sensitive disclosure occurs. This would, however, put the burden on the requester to prove that another technique would release more information without violating the requisite level of privacy. This burden would be almost impossible to meet. Without the underlying data with which to frame an argument, the requester would be in a position analogous to arguing a case without witnesses. All of his pleas would have to be made in general terms.

It would be more desirable for Congress to take these three steps. First, rather than defining the point at which information becomes exempt, Congress should define the point at which exempt data becomes nonexempt, after the application of disclosure-avoidance techniques.¹¹² Although such a definition should be as specific as possible, it could not be as clearly delineated as the current exemptions.¹¹³ To enable requesters to know what to expect, the Act should require agencies to issue regulations enumerating the disclosure-avoidance techniques to be applied to each type of record sought for statistical manipulation.¹¹⁴ The particular techniques chosen by an agency would depend on the information stored in the records together with related information known to be in the public domain. Any unsatisfied requester could attack the regulations.

110. See H.R. REP. NO. 1497, *supra* note 1, at 2, 1966 U.S. CODE CONG. & AD. NEWS at 2422, 2426; S. REP. NO. 813, *supra* note 38, at 3.

111. See *EPA v. Mink*, 410 U.S. 73, 80 (1972).

112. Although a mathematical definition of the probability that disclosure will occur exists, it is beyond the scope of this Note.

113. Any definition would have to take into account many factors that are specific to each type of data to be released and would depend upon the circumstances surrounding the release. WORKING PAPER, *supra* note 96, at 41.

114. Not all types of records may be statistically manipulated. Records must first have common information. See D. DENNING, *supra* note 96, at 339.

The agency would have the burden of proving that its regulations fell within the statutory requirements, but that burden would not be an impossible one. Such a definition might reduce the amount of litigation that might otherwise occur.¹¹⁵

Second, if a particular requester was not satisfied with information released under regulations that had passed statutory muster, Congress should place the burden on him to prove that any techniques he proposed would not disclose sensitive data. In such a case, the requester would at least have access to the information contained in the release made under agency regulations. Although a particular requester might not obtain useful data, more information will still be released to the public by this method than is released today.

Finally, if Congress requires an agency to apply disclosure-avoidance techniques, it should also require the requester to pay for the computer time necessary to apply such techniques. Although there is no charge for redaction,¹¹⁶ redaction requires only the release of nonexempt material that would have been released but for the fact that it was contained in a record along with exempt material.¹¹⁷ The application of disclosure-avoidance techniques, however, has the effect of making exempt information nonexempt. It requires the formation of a new record. A disclosure-avoidance technique is much more difficult and often more expensive to apply. Therefore, a charge for its application is appropriate.¹¹⁸

Before amending the FOIA, Congress should determine the amount of additional information the amendment would release. If the situation in *Yeager* is an isolated one, such an amendment would be costly and relatively ineffective. If, under the present state of information technology, any reasonable minimum standard of data protection would be so restrictive as to make most releases of data unusable, such an amendment would also be ineffective.¹¹⁹ If, however, a substantial amount of otherwise exempt material would

115. Hopefully, once a court finds that a regulation satisfies the statutory requirements, few people will relitigate the issue unless a substantial change occurs in the content of the information or in the available disclosure-avoidance techniques.

116. *See supra* note 63.

117. Although one might argue that in a record-oriented (as opposed to an information-oriented) statute redaction does make a substantive change, this argument is incorrect. Redaction does no more than release part of a record that was already releasable.

118. The agency might waive this fee after taking into account the financial position of the requester as well as the usefulness to the public of the disclosure.

119. Advances in the state of information technology may one day make release of a substantial amount of information feasible. Congress should not ignore the possibility of such future improvements.

be made available to the public, such an amendment, though costly, would promote the policies underlying the Act.

B. RELEASE IN COMPUTERIZED FORM

1. *Form of Release*

Although the question of form has not yet been raised in FOIA litigation,¹²⁰ it was raised by a plaintiff requesting information from a state agency. In *Miller v. Kusper*,¹²¹ the Seventh Circuit let stand the district court's decision that the first and fourteenth amendments to the United States Constitution do not require a government agency to release information in computerized form when that information is available in printed form also. The court considered it irrelevant that it would have been simpler and cheaper for the requester to use a release on computer tape.¹²²

When agencies store records in more than one form, it is preferable that courts require release in the form requested, absent a showing of need to use a particular form.¹²³ In any event, the law now requires, at the least, that records be released in the form in which the agency has chosen to store them. The question remains whether a requester can specify that information stored only in computerized form be released in printed form.¹²⁴ Although a requester may have the money or equipment to deal with records released in computerized form, the person requesting a small number of records may not have access to a machine to read records released on tape.¹²⁵ There appears to be no reason that, absent a

120. See *Yeager v. DEA*, 678 F.2d 315, 326 (D.C. Cir. 1982) (court declined to address issue of whether technical information needed to read computerized records was exempt, because the issue was inextricably bound to the issue of form of release).

121. 445 F.2d 1059 (7th Cir. 1971).

122. The plaintiffs were independent candidates who wished to produce a campaign mailing list. They requested a computerized list of names and addresses that was already available to them in the form of printed poll lists. The records were stored on computer tapes for the use of the City of Chicago's Board of Election Commissioners. It would have cost \$50 to obtain a copy of the computer tape that could have been used directly to produce the mailing list. Instead, the requester was forced to spend \$6000 to convert the printed data into computerized form. *Id.* at 1059-60.

123. The requester would, of course, pay whatever fees were involved in copying the information in the form requested. See *J. O'REILLY*, *supra* note 18, at 5-11. When, due to a showing of need, the agency releases records on a more expensive medium than was requested, perhaps only the cheaper fee should be levied.

124. It is doubtful that the reverse would be allowed. While it is relatively easy to print out computer data, it is costly and time consuming to transform printed matter into computerized form. See *Miller*, 445 F.2d at 1060.

125. The cost of the equipment necessary to read a computer tape into a computer may be over \$8,000. D. BENDER, *supra* note 11, at 2-44.

showing of need, information could not be released in the form most convenient to the requester. The Act does not specify the form of release; it requires only that release take place. By allowing the requester to specify the form, the policy of complete disclosure to the public can best be fulfilled.

There may be cases in which the agency can show a need to release information in a particular form,¹²⁶ such as where, for example, the form in which the records are kept may make them non-transportable.¹²⁷ It would be impractical to require an agency to release its records in that form. The agency should be required, however, to release the information in a form as close to that requested as is practical. For example, if the information were stored directly in the computer's memory, release should be required on computer tape. If the agency had no access to tape drives, however, printed information would have to suffice. An agency might show also that the information requested is too voluminous to be useful in anything but computerized form. In that case, a request for printed information should probably be considered overbroad.

Thus, disclosure to the public may best be achieved when the requester is allowed to specify the form of release. Although an agency should not be required to computerize manually stored information, it should be required to print out information when requested, if feasible. In this way, those not wealthy enough to afford the use of a computer are not excluded from disclosure of information stored only in computerized form.

2. *Technical Information*

Once the decision to release records on magnetic tape or in some other computerized form has been made, the classification of the information necessary to read those records becomes relevant. Technical information is a record like any other requested under the FOIA. In *Yeager v. DEA*, the DEA argued that the information fell under exemption 2,¹²⁸ which protects internal agency information for which the public could have no legitimate use.¹²⁹ Certainly, if such information were needed for access to released records, the public would have a legitimate need for that information. It is there-

126. J. O'REILLY, *supra* note 18, at 5-11.

127. One example of a storage medium that may not be transportable is the disk. With certain exceptions, a disk is to computer tape what a record is to audio tape. One of these exceptions is that a disk is often permanently attached to the drive that reads its information. To transport the information stored on the disk to another system, one normally copies it onto tape. See D. BENDER, *supra* note 11, at 2-80.

128. 678 F.2d 315, 326 (D.C. Cir. 1982).

129. See *supra* notes 36-38 and accompanying text.

fore doubtful that technical information relating to records released on computer tape would be exempt under exemption 2. This information must be examined to see if it fits within any of the other exemptions.

One type of technical information is the data coding, or encryption scheme.¹³⁰ This information may need to be exempted. If exempt data were stored along with nonexempt data, both would be similarly encrypted, but the Act mandates their segregation from each other. If the Act required release of the encrypting scheme along with the nonexempt data, any protection given the exempt data from theft would be lost. Thus, the encrypting scheme would have to be protected under the same exemptions as the encrypted data.¹³¹

A problem arises, however, if the format in which the data is stored is exempt from disclosure.¹³² Information that was released or useful only in computerized form would effectively be withheld from the public. A solution would be a requirement that all such records be released in a standard storage format.¹³³ The standard format should be chosen from among the common forms of data storage in use today.¹³⁴ While it would be more appropriate for Congress to choose a standard, a court should do so if the need arises.

The above discussion relates to the format in which the data is stored; the codebook also may need protection from disclosure. The codebook sets out the physical layout of information in a record in much the same way as labels and blank lines on a printed page.¹³⁵

130. Coding involves assigning numbers to represent various characters (letters, numerals, punctuation). Coding is used to detect transmission errors, to increase efficiency, and to make data unintelligible to those who do not have the coding key. In the latter case, the coding is called "encryption."

131. If the encryption code of protected data is not found to be exempt under the same exemption as the data, then that encryption is worthless. If this were the case, Congress would have to add another exemption.

132. A data storage format consists of information concerning the organization of the complete records. The coding scheme is one element of the format.

133. An agency could, of course, still store its information in the format of its choice. The information would be translated so that it may be released in the standard format, however.

134. ASCII would be an appropriate coding scheme because of its fairly standard use among computer manufacturers. S. MORSE, *THE 8086/8088 PRIMER* 6-7 (2d ed. 1982). It is a fairly simple matter for a computer using one encoding scheme to translate data into another. These almost universal standards do not exist for other aspects of the data format. However, these other aspects would rarely fall under an exemption.

135. In addition to explaining what each byte stands for, the codebook explains which bytes should be read in as characters (encoded as found in the data format), and which as binary numbers.

In some cases, knowledge that a particular piece of information even exists is exempt from disclosure.¹³⁶ If a codebook contained a category disclosing such knowledge, simply redacting out that label would suffice.

C. WHAT IS A COMPUTER RECORD?

The Freedom of Information Act requires the release of information only if it is contained in an agency record.¹³⁷ Most likely, the use of computers will broaden the definitions of the terms "record" and "agency record."

1. Agency Records

The Supreme Court held in *Forsham v. Harris*¹³⁸ that an agency record is one over which the agency has exercised a large degree of dominion and control.¹³⁹ In that case, the only control the agency exercised over the records consisted of a few on-site visits to the federal grantee together with an unexercised right to possess the records at any time. The Court held this dominion and control to be insufficient to classify the records as agency records.¹⁴⁰

It was implicit in *Forsham* that the agency did not have any of the data in its offices.¹⁴¹ A new problem may arise, however, when, in addition to granting money to a private organization, the agency also grants space and time on its computer system. The agency's unexercised right to custody of the records will then become an unexercised right of access to the records; they are already in its custody. The additional fact that the records were stored in the agency's own computer might convince a court to hold that sufficient control existed. This would be an incorrect conclusion. There is no appreciable difference between an unexercised right to possession and an unexercised right to access.¹⁴² In either case, the agency has an absolute right to the records. The Court held in *Forsham* that "records which have never passed from private to agency control

136. For example, if it were known that there is a category of information called "number of Russian satellites booby-trapped" contained in an otherwise nonexempt record, it would have to be segregated under the national security exemption. 5 U.S.C. § 552(b)(1) (1982).

137. 5 U.S.C. § 552(a) (1982).

138. 445 U.S. 169 (1980).

139. *Id.* at 180-84.

140. *Id.* at 171-73.

141. *Id.* at 186.

142. The only difference between the two is that data stored in an agency's computers is easier to access.

are not agency records."¹⁴³ No real control over the data has passed until the agency actually accesses the data. A federal grantee may be less willing to make efficient use of computer resources if it knows that its data may be subject to open inspection. At a time when even the largest computer systems are connected to the telephone system, the mere use of an agency's computers by a grantee should not cause his records to become agency records.¹⁴⁴

Of course, in the reverse case, where an agency used computer space and time of some outside organization, the outcome must be consistent. Since in this case the agency is exercising control over the data, the record would be an agency record.

2. *Records*

The definition of the term "record" is less clear in a computer system than it is in a manual one. In a normal data base operation, the data that is initially collected may go through several stages before it is finally stored for use. When the agency uses this data, it may process and edit the data further to produce a final output whose form depends upon the particular application.¹⁴⁵ Any copies of the raw data that were saved and the data base itself are records. It is possible that the programs used to produce the various outputs are also records.¹⁴⁶ Each of these items is stored, in one form or another, by the agency. The outputs produced from the data base by these programs are not records under accepted definitions, however, unless they are stored as well.¹⁴⁷

An agency is not required to compile new records,¹⁴⁸ or to retain old ones.¹⁴⁹ This is a good example of an area of the Act that should

143. 445 U.S. at 185.

144. *Cf. Goland v. CIA*, 607 F.2d 339 (D.C. Cir. 1978) (congressional transcript marked "secret" given to the CIA for limited reference purposes is not an agency record even while in custody of the agency), *cert. denied*, 445 U.S. 927 (1980).

145. Generally, more than one application may make use of the same data base. These applications may produce radically different outputs. For example, assume as a data base the names, addresses, and party affiliations of registered voters. Democrats wishing to make use of this data base will come up with a different mailing list than would Republicans. Uses of a single data base can vary widely.

146. Whether programs may be "records" for purposes of the Act has not been decided. *J. O'REILLY*, *supra* note 18, at 5-8. One state case has determined that programs are "records" for purposes of New York's disclosure laws. In that case, however, the programs were held to be exempt as a business secret. *Belth v. Insurance Dep't*, 95 Misc. 2d 18, 406 N.Y.S.2d 649 (N.Y. Sup. Ct. 1978).

147. The output is often produced on a screen rather than on printed paper. In many systems, however, it is not difficult to redirect screen output to a printer.

148. *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 161-62 (1975).

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

be changed to reflect computerized record keeping. If an agency already has the output programs, there is no justification for allowing it to avoid running them, so long as the requester is willing to pay for the run. This is very different from the *Yeager* case, in which the agency would have had to write new programs and apply new techniques. Courts should distinguish between the two situations and apply the exemptions to the output report data rather than to the data base information.

Another possible effect the computer may have on the definition of record is best illustrated by the case of *Krohn v. Department of Justice*.¹⁵⁰ The plaintiff requested information that was scattered throughout five thousand agency records. The court denied the request on the grounds that this was a request for information rather than for a record.¹⁵¹ Although it would have been very time consuming to search through that many records by hand, a properly programmed computer might have located the information quickly. Perhaps it is time Congress considered broadening the definition of a record to include such information.

D. SEARCHES

In one of the two references to computer stored records in the legislative history of the Act, the Senate noted that "[w]ith respect to agency records maintained in computerized form, the term 'search' would include services functionally analogous to searches for records that are maintained in conventional form."¹⁵² This suggests that any record that would probably have been located in a manual system must also be produced in a computer search, regardless of whether a new program must be written to retrieve the record.¹⁵³ Computerized searches are capable, however, of locating records which would not be found through a manual search.

If an agency has already obtained or written a search program capable of retrieving the record sought, there is no reason why the agency should not use that program to process a request from the public. An agency should not, however, be required to modify, more than minimally, its existing programs.¹⁵⁴ The FOIA does not require an exhaustive effort to find data, even if the requester is certain that

150. 628 F.2d 195 (D.C. Cir. 1980).

151. *Id.* at 197.

152. S. REP. NO. 854, *supra* note 12, at 12.

153. *Cf.* J. O'REILLY, *supra* note 18, at § 5.03.

154. An agency should not be required to write a new search program even if the requester is willing to pay for this service. An agency whose computer is already over-burdened may not be able to spare the extra computer time.

the record sought is in the agency files.¹⁵⁵ Although computers do not entirely eliminate the effort required to search for records, they do reduce it sufficiently to justify requiring a broader search.

E. ACCESS TO PROGRAMS

A computer program serves a dual purpose: it is both a tool and a record. As a tool, it performs a function for the agency; as a record, it contains information and may be copied. Although the issue has not been considered by the courts, this section will assume that a computer program is a record under the FOIA. Thus, if an agency does not wish to disclose a computer program, it would have to prove that the information contained in the program falls within one of the exemptions.¹⁵⁶

A problem arises when the government has developed, at high cost, sophisticated programs it wishes to sell on the open market.¹⁵⁷ If these programs are not protected by an exemption, the government will not be able to sell them for more than the search and copy fees required by the Act. The only hope is exemption 5.¹⁵⁸ The Supreme Court has recently extended this exemption to cover trade secrets and other confidential commercial information when the government can show a good reason to keep this information secret.¹⁵⁹ There are two possible barriers to such protection. First, exemption 5 covers only inter-agency or intra-agency memoranda or letters. Superficially, a computer program appears not to fit that description. However, the Act is concerned only with the program's role as a record. As a record, the program does not affect the public at all. It is solely a set of directives that a computer follows. It thus meets the test of an intra-agency memorandum.¹⁶⁰ The second barrier is the possibility that the Court's holding in *Federal Open Market Committee v. Merrill*¹⁶¹ will be narrowly limited to its facts. In that case, the exemption would protect only purely commercial in-

155. *Goland v. CIA*, 607 F.2d 339 (D.C. Cir. 1978), *cert. denied*, 445 U.S. 927 (1980).

156. A missile guidance system program, for example, would be protected as information pertaining to national security. 5 U.S.C. § 552(b)(1) (1982). A program purchased or leased from a private organization could be protected as a trade secret or as confidential business information submitted by the public. 5 U.S.C. § 552(b)(4) (1982). Valuable computer programs are often considered trade secrets by their publishers. Trade secret law protects their programs from illegal copying.

157. For example, NASA may wish to recoup some of the costs it expended in developing sophisticated data communications programs for the space shuttle.

158. 5 U.S.C. § 552(b)(5) (1982) protects intra-agency or inter-agency memoranda that are not discoverable in civil litigation.

159. *Federal Open Market Comm. v. Merrill*, 443 U.S. 341 (1979).

160. See *supra* notes 46-47 and accompanying text.

161. 443 U.S. 340 (1979).

formation, not technical information such as a computer program.¹⁶²

Programs are costly to develop and easy to copy. It is in the nation's best interests to allow the government to recoup its development costs from such items as computer programs. Whether or not the courts extend exemption 5 to cover computer programs, Congress should pass a clear exemption protecting government generated computer programs and other trade secrets.

V. CONCLUSION

In the coming years, Congress should take a close look at the power inherent in the computer. It should restructure the FOIA to take advantage of that power so that more information can be released to the public.

One possible criticism of imposing additional burdens on agencies that computerize is that such burdens may discourage agencies from using their computers, for fear of having to release more information. However, there are few agencies that can afford not to computerize. There is no other way for an agency to keep up with the enormous amount of information it deals with on a daily basis.

The Freedom of Information Act can be amended to accommodate the technology of today¹⁶³ and the problems of tomorrow. That technology can be used to further the policies behind the FOIA. It is time Congress took notice.

*John M. Graham**

162. For a more complete discussion of how exemption 5 may be used to protect government generated technical information, see generally Belazis, *supra* note 55.

163. Congress must differentiate not only between computerized and manual record keeping systems, but also between different computer systems. The sophistication of differing systems varies widely. This fact must be taken into account in any future FOIA amendment.

* Student, Hofstra University School of Law; Associate Editor, Hofstra Law Review.