NEWS MEDIA ACCESS TO COMPUTER RECORDS: UPDATING INFORMATION LAWS IN THE ELECTRONIC AGE

ELLIOT JASPIN*

MARK SABLEMAN**

I. INTRODUCTION

Sometime in 1990, Wyoming reached a milestone of sorts, when the number of personal computers in state government — slightly more than 3,000 — first outnumbered the state's free-roaming buffalo, Wyoming's official animal.[1] Aside from showing that technology breeds faster than buffalo, this demonstrates the speed and breadth with which city, state and federal governments have embraced the computer.

A General Accounting Office (GAO) report predicted that the federal government would nearly double its 1982 purchases of "information technology" in 1989.[2] For 1989, the GAO projected that the federal government's spending on computer-related equipment would be $17 billion.[3] While some of these purchases were items that are only marginally computer-related, a 1988 General Services Administration (GSA) study of the government's computer equipment produced a staggering list of computers and related equipment. The GSA study, which excluded equipment that costs less than $50,000, such as personal computers, found the federal government had 32,250 mainframe or mini computers. The information for these computers came from 24,063 tape drives and 41,557 disk drives.[4]

---

* B.A. Colby College, 1969; Director, Missouri Institute for Computer Assisted Reporting, University of Missouri School of Journalism, Columbia, Missouri.

** J.D. Georgetown University, 1979; Partner, Thompson & Mitchell, St. Louis, Missouri.

1. The size of the free-roaming buffalo herd—as opposed to the buffalo raised commercially—is, of course, a moving target, but federal conservation officials estimate 2,400 animals. Interview with Jody Mattox, State of Wyoming, Procurement Services Division, Cheyenne, Wyoming (March 29, 1991).

2. GAO, INFORMATION TECHNOLOGY ISSUES 4 (OCG-89-6TR) Nov. 1988.

3. *Id.*

4. COMPUTER AND BUSINESS MANUFACTURERS ASSOCIATION, *Information*

This is not to say that every government agency is computerized. Courts, for example, have been slow to use computers to track court cases.[5] But, the trend is unmistakable. Local, state, and federal agencies are converting from paper to electronic record keeping. In all likelihood, every important piece of information will be maintained electronically by the turn of the century.

While this creation of a large number of computerized government databases is significant, what has fueled interest in this information is the rise of relatively cheap and simple ways for citizens, and specifically journalists, to use this information. Computer-assisted reporting of some sort has been practiced for several decades.[6] But government information is usually stored on large mainframe computers because most government databases involve thousands, and usually millions, of records. For many years, unless journalists had access to a mainframe computer, they could not handle this volume of information. However, over the past five years personal computers with adequate storage and computing power have been developed that can mimic the operation of a mainframe computer. Over the last several years, more than a dozen major newspapers have installed personal computers along with specialized hardware and software that allows them to work with information from government databases.[7]

This new electronic government is already causing significant changes in the traditional relationships between government and the press. Many journalists see the promise of true and effective access to government records in computerized information and retrieval. But many government agencies and officials, concerned that electronic records could disclose too much, have either resisted altogether, or attempted to encumber, journalistic access to these records.

Technology Industry Data Book 1960-1988, (Jan. 1989).

5. *But see* Rothman, *The Computer Age is Coming, The Computer Age is Coming,* 16 LITIGATION NEWS 6 (Apr. 1991). The author describes the increasing computerization of federal and state court records and experimental efforts including "real-time" computerized court reporting in which judges, lawyers, jurors and litigants see the trial transcript as the trial proceeds. *Id.*

6. *See* P. MEYER, PRECISION JOURNALISM: A REPORTER'S INTRODUCTION TO SOCIAL SCIENCE METHODS 109-10 (1st ed. 1973).

7. Those news organizations that have installed computer assisted reporting programs with the assistance of the Missouri Institute for Computer-Assisted Reporting include the *New York Times, Wall Street Journal, Washington Post, Akron Beacon Journal, Dayton Daily News, Orange County Register, Kansas City Star, St. Louis Post-Dispatch, Cleveland Plain Dealer, Toledo Blade, Boston Herald, Boston Globe, Palm Beach Post, Atlanta Constitution, New York Newsday, San Francisco Chronicle, Roanoke Times and World News* and the *Philadelphia Inquirer.*

II. COMPUTER-STORED GOVERNMENT INFORMATION: ACCESS AND RESTRICTIONS ON ACCESS

A. *The Journalistic Promise of Computerized Information*

Unlike its paper counterpart, information in electronic form is extremely compact and instantly accessible. A 200 foot-high stack of paper records easily fits on one reel of nine-track magnetic tape. More importantly, while it would take a reporter weeks, if not months, to read through that pile of information, the computer can search it in a matter of minutes. Some newspapers, realizing the advantages a computer can give them, are establishing programs to buy computerized government records and analyze them electronically. However, such newspapers are still very much in the minority.[8]

It is hard to overstate the importance of electronic news-gathering. While the press likes to pride itself as being the watchdog of government, so far, it has been a one-sided contest. Newspapers, magazines and broadcast stations in the United States employ approximately 260,000 reporters and editors,[9] most of whom, in one way or another, cover the activities of 17 million government workers.[10] Reporters attend press conferences, scour government publications, and maintain informants in the bureaucracy. However, most official decisions are made by obscure officials in the countless government offices and are never known, much less reported. In some cases, the very anonymity of the bureaucracy hides the fact that little, if anything, is being done.

In East St. Louis, Illinois, for example, the city election board is responsible for insuring that the voter rolls are accurate and that those who vote are, in fact, eligible to vote.[11] But how can a reporter check whether city officials are doing their job short of sorting through thousands of records? The *St. Louis Post-Dispatch* solved the problem by using a computer to match a computerized list of registered voters against the city assessor's list. It found voters registered from vacant lots and abandoned houses. Next, it matched the voters against a computerized list of death certificates. In doing so, the newspaper discovered that dead people had voted in several elections.[12]

---

8. The *New York Times* and the *Wall Street Journal* are two of the newspapers in that minority.

9. U.S. BUREAU OF LABOR STATISTICS, 36 EMPLOYMENT AND EARNINGS 184 (Jan. 1989).

10. *Id.* at 94.

11. *Dead or Alive,* St. Louis Post-Dispatch, Sept. 9, 1990, at 1A.

12. *Id.*

Reporters also have used computers to find school bus drivers who were convicted drug dealers,[13] banks that discriminated against blacks in lending practices,[14] and questionable practices in campaign financing.[15] All of these stories required searching tens of thousands of records, and could not have been attempted reasonably without computer assistance.

B. *Government Resistance To Effective Access*

The trend towards computerized government records and its importance to news-gathering is clear. Less clear are the state and federal laws, procedures, and interpretations governing access to these records. A recent incident in Ohio typifies the troubled state of the law.

The *Dayton Daily News* requested a computer tape of Ohio's approximately seven million drivers license records. Because these records were kept on a computer, the state had the facilities to quickly and easily make an electronic copy for less than $1,000. There was also no question that the records were public. The state routinely provides copies of individual records in paper form. The newspaper was told it could have the records, but state law required the government to charge $3 per record. State officials told the newspaper that, if it wanted the information, it would have to hand over a check for $21 million.

What clearly has changed is not the substance of the information, but its form. Yet, this is a source of endless difficulty. Because most people, including lawmakers and bureaucrats, have little or no experience with computers, they tend to treat electronic information as if it were in a form they understand — paper. In the Ohio example, $3 may have been a reasonable cost to retrieve one paper record. But applying the same logic to electronic records produced an absurd result.

The issue is further complicated by the fact that computers are widely regarded as technical, powerful, and mysterious things that require a high degree of circumspection. The federal Freedom of Information Act (FOIA),[16] for example, assumes that public officials will have to search through paper records to find requested information.[17] The

13. Providence Journal-Bulletin, May 11, 1986, at A-13.

14. *Atlanta Blacks Losing in Home Loans Scramble,* Atlanta Constitution, May 1, 1988, at 1.

15. Lynn, *Computer Study of Cuomo Donors Finds Correlation with Contracts,* N.Y. Times, Nov. 1, 1990, § A at 1, col. 1.

16. 5 U.S.C. § 552 (1988).

17. *See generally* 5 U.S.C. § 552 (1988).

Act even permits the government to charge for the search time.[18] But when the Public Citizen Litigation Group requested computerized data from the Labor Department's Occupational Health and Safety Administration (OSHA), government officials balked.[19] OSHA argued that an electronic search of records required "programming" which is not specifically required under the Act.[20]

Storage in electronic form also challenges our assumptions about the way in which information can be viewed. When we talk about a record in paper form, there is little doubt about what we mean. It is, at the very least, one physical entity such as a tax form or a job application. Conversely, a computerized record may be a compilation of several different pieces of information that exist independently of one another in multiple files. These pieces of information are retrieved, assembled, and displayed in less than a second by a computer as if they were all part of a single record. In fact, a computer user may have no idea that the display on his or her screen was a compilation of information but, when this "record" is no longer needed, it ceases to exist as one entity. Even though this is a very common way of using information electronically, the government argued in *Yeager v. Drug Enforcement Administration*[21] that a request for information located in four different databases was "overbroad."[22] The irony is that the very nature of the electronic information, which makes it far easier to handle and rearrange, is being used as a justification under FOIA for denying access to this information.

While under the best of circumstances, electronic records challenge the way we think about and use information, computerization can also make it easier for the government to enforce secrecy. In the past, secrecy in government was enforced through a classification system and a rubber stamp. Things that needed to be kept secret were mixed up with information of marginal sensitivity and information that, if public, would be embarrassing to public officials. The battles in these cases centered on either the rationale behind a classification system or particular documents.[23] When the government moves the same information

---

18. 5 U.S.C. § 552(2)(4)(A) (1988).

19. Moore, *Access Denied,* NAT'L. J., Sept. 9, 1990, at 121.

20. *Id.*

21. 678 F.2d 315 (D.C. Cir. 1982).

22. *Id.* at 320.

23. A classic example was the Pentagon Papers, which were considered highly secret by the government, even though much of it dealt with the history of the U.S. involvement in Vietnam. While this information was embarrassing to the government, it was not harmful to prosecution of the war.

into a computer system, it can protect secrecy not only by enforcing a classification system, but also by raising a series of objections based on the storage medium. The government may claim, for example, that disclosure would be too costly, that it would require special programming or that it would involve disclosure of proprietary software. In short, not only have computers given journalists new opportunities, but they also have provided bureaucrats with new excuses for withholding information.

III. NATURE OF ELECTRONIC RECORDS

Before beginning a discussion regarding ways to update laws that govern access to information, it is important to understand how the technology has changed from the days of paper records.

A computer is a vast number of switches. Each switch in memory is called a "bit" and its position is symbolized by a "1" or a "0." If a switch is open, it is a "0" and, if it is closed, a "1." The bit, in a sense, is like a line on a piece of paper. One line is not very meaningful but several put together in a pattern gives us an "A." By the same token, if we take a collection of eight bits and put them together in a pattern we can represent that same "A" electronically as "11000001." In computer jargon the eight bits are called a "byte" and the whole system of bits and bytes is referred to as the binary code.

When someone sits down at the keyboard of a computer and begins to type a sentence, each keystroke sends a signal to the computer to store the bit pattern associated with that key in the computer's memory. Thus, by striking the letter "A," eight of the switches that make up the computer's memory are set open or closed to represent the binary pattern of an "A": 11000001. To the computer, a tender love letter, a financial report or a shopping list are the same thing: a collection of "1's" and "0's". However, the way this information is viewed or organized or, more importantly, how the computer is told to deal with the information, becomes a crucial issue.

For example, if we hand a child a list of names and ask that it be alphabetized by last name, he or she will come back with a list that has "Jones" before "Smith." Not so a computer. If you type "John Doe" into a computer, it will have no way of distinguishing between the first and last name because it is all a lot of bits and bytes strung together.

To get around this problem, computer programmers use the idea of "records" and "fields." Each one of the names in a list becomes a single record. For reasons that will soon become apparent, all records in the list are a set length of twenty-five spaces. The records, in turn, are divided into fields. There is not an actual physical division. Instead, the

first ten spaces are set aside to be "first name" and the remaining fifteen spaces are "last name." When the computer is asked to sort a list by last name, it uses the information stored in the last fifteen spaces of each records — the "last name" field.

The way in which the information is organized is described in something called a record layout. Typically, a record layout will list the field name, the starting position of the field, its length and the type of information stored there. The record layout of a city payroll file might look like this:

DIAGRAM 1: Typical Record Layout

Field	Start	Length	Type
City ID	1	4	A
Last Name	5	15	A
First Name	20	10	A
Pay Period	30	6	A
Salary	36	8	N
Overtime	44	8	N
Sick Pay	52	8	N
Job Code	60	2	A

This means that something called the "City ID" code begins in the first position of each record, is four positions long and is made up of "alphanumeric"[24] characters. Beginning in the fifth position is a field called "Last Name" that takes up 15 spaces and is also alphanumeric. This pattern continues until the "Salary" field is reached which is eight positions long and contains only numbers. The last field in the record, entitled "Job Code," refers to a coding system used to describe what a person does. Codes are used to save time and space on electronic records. It is far easier to type in "B2" instead of "Waste Collection Engineer" for everyone who works as a garbage collector. Furthermore, the computer can be programmed to take "B2", look it up in the electronic version of a code book and print "Waste Collections Engineer." The record layout and the codes are referred to as the "documentation."

Most people would describe this collection of records as a database. However, technically this may not be correct. In many cases one

24. There may be numbers mixed in with the letters in the field.

file or table of information may constitute a database. But, there are times when a database will involve a series of tables that contain related information.

Assume that in addition to keeping salary information, the government also wanted to keep information on disciplinary actions taken against any of its employees. To enter this information into the computer, a programmer could add more fields to the employee record. These fields, for example, would contain the date of the infraction, type of wrongdoing, and punishment. The first time an employee's record needed to be updated, there would be no problem. But, what if a person had two infractions? There would be no place in the electronic record to add information about the second offense. One way to solve that problem would be to set up several fields in each record to record infraction #1, infraction #2 and infraction #3. While such an approach might work in most cases, it would fall apart the first time a person reached a fourth infraction.

To solve this kind of problem, the relational database was invented. Instead of putting all employee information into one table, two tables are created: one contains employee information and the other contains employee infraction information.

DIAGRAM 2: Typical Use of Tables in Relational Database

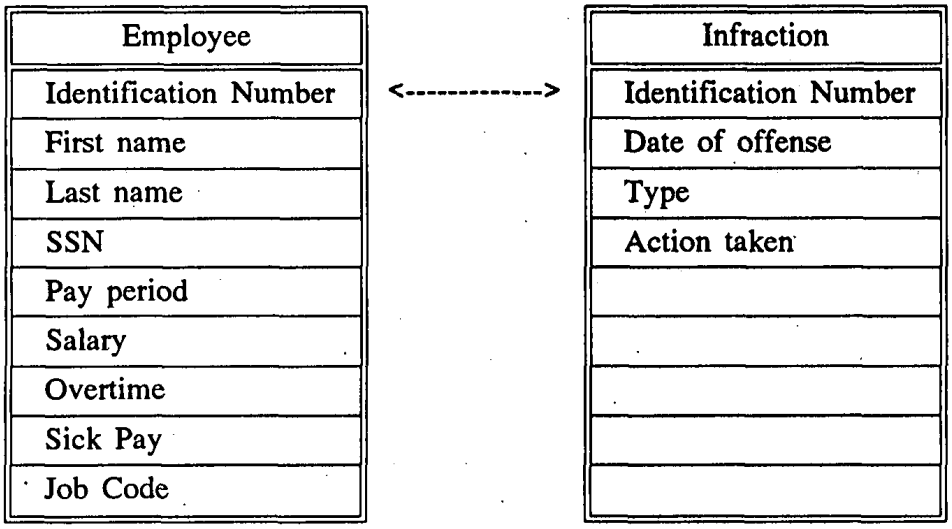
Employee
employee 1
employee 2
employee 3
employee 4
employee 5
employee 6
employee 7
employee 8
employee 9

Infraction
employee 1 - #1
employee 1 - #2
employee 6 - #1
employee 6 - #2
employee 6 - #3
employee 6 - #4
employee 8 - #1
employee 9 - #1
employee 9 - #2

Each time an employee is disciplined, a record of that action is added to the employee infraction table (Diagram 2).

This solves the problem of finding space for each infraction, because an almost infinite amount of records can be added to the infraction table. But, how do you know which employee committed which infraction? One solution would be to include all of the employee information in the record layout for employee infractions. However, this would waste an incredible amount of time and space because the same employee information such as name and address was entered over and over again. To get around this problem, the idea of key fields was developed. In the sample record layout above, each employee has an identification number that is unique to that person. If that number is included in the infraction record, a relationship between the two records has been created. Because the two tables hold information about a common element "employees" they are considered to be part of one database. Hence the name, relational database.

DIAGRAM 3: Typical Relational Database



It is now possible to retrieve information from one table that will list the employee's name and, using the identification number, search the second table to obtain any infractions. What will appear on the computer screen will be the name of the individual and a list of the various times the person was disciplined. A computer user might have no idea he was actually drawing information from two separate tables of information.

While organization of information into fields and records may seem to be a concern only to computer programmers, it is at the very heart of a revolution in human understanding that began with the invention of the printing press.

Prior to the invention of moveable type, books were a scarce commodity and found mostly in medieval monasteries. Unlike today's modern libraries, books in a monastery were simply piled up in a room like sacks of flour. With so few books, there was no need to keep them in order. When books became more numerous, it became necessary to catalogue and index them. How else to find what you needed? With the creation of lists and indexing schemes came a change in the way we thought about things. Through the indexing process, information patterns emerged from what, at first glance, appeared to be a series of events so random as to be meaningless.

The documentation of a computer database is a direct descendant of a process that started in a monastery overwhelmed with books. The difference is, that through electronics, we can catalogue and efficiently retrieve not only books, but every word in those books. We are able to reduce large masses of information to their smallest significant parts,

index, and categorize those parts, and then rebuild them with a few keystrokes into an intelligible whole.

We can see this change in something as simple as the creation of a list of names. Prior to the introduction of the computer, a typical method for handling a list of names was to place each name on a separate piece of paper and sort the pieces of paper. As a slight refinement, the user might list the surname first on the paper to make sorting easier. By contrast, someone using a computer will break that same list of names down into a last name, first name, middle name, and title field — each of which can be sorted and used independently. More importantly, each element of the name can be cross-matched with other lists of names in other databases to see if there is any pattern or relationship.

Until now, the discussion has assumed that the computer into which the data has been typed had an unlimited capacity to hold information. In fact a computer's memory is not only limited but volatile. Each of the switches is operated electrically, and if the power is cut, the switches are no longer able to function. That is why the content of a computer's memory is lost when the power is turned off.

To save information, computers use a variety of techniques to copy information from the computer's memory to a safer medium. How this is accomplished and in what form the information is stored can have an effect on the legal issues of access. When people say they want access to electronic information, what they are actually saying is that they want a duplicate of the information stored outside of the computer's memory. How difficult is it to make such copies? What is the expense involved? What format should be used in making these copies? These are technical as well as legal questions, and an understanding of the technical issues is necessary in developing solutions to the legal issues raised.

The most common form of storage is the floppy disk. This is nothing more than a thin circular piece of plastic coated with a substance that is sensitive to a magnetic field. By exposing this coating to magnetic pulses, the computer can create a series of "bumps" similar to the irregular shape of a phonograph record to represent the ones and zeroes in the computer's memory.

Floppy disks can store up to 1.4 million characters, but this is not nearly enough space for mainframe computers. Instead of using floppy disks, mainframe computers usually store their information on nine-track magnetic tape. The tape looks similar to the recording tape used on a reel-to-reel tape deck and can hold up to 300 million characters of information. Because each electronic character is made up of eight bits, the information is stored as a series of lines or tracks of eight

bits arranged vertically across the tape.

DIAGRAM 4: Typical Bit Arrangement on Tape

1	0	0	1
1	1	1	0
0	1	0	0
1	1	1	0
0	1	0	0
1	0	0	0
1	1	1	1
0	0	0	0

How closely together these lines of information are recorded is known as tape density and is expressed in bits per inch (bpi). Thus, a tape that is recorded at 1600 bpi, has 1,600 bits on one inch of tape.

For example, a person might request a government computer tape in EBCDIC at 1600 bpi. To a person unfamiliar with tape storage, the request might appear burdensome. However, we now know that all the person is asking is that the government use a standard coding scheme for its information and that it be recorded at a particular tape density. It is as reasonable as asking that the information in paper form be in English on sheets of 8 1/2" x 11" paper. Computer jargon, in this case, can serve to obscure understanding of what is happening.

"Programming" is another word that carries with it misconceptions that tend to overwhelm the uninitiated. In our sample record layout above, there is a field for Social Security number. If a reporter requested copies of that information, the government might argue that it would require programming to provide the record with the social security number redacted. If programming is regarded as an arcane and highly difficult activity, this may sound like an undue burden is being placed on the government. However, that is not the case.[25] To draw an analogy, it is like saying that using a boat requires seamanship without giving any regard to the different levels of skills required to operate different boats. Rowing a boat on a placid lake requires one level of seamanship, while sailing a yacht in defense of the America's Cup requires quite another level.

If a programmer wanted to select all information from our employee database except for the Social Security number, he or she would

25. To put it in the vernacular, there is programming and then there is programming.

tell the computer to "select" certain fields and omit from that list the field for Social Security number. Such a command might look like this:

> Select first-name, last-name, pay-period, salary, overtime, job-code from employee[26]

In the sense that this is a command that the computer will use to perform some useful function, it could be termed programming. Nonetheless, the government would have a difficult time claiming that typing the above command involves any undue burden. In fact, just the opposite is true. In most imaginable situations, it is far easier to manipulate electronic records than it is to redact information in paper form.

In some instances the government will not object to using computers to prepare a response to a FOIA request but will balk at providing the information electronically. Why should the government be compelled to provide information in a specific form? In one sense, such an objection is plausible. If the information is not on computer, it would be unfair to force the government to enter the data electronically simply to meet an FOIA request. But, what if the information is already in electronic form? From a technical standpoint, there is no difference in the level of effort required for copying information stored in a computer to a magnetic tape or to a printer. If anything, producing magnetic tape is quicker because the mechanical process of placing ink on paper will almost always be slower than the electronic recording process.

IV. How Reporters Use Computer Records

The earlier example of how names can be broken apart and analyzed using a computer typifies the impact computers are having on the journalistic process.

The *Kansas City Star* used just such an analysis of names to develop a story on inadequate personnel practices in the Kansas City Fire Department.[27] The newspaper assigned a reporter to work full time purchasing and analyzing government computer tapes. The reporter used a personal computer which was able to read information directly from the large reels of magnetic tapes used to store information on a mainframe computer.

Using this computer system, the *Star* purchased a copy of each one of Missouri's four million driver's license records and culled out the driving records for people from the Kansas City area. The newspaper

---

26. The command is written in a database language called SQL and will work on any computer using this particular language.

27. Reeves, *Kansas City Firefighters Catch Heat Behind the Wheel,* The Kansas City Star, Dec. 30, 1990, at A1.

then developed another database of Kansas City firefighters. The computer made it possible to break down each person's name into its constituent parts, cross-index those names and find firefighters who, while assigned to drive fire engines, were using drivers licenses that had been suspended or revoked for such things as drunk driving.

It is equally important to note that the brute force of the computer makes it possible to work with millions of records. Without having this kind of power, newspapers are often unable to monitor even the most basic government function, such as tax collection.

New York City, for example, taxes approximately 1.5 million parcels of land. *Newsday* reporter Penny Loeb wondered just how well the city, which, like many major cities, is facing fiscal crisis, is handling its tax collections. Because of the huge number of taxable properties, the city has computerized its collections system. Loeb was able to purchase a copy of the computer tape containing the collection records for all of the city's taxable properties for $225 and, using a personal computer hooked to a tape reader, analyze the information.

Each record contained fields that identified the property's location as well as two fields that indicated whether there is an open balance for that property. If the taxpayer owes the city money, there is a negative number in the open balance field. On the other hand if property owners have for some reason overpaid their taxes, there is a positive number in that field. What struck Loeb, as she looked through the information, were the number of records that showed the city owed money. To find out just how many people were due refunds, Loeb created a subset of the larger database by telling the computer to save only those records where there was a positive number in the open balance field.

The computer found that approximately a third of the 1.5 million tax records showed the city owing money. To assess the size of the problem, Loeb used the computer to total the amount of refunds due. In a matter of minutes the computer reported that the city owed, and had not refunded, approximately $275 million.

When Loeb interviewed city officials, they readily acknowledged that they had not been refunding overpayments or even telling taxpayers that they were owed money. When asked why no one was told about refunds, one city official explained, "We are not required by law to let anybody know about credits." In some cases the city had even tried to foreclose on homes for supposed non-payment of taxes when, in fact, it owed the property owner money.[28]

---

28. Loeb, *City Mum on Funds it Owes to Taxpayers,* Newsday, Jan. 7, 1991, at 5.

V. CURRENT LEGAL TREATMENT OF ACCESS TO ELECTRONIC RECORDS

There are two principal ways that electronic information is obtained from the government. Typically, reporters or researchers will request copies of electronic information pursuant to the federal Freedom of Information Act or its state or local level counterpart. In these cases, officials sometimes challenge a reporter's right to the information.

At the same time, many government agencies freely, and perhaps even eagerly, provide some kinds of information through on-line databases or bulletin board services. For example, the Securities and Exchange Commission's *EDGAR* system[29] is specifically designed to allow prompt and widespread dissemination of information filed at the Commission.[30] Users can use their own computer to telephone the SEC's computers and retrieve information they need.[31]

Many other federal agencies actively disseminate computerized information, including: the Census Bureau, which makes available numerous statistical data compilations;[32] the Food and Drug Administration, which makes available an electronic bulletin board of its news and recall releases;[33] the Environmental Protection Agency, which makes available its electronic National Toxic Release Inventory database;[34] the Agriculture Department which makes available time-sensitive economic,

---

29. Electronic Data Gathering Analysis and Retrieval (EDGAR) of SEC filings.

30. *See Federal Information Dissemination Policies and Practices: Hearings before the Government Information, Justice, and Agriculture Subcommittee of the Committee on Government Operations,* 101st Cong., 1st Sess. 61-69 (1989) [hereinafter *1989 House Hearings*] (statement of John Penhollow, Director of the SEC Office of EDGAR Management).

31. *Id.*

32. *See Electronic Collection and Dissemination of Information by Federal Agencies: Hearings Before a Subcommittee of the House Comm. on Government Operations,* 99th Cong., 1st Sess., 259-66 (1985) [hereinafter *1985 House Hearings*] (testimony of Bryant Benton, Associate Director of the Bureau of the Census for Management Services).

33. *1985 House Hearings, supra* note 32, at 240-47 (testimony of Gerald F. Meyer, Associate Commissioner for Management and Operations, Food and Drug Administration).

34. *1989 House Hearings, supra* note 30, at 75-85 (testimony of Edward J. Hanley, Director, EPA Office of Information Resources Management). Electronic dissemination of the toxic chemical inventory is mandated by the Emergency Planning and Community Right-To-Know Act of 1986, Pub. L. No. 99-499, § 313(j), 100 Stat. 1745 (1986) (codified at 42 U.S.C. § 11023(j) (1988)). *See generally* T. MCINTOSH, FEDERAL INFORMATION IN THE ELECTRONIC AGE: POLICY ISSUES FOR THE 1990S 42-43 (1990).

crop, and trade information;[35] and the Commerce Department, which makes available the National Technical Information Service, a compilation of many different government-prepared technical publications and data compilations.[36]

Although legal issues may arise with respect to such information, particularly with respect to the means of its dissemination and applicable fees, there is no dispute that the public and the press have a right to such information in useable electronic form. Government handling of such information falls under the rubric of *information dissemination policy*, a subject generally beyond the scope of this article.

For journalists and researchers, the more important and daunting issues of access to government information involve information that the government does not freely or voluntarily make available. When met with government resistance, the public must turn to the provisions of the Freedom of Information Act or its state law counterparts to compel the government to produce the requested information. The law in this area is crucial because the boundaries within which production of government information can be compelled influence voluntary compliance with the FOIA and even government voluntary dissemination policies. In these battles, a number of unique issues are raised:

(1) Are computer records covered by the Freedom of Information Act and similar state public records laws?

(2) Must agencies make special searches for computer records or prepare special search programs?

(3) Does a citizen have the right to obtain information in electronic form?

(4) How should confidential information contained in electronic files be redacted?

(5) Must agencies utilize their computer capabilities for rearrangement or aggregation of data?

(6) What fees apply for retrieval of computer records?

(7) What special problems exist when commercial services use or assemble government records, or when governmental entities establish and maintain commercially valuable libraries and databases?

(8) Can access to government electronic information be

---

35. *1985 House Hearings, supra* note 32, at 250-55 (testimony of Glenn P. Haney, Director, Office of Information Resources Management, Department of Agriculture).

36. *1989 House Hearings, supra* note 30, at 402-08 (statement of Joseph E. Clark, Deputy Director of the National Technical Information Service). The NTIS consists of more than 4,000 electronic data files and software products which originate from many different agencies. *See generally* T. MCINTOSH, *supra* note 34, at 37-40.

restricted because of copyright law?

(9) Do government agencies have any obligation to create or preserve electronic records?

Few of these questions have been directly addressed by access statutes. Moreover, judicial resolution of these issues has been inconsistent, both in the outcomes reached and in the principles applied.

Because most freedom of information acts were written without computer technology in mind, they provide few clues for handling the special problems raised by computer records. Courts frequently have made *ad hoc* judgments, often based on analogies or analysis of doctrines that were developed in connection with different situations. Also, fears, suppositions and misunderstandings regarding computers and computer records have influenced decisions.

The existing decisions often take contradictory approaches and involve questionable assumptions. A unified new approach is needed, one that recognizes the character, pervasiveness, and importance of government computer records in today's society.

A. *Background: Federal and State Freedom of Information Acts*

The federal Freedom of Information Act is the most important government records law because of the obvious importance of the federal government and its pervasive records. Many state records access acts were patterned after it. FOIA was meant to be a broad mandate of disclosure of government records, except in limited cases where non-disclosure was needed for specific verifiable reasons.[37]

FOIA makes all federal agency records presumptively available to the public, upon a request reasonably describing the records sought. Certain exemptions are granted. These exemptions are to be "construed narrowly, in such a way as to provide the maximum access consonant with the overall purposes of the Act."[38] It is not mandatory for agencies to withhold documents in these categories, however. The Act simply requires disclosure of all records "except as specifically stated,"[39]

---

37. The disclosure-oriented philosophy of the Act has not been realized. *See* Fricker, *Information Please: Is FOIA a Myth?,* A.B.A. J., 57 (June 1990). Exceptions, rather than being limited, have tended to become almost routine in many areas. And while the Act was meant to provide quick and speedy answers to requests, requesters usually receive a quick denial as their only prompt response, followed by many long delays as they further pursue their requests for disclosure. *See 1989 House Hearings, supra* note 30, at 472 (testimony of U.S. Rep. Gerald D. Kleczka).

38. Vaughn v. Rosen, 484 F.2d 820, 823 (D.C. Cir. 1973).

39. 5 U.S.C. § 552(c) (1988).

and it nowhere forbids disclosure.[40] Thus, agencies may disclose these records if they wish.

There are nine exemptions to the Freedom of Information Act. The most frequently litigated exemptions are:

1. National security.[41]
2. A catch-all exemption for information specifically exempted from disclosure by statute.[42]
3. Trade secrets and private confidential information.[43]
4. Inter-agency or intra-agency records.[44]
5. Personal privacy records including personnel, medical and similar files.[45]
6. Law enforcement records.[46]

---

40. *See* 5 U.S.C. § 552 (1988).

41. 5 U.S.C. § 552(b)(1) (1988).

42. 5 U.S.C. § 552(b)(3) (1988).

43. 5 U.S.C. § 552(b)(4) (1988). This refers to information obtained from outside the government which the owner or original source of the information wishes to keep confidential.

44. 5 U.S.C. § 552(b)(5) (1988). This refers to internal government records which, if in existence among private parties, would be considered exempt from discovery in a court case because of the work product doctrine or the attorney-client privilege. *See* Access Reports v. Department of Justice, 926 F.2d 1192 (D.C. Cir. 1991).

45. 5 U.S.C. § 552(b)(6) (1988). This exemption covers information contained in a personnel, medical, or similar file where the release of the information would be a "clearly unwarranted invasion of privacy." Files "similar to personnel and medical files" include all other files which contain information about particular individuals. However, a government record must contain personal information about an individual before it can be considered subject to the personal privacy exemption. Thus, privacy with regard to this exemption is a narrow category relating to specific information about individuals, and it does not include all information which individuals may consider "private" about themselves. Department of State v. Washington Post, 456 U.S. 595 (1982). State privacy laws often similarly exempt from state information access laws so-called "personal information" — i.e., information maintained and retrievable by a person's name or another identifier. *See* Spargo v. N.Y. State Comm'n on Gov't Integrity, 531 N.Y.S.2d 417 (N.Y. App. Div. 1988), *appeal denied,* 531 N.E.2d 299 (N.Y. 1988).

46. 5 U.S.C. § 552(b)(7) (1988). These records are exempt to the extent production (a) would hinder enforcement proceedings, (b) would deprive a person a fair trial, (c) "could reasonably be expected to constitute an unwarranted invasion of personal privacy," (d) would disclose confidential sources or confidential information, (e) would disclose law enforcement techniques such that they would be circumvented, or (f) would endanger anyone's life or physical safety. Wellford v. Hardin, 444 F.2d 21, 23-25 (4th Cir. 1971).

The purpose of this exemption is to maintain confidentiality of "information gathering steps" and "to prevent premature discovery by a defendant in an enforce-

FOIA establishes simple procedural requirements for requesting information. The request, which need not be in any particular form, is usually done by letter. It need only "reasonably describe" the records sought.[47] The agency must make a reasonable search for the records and produce them, unless they are exempt.[48] Because of the presumption of openness, agencies bear the burden of proving that an exemption applies, based on specific and detailed reasons applicable to the specific documents requested.[49]

The agency is required, in response to a proper request, to determine within ten business days whether it will comply.[50] If the agency refuses to comply, an appeal can be made to the agency, and the agency is required to determine any appeal within twenty business days.[51] Agencies can extend their time limits another ten business days "in unusual circumstances."[52] If the agency fails to comply with the time limits in the Act, the applicant is deemed to have exhausted his administrative remedies and thus may sue in court.[53]

Suits appealing from adverse FOIA request determinations may be filed in any United States District Court, at any time up to six years after the agency's denial of the appeal. On a *Vaughn* motion, the Court may order the government to produce an index describing the withheld documents and the justification for each claimed exemption.[54] FOIA provides for the government to pay plaintiff's attorneys' fees if plaintiff

---

ment proceeding." Thus, "the emphasis . . . is upon the investigatory character of the files, and under § 552(c) the exemption should be limited 'specifically' to files of this type. It should not be enlarged . . . to include records of administrative action taken to enforce the law." *Id.* at 25.

Under the law enforcement exception, "rap sheets" have been held exempt from disclosure, because disclosure of such information about private citizens would be unwarranted in light of the purposes of the Act (to allow citizens to be informed about the conduct of government) and the broad privacy protection contained in 5 U.S.C. § 552(b)(7)(c) (1988) pertaining to law enforcement investigatory records. United States Dept. of Justice v. Reporters' Comm. for Freedom of the Press, 489 U.S. 749 (1989).

47. 5 U.S.C. § 552(a)(3) (1988).

48. Miller v. United States Department of State, 779 F.2d 1378, 1383 (8th Cir. 1985).

49. Mead Data Central, Inc. v. Department of Air Force, 566 F.2d 242, 258 (D.C. Cir. 1977).

50. 5 U.S.C. § 552(2)(6)(A)(i) (1988).

51. *Id.* § 552(2)(6)(A)(ii) (1988).

52. *Id.* § 552(2)(6)(B) (1988).

53. *Id.* § 552(2)(6)(C) (1988).

54. Vaughn v. Rosen, 484 F.2d 820, 827 (D.C. Cir. 1973).

has "substantially prevailed."[55]

State public records laws vary considerably in their format, substantive provisions, and procedural requirements. Some state statutes are structured as fairly simple declarations that all state records are public, and leave exceptions to other, specifically enacted statutes.[56] Other states have followed the format of the federal Freedom of Information Act fairly closely.[57]

B. *Issues Relating To Statutory Access To Government Computer Records*

1. Coverage of Computer Records

It is now well established, despite some adverse decisions, that the federal FOIA and most state public records law cover computer records. Indeed, the leading decision written by Judge (now Justice) Anthony Kennedy states directly: "[T]he FOIA applies to computer tapes to the same extent it applies to any other documents."[58] Other courts and the Administrative Conference of the United States are in accord.[59] Also, the federal Computer Security Act of 1987, designed to protect government computer systems, specifically provides that it does not affect FOIA.[60] Thus, when the government lacks the authority to withhold information in print form, it also lacks the authority to withhold the same information maintained in electronic format, including comput-

---

55. 5 U.S.C. § 552(2)(4)(E) (1988).

56. "Every person who has custody of a public record shall permit the record to be inspected and examined by any person desiring to do so." FLA. STAT. ANN Section 119.07 (1)(a) (West 1982 & Supp 1992). "All public records which are presently provided by law to be confidential or which are prohibited from being inspected by the public, whether by general or special law, are exempt from the provisions of subsection (1). *Id.* at Section 199.07 (3)(a).

57. *E.g.*, ILL. REV. STAT. ch. 116, para. 102-11 (1991).

58. Long v. United States Internal Revenue Service, 596 F.2d 362, 365 (9th Cir. 1979).

59. Yeager v. Drug Enforcement Admin., 678 F.2d 315, 231 (D.C. Cir. 1982); Mayock v. Immigration and Naturalization Serv., 714 F. Supp. 1558, 1566 (N.D. Cal. 1989), *rev'd on other grounds,* 938 F.2d 1006 (9th Cir. 1990); St. Paul's Benevolent Educ. and Missionary Inst. v. United States, 506 F. Supp. 822, 828 (N.D. Ga. 1980)(computer tape prepared by private groups with assistance of federal Centers for Disease Control held to be agency record subject to FOIA); ADMIN. CONF. OF THE U.S., RECOMMENDATION ON "FEDERAL AGENCY USE OF COMPUTERS IN ACQUIRING AND RELEASING INFORMATION", 1 CFR § 305.88-10 (1988) (hereinafter ADMINISTRATIVE CONFERENCE REPORT).

60. Computer Security Act, Pub. L. No. 100-235, § 8 (1987) (codified at 40 U.S.C. §759 (1988)).

erized data base, optical disk, or other computer system storage medium.[61]

Many state public records acts specifically state that they cover computer records. California, for example, defines a public record as any "writing containing information relating to the conduct of the public's business"[62] and lists among the various forms of writing "magnetic or paper tapes, photographic films and prints, magnetic or punched cards, discs drums and other documents."[63] In cases where computerized information is not specifically mentioned in the definition of a public record, states such as Delaware say that a record is public "regardless of physical form or characteristic."[64] In other states, courts have construed the acts to cover computer records.[65]

2. Agency Search and Programming Responsibilities.

Must agencies make special computer searches for the information requested, or prepare special computer programming for such searches? Because it would normally be impossible for a member of the media or public to conduct his or her own search of government computer files, the answer to this question can be crucial when FOIA requests are made for information contained in government computer records.

FOIA requires agencies to make reasonable efforts to comply with requests that reasonably describe the requested information.[66] But, it does not require agencies to create new records.[67] These two principles usually define the debate regarding an agency's search and programming responsibilities with respect to computer records. The requester will point to the agency's responsibility to make a reasonable search. The agency, if it wishes to object to the request, will claim either that the programming does not fall within the scope of a reasonable search,

---

61. H.R. REP. NO. 153, 100th Cong., 1st Sess., pt. 2, at 30-31 (1987).

62. California Public Records Act, CAL. GOV'T CODE §6252(d) (West 1980).

63. *Id.* 6252(d),(e).

64. Delaware Freedom of Information Act, DEL. CODE ANN. tit. 29 §10002(d) (1990).

65. Menge v. Manchester, 311 A.2d 116 (N.H. 1973) (computerized tape of field record cards compiled by city assessor's office for use in arriving at real estate tax assessments held to be a "public record" under state FOIA law); Minnesota Medical Ass'n v. State, 274 N.W.2d 84 (Minn. 1978)(data concerning payments to medical assistance vendors stored on computer tapes held to be "public records" available to public under state Data Privacy Act).

66. Miller v. United States Dept. of State, 779 F.2d 1378, 1383 (8th Cir. 1985).

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

or that the agency is not required to create new records for the requester.

The legislative history of the Freedom of Information Act shows that Congress expected computer searches to include "services functionally analogous to searches for records that are maintained in conventional form."[68] However, charges may be leveled for "services involving the use of computers needed to locate and extract the requested information."[69] Although the reference to computer searches may relate to searches of hard copy files with computerized indexes, it seems clear that Congress also intended to require searches of information maintained in electronic databases.

Some agencies also object to programming on the grounds that requesters are really demanding the creation of a new record, which is improper under FOIA. They claim that by selecting certain pieces of information out of one record, or by drawing together several different bits of information out of several records, an agency is being asked to create a new record. However, this argument misunderstands the nature of computer records. Virtually all government financial records are organized as a collection of different records that the computer pulls together. One administrative FOIA appeal decision specifically held that "the mere retrieval of information already existing in a database, even if a computer must be programmed to select specified types of data, does not constitute creation of a new record."[70]

Some agencies have resisted computer searches on the ground that if programming is required, the request is improper. Some agency regulations even explicitly state that the agencies will not create new programming to search their computer records.[71] Patti Goldman, an attorney for Public Citizen Litigation Center, a public interest group, explained in testimony before the Government Information, Justice and Agriculture Subcommittee of the House Committee on Government Operations that she has repeatedly encountered resistance from agencies that consider basic search programming beyond the requirements of FOIA. Some of these agencies have since backed down from this position.[72]

Part of the problem with the argument that computer program-

---

68. S. REP. NO. 854, 93rd Cong., 2d Sess. 12 (1974).

69. *Id.*

70. *1989 House Hearings, supra* note 30, at 495-96 (citing DOE Case No. KFA-0146 at 4-5 (Nov. 24, 1987)).

71. *E.g.*, 32 C.F.R. § 286 (1989) (Dept. of Defense FOIA regulations).

72. *1989 House Hearings, supra* note 30, at 474-503 (testimony of Patti Goldman, Public Citizen Litigation Center).

ming is not required under FOIA is that the term "programming" is ambiguous and has no fixed meaning. Essentially, every computer operation of any nature involves some programming. As OSHA's computer director testified in one case, "[I]t takes programming of the computer to do anything and to do everything. There is nothing that happens without some sort of programming."[73]

Realistically, agencies should have no objection to a requirement that they do an ordinary or modest amount of programming in response to FOIA requests. Some FOIA officers have reportedly even welcomed the opportunity to use computer programming to conduct searches for information because it allows them to find and produce information in the most economical ways.[74]

Several state courts have held that agencies must conduct searches for computerized information even when it requires creation of a new computer program. In *Family Life League v. Department of Public Aid*,[75] for example, the Illinois Supreme Court required the Illinois Department of Public Aid to devise a computer program that would generate requested information[76] while protecting confidential data.[77] The court required plaintiffs, as they had previously agreed, to bear reasonable costs associated with such programming.[78]

A Florida court reached an opposite result, holding that an agency cannot be required to use a special program, even when it is prepared by or at the expense of the applicant.[79] In *Seigle*, the court viewed the applicant as attempting to get a "free ride" from the state agency.[80] The applicant could have reclassified the information he requested with the assistance of an outside paid expert; instead, he sought to have the agency do the work for him.[81] The court found that it was

---

73. *1989 House Hearings, supra* note 30, at 492 (testimony of Patti Goldman, Public Citizen Litigation Center) (quoting deposition of John A. Katzlinas in Public Citizen v. OSHA, No. 86-0705 (D.D.C.).

74. T. MCINTOSH, *supra* note 34, at 93, 98-99. One FOIA officer explained in response to a Justice Department questionnaire that "segregating portions of documents by computer would leave out so many steps in redacting and xeroxing that a great deal of time and money could be saved." *Id.* at 98 (quoting Lolo L. Secora, a U.S. Information Agency FOIA officer).

75. 493 N.E.2d 1054 (Ill. 1986).

76. Specifically, lists of physicians, hospitals and others that provided abortion services. *Id.* at 1056.

77. *Id.* at 1059.

78. *Id.*

79. Seigle v. Barry, 422 So. 2d 63, 66 (Fla. Dist. Ct. App. 1982), *review denied*, 431 So. 2d 988 (Fla. 1983).

80. *Id.*

81. The court appeared preoccupied with the possibility that a large amount of

not the intent of Florida's public records law to force public officials to compile charts and prepare documentary evidence.[82] Rather, the sole intent of the act was to make available to the public, information in some meaningful form, not necessarily the form which the applicant desires.[83]

Notably, in *Seigle*, all of the information was available to plaintiff without the special programming. In cases of this nature, where the government can turn over all its computer records to the requester, and no confidential information or other obstacle prevents the release of all tapes or records, the Florida court's conclusion that special programming is not required may be appropriate. This is a different situation, however, from *Family Life League*[84] and other cases where the computer tapes contain confidential information or other information that could not be disclosed. In those cases, where simple, standard programming is necessary to allow meaningful access to the information sought, basic FOIA principles require agencies to use such programming to search and isolate from their total records the portions that can or should be disclosed.

The Administrative Conference of the United States also has recommended that agencies not deny access to electronic records on grounds that retrieval of electronic information is equivalent to creation of a new record, or that programming is required for retrieval.[85] Rather, agencies should use a "standard of reasonableness in determining the nature and extent of the programming that provides an appropriate search for and retrieval of records in responding to FOIA requests."[86] Thus, to some extent, the Administrative Conference believes that FOIA requesters may legitimately ask an agency to produce data organized in formats other than those used by the agency in the regular course of its operations.[87]

Courts have ruled in general terms that different access requirements for computer records "may not be used to circumvent the full disclosure policies of the FOIA. The type of storage system in which the agency has chosen to maintain its records cannot diminish the duties

---

expense and time would be wasted if the government was required to rearrange and reformat information to suit every requester's particular needs. *Id.*

82. *Id.*

83. *Id.*

84. Family Life League v. Dept. of Public Aid, 493 N.E.2d 1054 (Ill. 1986). *See supra* notes 75-77 and accompanying text.

85. ADMINISTRATIVE CONFERENCE REPORT, *supra* note 59, at 50.

86. *Id.* at 51.

87. *Id.*

imposed by the FOIA."[88] This is obviously the correct result, since computerized records are simply another form of information storage, a modern technological equivalent of the basic office filing cabinet. Certainly with respect to records that were once maintained in hard copy files, and which are now maintained in computer-accessible electronic storage, the computerized records should be as readily available as the hard copy records were.[89] Thus, both the policies and practicalities of FOIA's requirement for reasonable searches mandate that such searches be made of computerized information as well as hard copy information.

3. Production of Computer-Format Documents

If journalists are to use government computer records in a meaningful way, they must have access to those records in a useable electronic format. Most laws pertaining to records, because they were written with paper records in mind, are silent as to production format.[90] Relatively few cases have addressed the production format issue, and there is currently a split of authorities.

Agencies frequently take the position that requesters are entitled to records only in a standard documentary format, even if those records are also (or even primarily) maintained electronically. One frequently cited federal case, *Dismukes v. Department of Interior*[91] upholds this position. However, *Dismukes* is infrequently followed, and it appears now to be largely discredited by the majority of reported decisions, and by the actual practice of the U.S. Department of Justice.

In *Dismukes*, the plaintiff sought a computer tape listing of participants in an oil and gas lease lottery.[92] The information was maintained by the agency both on a computer tape and on microfiche records.[93] Both the computer tape and the microfiche were concededly non-exempt agency records under FOIA.[94] However, the agency refused to produce the information on computer tape as requested and stated the

88. Yeager v. Drug Enforcement Admin., 678 F.2d 315, 321 (D.C. Cir. 1982).

89. Indeed, lawyers who use the ubiquitous "Lexis" and "Westlaw" computerized legal research systems know that searching computerized databases can often be easier than searching records maintained in hard copy files.

90. Some of these laws are changing in this respect. In 1989, Oregon amended its records law to specifically require that electronic records be provided in the format sought by the requester if it is available. *See* Oregon Open Records Act 1989, Or. Laws 546, § 2 (codified at OR. REV. STAT. § 192.440(2) (1989)).

91. 603 F. Supp. 760 (D.D.C. 1984).

92. *Id.* at 760-61.

93. *Id.* at 761.

94. *Id.*

information was available only on microfiche.[95] During judicial review, the district court upheld the agency's refusal to produce the computer records and agreed that production of the records in microfiche form was sufficient.[96]

The court in *Dismukes* recognized that there may be some special significance to electronic records.[97] In some cases electronic records may contain more or different information than paper records.[98] Nonetheless, in comparing the Interior Department computer tape and microfiche, the court concluded that they contained identical information, and thus production of only the microfiche was sufficient under FOIA.[99]

The court essentially ignored the plaintiff's claim that the microfiche form would hamper his access to the information. Instead, it focused on the Department's ease of operations, since the Department had already chosen to release information in microfiche form and that format served a broader audience.[100] In essence, the court held that convenience to the agency was a sufficient reason to deny access to computer tapes, at least when equivalent information was available in other forms.[101]

The *Dismukes* court's view of FOIA is too crabbed. It exalts form over purpose, by allowing the legally mandated disclosure of information to be met in a way which is impractical to many users. In its blindness to technological realities, the legal principle behind *Dismukes* is no different than that of the official who tells a reporter that he can inspect files and attempt to remember what he has seen, but cannot take notes or photocopies. Such limited interpretations of the right of access are contrary to the spirit and purpose of FOIA.

Indeed, the House of Representatives committee with FOIA responsibility has explicitly disagreed with the *Dismukes* position. In its

---

95. *Dismukes*, 603 F. Supp. at 760.

96. *Id.* at 763.

97. *Id.* at 762.

98. For example, the court said that plaintiff might argue that a transcript and an audio tape, for example, might not be equivalent records if the audio tape contained additional information, such as inflections and tones, that were not contained on a written transcript. *Id.*

99. *Id.* at 763.

100. *Id.* at 762-63.

101. The court explained, the "defendant has no obligation under FOIA to accommodate plaintiff's preference. The agency need only provide responsive, nonexempt information in a reasonably accessible form, and its offer to plaintiff [of microfiche] satisfies that obligation." *Id.* at 763.

policy overview of electronic collection and dissemination of information by federal agencies, the House Committee on Government Operations has explained:

> Public access is a dynamic concept. If an agency has developed the ability to manipulate data electronically, it is unfair to restrain the public to paper documents. An agency cannot justify denying the public the benefits of new technology by preserving, without involvement, the same type of access that was provided in the past.[102]

The most telling refutation of *Dismukes*, however, is the Justice Department's own failure to follow it in actual practice. In numerous post-*Dismukes* cases where requesters have sought government computer tapes, agencies initially refused to disclose the tapes based on *Dismukes*, but immediately backed down and produced the tapes once litigation had begun.

One frequent FOIA practitioner, Ronald Plesser, explained his experience with *Dismukes* to a House government information subcommittee:

> I have prosecuted many requests for electronic records and generally I have been successful where the underlying information is public. When I proceed to court, the government generally settles. This is fortunate for my clients who can require public release of data with a minimum of effort. It may, however, be unfortunate for the development of the law because the Justice Department has in many cases avoided judicial decisions on these important issues. It is my experience that when you come to court with a case concerning electronic access to otherwise public information, the Justice Department usually capitulates. Meanwhile, when you go back to the agencies on the next case, they will continue to assert these discredited theories.[103]

Plesser provided, and the subcommittee published in its hearings, several of these settlement agreements.[104]

While the Department of Justice's selective enforcement of

---

102. HOUSE COMM. ON GOVERNMENT OPERATIONS, ELECTRONIC COLLECTION AND DISSEMINATION OF INFORMATION BY FEDERAL AGENCIES: A POLICY OVERVIEW, H.R. REP. NO. 560, 99th Cong., 2d Sess., at 10 (1986).

103. *1989 House Hearings, supra* note 30, at 510-11 (testimony of Ronald L. Plesser).

104. Initial refusal by Air Force Department to produce computer records, followed by Stipulation of Dismissal of FOIA case four months later in which the Department agreed to make the requested computer tapes available). *Id.* at 517-20. Settlement agreement in which Government Printing Office agreed to produce computer records. *Id.* at 521-26. Consent order in which Customs Service agreed to produce computer records. *Id.* at 527-33.

Dismukes may not mislead experienced FOIA practitioners, the continued presence of *Dismukes* as the leading reported federal appellate decision on this issue has improperly skewed the development of the law. For example, the Court of Appeals for the Ninth Circuit followed *Dismukes*, noting the "scant authority" available and characterizing *Dismukes* as "apparently the only case that has directly confronted the 'choice of format' issue."[105] The court saw *Dismukes* as dispositive and did not even publish its own decision.[106]

Production of information in electronic form is not really a burden to agencies, and the Administrative Conference of the United States has recognized that it is in an agency's own interest to both acquire and release information in electronic form.[107] The Administrative Conference has recommended that when agencies are required to disclose their records in a public reference room, they should provide for electronic disclosure as well as paper disclosure of any information already in electronic form.[108] At the least, agencies should also make their electronic information available in an easily usable electronic form.[109] And, even when agencies are *not* required to disclose information in an electronic form (as held by the court in *Dismukes*), agencies should consider "upgrading" the information to electronic disclosure.[110]

State courts, for the most part, have required production of electronic documents in a suitable electronic format. In *American Federation of State, County & Municipal Employees v. County of Cook*,[111] the Illinois Supreme Court specifically disapproved *Dismukes*.[112] Analyzing the Illinois Freedom of Information Act (Illinois Act), the court looked to the Illinois Act's broad wording, which includes electronic data processing records under its definition of "records."[113] Thus, the court concluded that the Illinois Act requires disclosure of computer tapes themselves when they are requested.[114] The burden should be on the

105. Van Strum v. United States EPA, 892 F.2d 1048 (9th Cir., Jan. 4, 1990) (unreported decision; text in WESTLAW).

106. *Id.*

107. ADMINISTRATIVE CONFERENCE REPORT, *supra* note 59, at 51-53.

108. *Id.* at 53.

109. *Id.*

110. *Id.*

111. 555 N.E.2d 361 (Ill. 1990).

112. *Id.* at 365.

113. *Id.* at 364. The court noted that the Illinois Act included "tapes, recordings, electronic data processing records, recorded information and all other documentary materials, regardless of physical form or characteristics." *Id.* (citing ILL. REV. STAT. ch. 116, para. 202(c) (1985)).

114. 555 N.E.2d at 364.

agency to show that some exemption applies to computer tapes if the agency desires to refuse to disclose them.[115] This same reasoning would apply to *Dismukes*, of course, since it is well established that computer tapes are "records" under the federal FOIA. The Illinois court specifically rejected the agency's argument that production of tapes in computer format was inconvenient.[116] Even if one form of disclosure is more convenient to the agency, the court held information can be disclosed in different forms to different parties.[117] Since the Illinois Act focuses on disclosing information to the public, the public's convenience and not the agency's, must control.[118]

Similarly the Ohio Supreme Court in early 1992 recognized that *because* of the extra convenience of electronically stored records, the records should be produced in that format. In *State ex rel. Margolius v. Cleveland*,[119] the court characterized the electronic format as a "value added" to the records which should be shared with the public where needed. The court reasoned that if an agency possessed two sets of the same records, one organized in a file cabinet and the other in a random stack of papers, the public would obviously be entitled to access to the organized set. The same principle supports production of documents in electronic format:

> In a similar vein, a set of public records stored in an organized fashion on a magnetic medium also contains an added value that inherently is a part of the public record. Here, the added value is not only the organization of the data, but also the compression of the data into a form that allows greater ease of public access.[120]

Likewise, in *Brownstone Publishers, Inc. v. New York City Department of Buildings*,[121] a New York court disapproved *Dismukes*, holding that the New York's Freedom of Information Law required disclosure of computer records themselves.[122] Both the trial and appeals courts found persuasive the New York policy requiring "full" and "maximum"

---

115. *Id.* at 366.

116. *Id.* at 364-65. The standard in Illinois is "unduly burdensome" not merely inconvenient. *Id.*

117. *Id.*

118. *Id.* at 366.

119. 584 N.E.2d 665 (Ohio 1992).

120. *Id.* at 669.

121. 550 N.Y.S.2d 564 (N.Y. Sup. Ct.), *aff'd*, 560 N.Y.S.2d 642 (N.Y. Div. App. 1990).

122. *Id.* at 566.

access to public records.[123] Moreover, the trial court noted that the agency could really show no hardship was involved in copying a computer disc onto a computer tape, as requested.[124]

In *Menge v. City of Manchester*[125] the New Hampshire Supreme Court similarly held that computerized tapes of field record cards compiled by the City of Manchester in arriving at real estate tax assessments were public records.[126] Unlike the *Dismukes* court, which held the agency's convenience to be conclusive, the court in *Menge* weighed not only the agency's convenience, but also the *requester's* convenience.[127] The court found that the relative ease and minimal cost for the agency of reproducing computerized tape was well outweighed by the expense and labor that would be involved for the requester if it had to abstract information from traditional paper records.[128] Thus, the court held that the computer tapes were public records and must be reproduced and provided to the requesters at the requester's own expense.[129]

Again, in *Ortiz v. Jaramillo*,[130] the court required a county clerk to produce a magnetic tape of voter registration records, and not just a hard copy of the records.[131] The court stated that the right to inspect public records should carry with it the benefits arising from improved methods and techniques of recording and utilizing information so long as proper safeguards as to use, inspection, and safety were maintained.[132] Because computer tape copies can be made with reasonable safety, the court held that such tapes had to be made available for public copying.[133]

Other state courts have emphasized that requesters should not be required to engage in the unnecessary make-work of going through paper documents, or traveling to different places to view paper documents, when the same information can be readily and simply produced in a computer format.[134] A few state authorities are contrary, and, like

123. *Id.*; 560 N.Y.S.2d at 643.
124. 550 N.Y.S.2d at 566.
125. 311 A.2d 116 (N.H. 1973).
126. *Id.* at 118.
127. *Id.*
128. *Id.*
129. *Id.*
130. 483 P.2d 500 (N.M. 1971).
131. *Id.* at 502.
132. *Id.* at 501.
133. *Id.* at 501-02.
134. Skikszay v. Buelow, 436 N.Y.S.2d 558 (N.Y. Sup. Ct. 1981) (where requester could obtain information if he spent the time to go through the records manually and copy the necessary information, copies and computer tape format should be

Dismukes, hold that production in any one format is sufficient to satisfy the records law.[135]

4. Redaction of Confidential Information

In keeping with the disclosure-oriented purpose of FOIA, documents cannot be withheld merely because they contain some confidential information. Rather, confidential information is required to be redacted from the documents whenever possible, and nonexempt portions of the documents produced.[136]

In *Long v. IRS* (*Long I*),[137] an extended case involving confidential taxpayer information, the U.S. Court of Appeals for the Ninth Circuit, in a majority opinion written by Judge (now Justice) Anthony Kennedy, held that the Internal Revenue Service (IRS) was required to produce computer tapes of its Taxpayer Compliance Measurement Pro-

---

made available); Martin v. Ellisor, 223 S.E.2d 415 (S.C. 1976) (information should be made available in computer tape format where reproduction of computer tape places no greater burden upon the government agency than other available means of reproduction, and where the requesting party is willing to pay the cost of reproduction of the computer tape).

See also Long v. IRS, 596 F.2d 362, 369 (9th Cir. 1979). This decision tends to support production of the information in a meaningful computer format. Judge Kennedy rejected the IRS's contention that the plaintiff did not need to examine raw data, noting that examination of source data was essential to allow researchers to conduct their own analysis. *Id.* This reasoning tends to support production of records in computer format, since that format also facilitates analysis by the accessing party.

See generally Annotation, *State Freedom of Information Act Reports: Right to Receive Information in a Particular Medium or Format*, 86 A.L.R. 4th 786 (1991).

135. *E.g.*, Tax Data Corp. v. Hutt, 826 P.2d 353 (Colo. 1991) (upholding agency regulations that denied direct access to agency computer terminals for requesters on basis that the state statute allowed agencies to set regulatory limits on access); Hoffman v. Pennsylvania Game Commission, 455 A.2d 731, 733-34 (Pa. Commw. Ct. 1983) (game commission allowed to make subscriber mailing list available only in hard-copy format, even though mailing list is stored electronically; commission had broad discretion to chose the appropriate format for disclosure of the list); Chapin v. Freedom of Information Comm'n, 577 A.2d 300 (Conn. App. Ct.), *cert. denied*, 580 A.2d 56 (Conn. 1990) (following *Dismukes* and holding that the agency need not produce computer records because Connecticut's FOIA states that agencies with computer records "shall provide a print out of data;" and, as such, the court concluded that *only* a print out need be provided).

136. 5 U.S.C. §552(b) (1988) provides: "Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection."

137. 596 F.2d 362 (9th Cir. 1979).

gram with personal identifying information deleted.[138] The court, thus, refused to permit the IRS to avoid disclosure of all information simply because some personal identifying information was contained in the database. In a later case, however, (*Long IV*),[139] Judge Kennedy explained that, in some instances, deletion of confidential information may involve such extensive work "that the remaining information is not reasonably segregable."[140] In such instances, the agency need not produce the records at all.

Although the legal principles stated in both *Long* decisions are sound, the factual assumption in *Long IV* that confidential information in computer records may not be "reasonably segregable" may be questionable. As a practical matter, computer-stored information is much *more* likely to be "reasonably segregable" than hard copy records. Again, understanding how a computer works is essential. As explained above,[141] relatively few simple commands can usually accomplish the necessary redaction.

In producing hard copy records with confidential information deleted, agencies routinely pore over paper documents line-by-line, and even word-by-word, in order to delete exempt information by hand using black markers. In contrast, it is usually much easier to redact information from computer records.

In the case of information stored in computers and organized in standard fields, a relatively simple programming step can insure that all information in a particular field (i.e., taxpayer name and other identifying information) can automatically be redacted and left off of printouts or duplicate electronic files. Accordingly, in most cases, it is much *less* likely with computer records than with paper records that deletion of confidential information would involve such extensive work that the remaining information is not reasonably segregable.

In 1984, for example, Thomas J. Moore, who was then a reporter for the Knight-Ridder Newspapers Washington Bureau, began examining the safety record of interstate trucking companies.[142] This was not a simple task, considering that Moore wanted to look through the records of approximately 250,000 trucking companies, 90,000 accident reports filed with the federal government, 80,000 truck inspection reports and

---

138. *Id.* at 366.

139. 825 F.2d 225 (9th Cir. 1987). The *Long* case had a "long and tortuous history" including repeated trips up and down the appellate system.

140. Long v. IRS, 891 F.2d 222, 230 (9th Cir. 1988) (hereinafter *Long. IV*).

141. *See supra* notes 25-26 and accompanying text.

142. Interview with Thomas J. Moore, Knight-Ridder Newspapers.

roughly 5,000 trucking company safety reports. The only way he could tackle this story was to obtain the electronic version of all these records that the Department of Transportation kept on its computer. But federal officials raised an objection.

"They did not want to release the name and social security number of drivers in the accident reports," Moore explained.[143] "They felt it would be an invasion of privacy. But I was focusing on unsafe trucking companies not individual drivers."[144] Because a driver's name and social security number were separate fields within the records, the government was able to delete the information with very little effort when it made copies of the computer tapes. Moore received the edited version, 425,000 electronic records on fifteen reels of computer tape, in nine days. After he had analyzed the electronic records, Moore decided to request the paper records of sixteen companies that appeared to have the worst safety records in the industry.

"There are nuances in the paper record. I also wanted additional confirmation of the information I was seeing on the computer," Moore said.[145] However, deleting a driver's name and social security record from the paper record was much more involved than deleting it from the electronic counterpart. A clerk had to first locate the record, read through it to find any names or social security numbers, cover the information with tape, photocopy the taped version, remove the tape, and then return the original to the file. After seven and a half months, the Department of Transportation had only been able to edit and photocopy roughly 500 paper records from five of the sixteen trucking companies.[146]

State courts also have required programming to insure that confidential information is deleted from computer records produced pursuant to state public records acts. For example, the Illinois Supreme Court required the Department of Public Aid to create a computer program to produce certain of its records with confidential information deleted.[147] The court held that such a program was required, because, otherwise, the purpose of the state public records act "would be totally thwarted if

---

143. *Id.*

144. *Id.*

145. *Id.*

146. The story that Moore published was a four-part series showing federal officials were usually unwilling to crack down on unsafe trucks, although the number of people killed in truck accidents far exceeded deaths from all other forms of commercial travel.

147. Family Life League v. Department of Public Aid, 493 N.E.2d 1054 (Ill. 1986).

an entire record could be kept closed simply by inserting some minute confidential information, particularly when the confidential information can be deleted."[148]

In analyzing issues of redaction of confidential information, therefore, courts must consider the extent to which redaction can be accomplished, and non-exempt information isolated for disclosure, by means of computer programming. If computer programming of the kind normally carried out in the agency can accomplish this task, then the information *is* reasonably segregable and this computer-directed redacting should be carried out.

American Friends Service Committee v. Department of Defense,[149] illustrates the proper analysis. Plaintiff sought non-confidential information from classified Defense Department technical bulletins.[150] The plaintiff noted that the agency itself had computer software which it currently used to create unclassified technical circulars, and urged the court to require modification of that software so that it could be used to isolate non-confidential materials from the earlier bulletins.[151] The court implicitly acknowledged that plaintiff's requested solution — requiring modification and use of software to redact confidential information — could be appropriate under FOIA. The test, essentially, was a factual one, depending on *how much* modification and extra work was entailed. In this case, because the extra efforts would have been quite extensive, computer-directed segregation of non-confidential information was not reasonably feasible.[152] The decision, however, supports the principle that computer-directed searches to redact confidential information may well be appropriate in other instances, even if some rewriting and modification of software is required.[153]

---

148. *Id.* at 1058.

149. No. 83-4916 (E.D. Pa. Aug. 4, 1988) (1988 WESTLAW 82852), *aff'd*, 869 F.2d 587 (3rd Cir. 1989).

150. *Id.* at 1.

151. *Id.* at 1-2.

152. The court explained:

> The evidence is that there are between 12,000 and 15,000 entries for each of the biweekly TABs. For the time period in question, this would require analyzing for deletion and/or restatement, re-indexing and re-sequencing somewhere between 1,250,000 and 1,500,000 individual entries and then making a determination as to whether the reconstituted documents as a whole posed a substantial risk to national security. Under these facts, the TABs are not reasonably segregable, even if mere deletions, no matter how extensive or voluminous, might be held to be reasonably segregable.

Id. at 5.

153. The court expressly reserved this issue:

5. Rearrangement or Aggregation of Information

Information stored electronically often can be easily compiled, aggregated, and rearranged using computer programs. The deletion of confidential information just discussed[154] is one such form of rearrangement of data. Can persons requesting access to government records also ask for further, more sophisticated kinds of manipulation of the data? Specifically, do these capabilities to rearrange data, when coupled with the pro-disclosure purposes of FOIA, create new obligations or agencies? So far, three reported cases have addressed these questions and have answered them differently.

In *Yeager v. Drug Enforcement Administration*,[155] a sophisticated computer user requested disclosure of four Drug Enforcement Administration (DEA) computerized record-keeping systems.[156] One of the systems, the Narcotics and Dangerous Drugs Information System (NADDIS) contained both exempt and arguably nonexempt data.[157] The NADDIS computer system contained over one million records on suspects, drug offenders, informants and witnesses.[158] Each of the records contained standard information fields in which particular data concerning each person is entered, if available.[159] Information in certain fields, such as the name, address and social security number of the individuals involved, was plainly exempt from disclosure under FOIA.[160] Information in other fields, such as occupation or geographic-

---

> Whether, if the technology is available, a governmental agency could ever be required to develop a computer program to delete exempt portions of agency records and rearrange or reformulate the information in some fashion so as to be available for a FOIA requester need not be decided in this case.

Id. at 6.

A computer program search to redact confidential information was also requested in *Clarke v. United States Department of Treasury*, No. 84-1873 (E.D. Pa. Jan. 28, 1986) (1986 WESTLAW 1234), where the plaintiff sought, from a confidential Treasury Department database, the names and addresses of all registered owners of government flower bonds. *Id.* at 1. The court did not reach the issue of the appropriateness of such a computer search because it ruled that the information sought was exempt. *Id.* at 2.

154. *See supra* notes 136-153 and accompanying text.

155. 678 F.2d 315 (D.C. Cir. 1982).

156. *Id.* at 317.

157. *Id.* at 318.

158. *Id.* at 322.

159. *Id.* at 322 n.15.

160. *Yeager* at 322. This information was exempt under 5 U.S.C. § 552(b)(7) (1988) — the "investigatory records compiled for law enforcement purposes" exemp-

al location, was in a gray area. Such information could indirectly lead to identification of an individual, and thus was arguably exempt. But depending upon how it was presented, it might be possible for this data to be disclosed in a way that would not indirectly aid identification of the individuals, and thus, not violate the FOIA exemption.[161]

The plaintiff did not contest DEA's claim that both categories, "hard core" personal identifiers (name, address and related fields) and "soft core" personal identifiers (such as occupation and geographic location) were exempt.[162] Rather, plaintiff asserted that the "soft core" personal identifiers could be disclosed in a way that would not reveal the identity of the persons in the DEA files by using a computer disclosure-avoidance technique, "compacting."

Disclosure-avoidance techniques, as explained by the court, are techniques that "have been developed to facilitate the release of statistical information so that the information cannot be traced to a specific individual."[163] One of these techniques, called "collapsing" or "compacting," involves expressing specific information, such as a date or a city, in more general terms, such as a ten-year span or a geographic region.[164] The plaintiff urged that "compacting" was simply another way of reasonably segregating information and thus was required by the FOIA.[165]

The district court rejected plaintiff's argument as to a duty to use disclosure-avoidance techniques, as "beyond the statutory directive" of FOIA.[166] The D.C. Circuit affirmed, rejecting the argument as "conceptual gerrymandering of the boundaries of agency duty."[167] In analyzing Yeager's claim, the circuit court viewed the disclosure-avoidance technique issue as a battle between two competing policies: the full-disclosure policy of FOIA, and the well-established principle that an agency need not create a new record. It is well settled that an agency is not required by FOIA to create a new document in order to satisfy a request.[168] It is equally well settled that merely deleting some informa-

---

tion.

161. *Id.* at 322.

162. *Id.*

163. *Id.* at 319 n.9.

164. *Id.*

165. *Yeager* at 322.

166. *Id.* at 319 (quoting Yeager v. Drug Enforcement Admin., No. 76-093, 6 (D.D.C. Oct. 30, 1980)).

167. *Id.* at 322.

168. *Id.* at 321 (citing NLRB v. Sears, Roebuck & Co., 421 U.S. 132, 161-62, (1975)).

tion from agency records does not make the document a "new document" that is exempt from disclosure.[169] As noted by the D.C. Circuit in *Yeager*:

> Agencies are not, however, required to commit to paper information that does not exist in some form as an agency "record." Thus, they need not write an opinion or add explanatory material to a document.[170]

The court viewed Yeager's proposed techniques as requesting the creation of a new record.[171]

The court held that it was not Congress' intent to force agencies to rearrange and reorganize the requested record's content.[172] Moreover, Congress certainly did not desire to impose a "greater segregation duty upon agencies that choose to store records in computers than upon agencies that employ manual retrieval systems"[173] — the odd situation that would result if the court imposed "compacting" or similar duties on agencies with computer records. The bottom line of the *Yeager* ruling is that "[a] requester must take the agency records as he finds them."[174]

The *Yeager* decision did acknowledge that freedom of information rights of access to information cannot be diminished merely because records are kept in computer storage form rather than manual storage systems.[175] And, though it rejected a "compacting" requirement as a matter of interpretation of FOIA, the D.C. Circuit in *Yeager* acknowledged both the practicality and the potential usefulness of such techniques:

> It cannot be gainsaid that computers have become an integral part of the functioning of our society. Both private and governmental entities use the storage, processing, and retrieval capabilities of computers to improve organizational efficiency. The DEA has developed sophisti-

---

169. *Id.* at 321 (citing *Long I*, 596 F.2d at 366 (9th Cir. 1979)); Disabled Officer's Ass'n v. Rumsfeld, 428 F. Supp. 454, 457 (D.D.C. 1977).

170. 678 F.2d at 321 (*citing* NLRB v. Sears, Roebuck & Co., 421 U.S. 132, 955 S. Ct. 1504, 1521-22 (1975)).

171. *Id.* at 323.

172. *Id.*

173. *Id.* at 322.

174. *Id.* at 322-23.

175. *Yeager* at 321. "Although accessing information from computers may involve a somewhat different process than locating and retrieving manually-stored records, these differences may not be used to circumvent the full disclosure policies of the FOIA. The type of storage system in which the agency has chosen to maintain its records cannot diminish the duties imposed by the FOIA." *Id.*

> cated computer software in order to increase the efficient use of a vast amount of information gathered by its agents provided by informants and witnesses, and obtained from other sources.
>
> . . .
>
> The interpretation suggested by Yeager may be desirable in terms of full disclosure policy and it may be feasible in terms of computer technology; these factors notwithstanding, however, we are not persuaded that Congress intended any manipulation or restructuring of the substantive content of a record when it commanded agencies to "delete" exempt information.[176]

Similarly, in *Long IV*,[177] the requester sought various editing strategies including deletions of certain information on a rotating basis. The Ninth Circuit majority concluded that those strategies involved such extensive editing that they would amount to creation of new records and were impermissible.[178] In this regard, *Long IV* reached the same result as *Yeager*.

The Illinois Supreme Court, however, required computerized "scrambling" or "recodifying" of otherwise exempt student test scores in *Bowie v. Evanston Community Consolidated School District*.[179] Although individual student test scores were exempt from disclosure, the court ordered the district to "scramble" the record and reveal test scores by race. The court rejected arguments that by requiring "scrambling" it was requiring the school district to create a new record. Two justices dissented, citing *Yaeger* in support and claiming that the state legislature did not intend "to impose a duty on public bodies to use their computer capabilities to provide information in a form that would make the material nonexempt."[180]

In some cases agencies have voluntarily produced information in "aggregate" form where the underlying data was largely exempt. In one case, an agency itself aggregated exempt bank examination data, and produced aggregated data showing mortgage rejection rates by the geographic area and the race of the customer.[181] By this means — aggregation of exempt information — the privacy of the individual exempt data was fully preserved, but the significance of the data nonetheless revealed to the benefit of the press and the public.

Perhaps the strongest justification for the result reached in *Yeager*

---

176. *Id.* at 320-21 (footnote omitted), 323.
177. *Long v. I.R.S.* 825 F.2d 225 (9th Cir. 1987).
178. *Id.* at 230.
179. 538 N.E.2d 557 (1989).
180. *Id.* at 563.
181. Interview with Bill Dedman, former reporter, Atlanta, Ga. (May 1991).

and *Long IV* is that this is truly uncharted waters, unanticipated by Congress and unanswered by the direct language of FOIA. If Congress does not directly address this issue, courts will be lost at sea on an issue that is bound to rise again, as electronic use and rearrangement of data becomes readily available. As long as FOIA is silent on this issue, courts will have to examine the particular computer data rearrangement techniques at issue and make a factual determination as to whether those techniques more closely resemble deletion of reasonably segregable information (which is required under FOIA), or creation of new records (which is not required).

Such scholastic hair-splitting to decide those issues makes little sense. Congress should amend the FOIA and directly address the propriety of requests for agencies to use computer data rearrangement techniques. These techniques should be required, where they are reasonably available, because they promote the disclosure of non-exempt information and because agencies have not put forth any greater justification for not using these techniques other than it inconveniences them. In fact, the present way of framing the issue, whether or not a new record is being created, is unrealistic. Since computers, in their normal operation, are designed to bring together and summarize information from disparate sources, it hardly makes sense for an agency to claim they are faced with some special or burdensome task. When information is on paper, the task of assembling summary and aggregate data may be an undue burden. But, when the information is in electronic form, summarization and aggregation become trivial tasks.

As computer capabilities increase, the gulf between current laws and the way information is actually used is bound to grow. Even now many people are able to write programs to run on government computers that will perform aggregation. As computer software becomes easier to use, agencies' claims that programming is a "burdensome" process will make even less sense. Refusing to utilize all available electronic means of disclosing non-exempt information is no more appropriate than refusing to utilize simpler technology, such as black markers, to delete exempt information from paper records.

In making any appropriate amendments to FOIA, Congress can, of course, make adequate provision for payment by requesters of direct costs associated with such techniques. Moreover, a reasonableness limitation can be imposed even on data-rearrangement, so that agencies are not being required, in the words of the Administrative Conference, "to create large new databases for private advantage, thus using agency

resources for private purposes."[182] Short of that extreme, data-rearrangement techniques can further disclosure of non-exempt government information at little inconvenience or disadvantage to government agencies.

6. Fees for Computer Records

The FOIA and most state records laws allow agencies to charge "reasonable fees" for "direct" costs of searching for and copying records. In some cases, however, these costs may be reduced or waived. The reasonableness of the fee charged can be crucial to journalists, since large fees could prohibit or inhibit journalists from obtaining the records they need for many kinds of investigations.

Under the FOIA, when "a representative of the news media"[183] makes a request, fees generally are limited to the "reasonable standard charges for document duplication."[184] This is a significant reduction from the general FOIA fees, which includes charges for search time as well.[185] Search time fees can often be prohibitive, since they include even government employees' salaries and benefits.

The 1986 amendments to the FOIA generally reduced fees for information retrieval. In addition to significantly reduced fees for journalists, requests by non-commercial users involving fewer than 100 pages and two hours of search time are now free.[186]

Courts generally have viewed the fee reduction for news reporting liberally, and most regular news organizations should have little difficulty qualifying for it. Moreover, a key case, *National Security Archive v. Department of Defense*[187] broadly construed the groups and purposes for which a waiver or reduction of fees is appropriate.[188]

The plaintiff in *National Security Archive* was a firm that obtained documents from the government, culled information from the documents, and sold their documents to groups particularly interested in them, such as medical groups and other users. Although this could be viewed as a commercial enterprise, the court found that by thus publishing and disseminating information to the news media, the plaintiff qualified as a representative of the news media.[189] This was a realistic and practical

182. ADMINISTRATIVE CONFERENCE REPORT *supra* note 59, at 51.
183. 5 U.S.C. § 552(2)(4)(A)(ii)(II) (1988).
184. *Id.*
185. § 522(a)(4)(A)(ii)(III) (1988).
186. 5 U.S.C. §552(a)(4)(A)(iv)(II) (1988).
187. 880 F.2d 1381 (D.C. Cir. 1989), *cert. denied,* 110 S. Ct. 1478 (1990).
188. *Id.*
189. *Id.* at 1385-87.

holding given that specialized information conduits, such as the National Security Archive, perform valuable middleman services by assisting with information-gathering tasks that would often be impossible for a single reporter or news medium to handle on its own.

Moreover, in *National Security Archive*, the court defined the statutory language, "a representative of the news media," broadly, as follows: "[A] person or entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience."[190] This is an expansive definition, and one that is useful not only to the general news media, but also to free-lancers and small publications, such as newsletters. All information-gatherers and publishers who fit this broad definition are, under *National Security Archive*, entitled to the benefit of the FOIA fee reduction provision.

In addition to fee reduction for news reporting, FOIA provides for waiver of fees in cases where disclosure will benefit the public interest. Courts have held that this standard is a mandatory one, and when compliance with a request for documents will benefit the public at large, the agency may not refuse to waive fees.[191] However, the person who requests the waiver must do more than make bare, unsupported assertions that the research will meet the public interest test.[192]

7. Fees For Commercially Valuable Computer-Stored Information

Some of the most troublesome legal issues relating to access to government computerized information derive from the fact that some such information has great commercial value, while other government information has little or no commercial value. The computer revolution has made this distinction significant.

Prior to widespread use of computers, the commercial value of certain government information had relatively little impact upon the availability or ease of availability of that information to the public. Valuable commercial information (*e.g.*, Agriculture Department forecasts,

---

190. *Id.* at 1387.

191. Badhwar v. Air Force, 615 F. Supp. 698 (D.D.C. 1985); Long v. IRS, 566 F. Supp. 799 (W.D. Wash.); Diamond v. FBI, 548 F. Supp. 1158 (S.D.N.Y. 1982); Eudey v. CIA, 478 F. Supp. 1175 (D.D.C. 1979); *Ettinger v. FBI*, 596 F. Supp. 67 (D. Mass. 1984).

192. Burris v. CIA, 524 F. Supp. 448 (M.D. Tenn. 1981) (mere statement that requester was an author who planned to write a book did not meet public interest standard for waiver of fees); Blakely v. Department of Justice, 549 F. Supp. 362 (D.D.C. 1982), *aff'd*, 720 F.2d 215 (D.C. Cir. 1983) (more than impressive credentials and worthy intentions required).

government technical studies, and securities filings) was made available on paper and was equally available to commercial or non-commercial users.

Given the benefits and capabilities of computerized information, however, commercial users in many fields pressed for computerization of the government records they used. In some cases, the users even assisted with that computerization. For the most part, government agencies were eager to cooperate with the industries they served. Additionally, in the Reagan administration, the Office of Management and the Budget, in its Circular A-130[193] concerning information dissemination policies under the Paperwork Reduction Act, encouraged agencies to go the "privatization" route, and wherever possible, rely on the private sector for electronic dissemination of information.[194]

As a result, electronic dissemination of government information has proceeded most rapidly with respect to commercially valuable information.[195] Often that commercially valuable information is disseminated through commercial services and industry-connected channels, at fees geared to the standard commercial uses of the information. For example, the Securities and Exchange Commission (SEC) has used commercial services to disseminate news and security filings. These services have assisted in setting up the SEC's information dissemination systems, given the SEC free access to the new electronic data bases, and controlled the commercial electronic dissemination of those data bases charging standard commercial fees. As a result, public users can access these systems only by using one of a few public terminals in the SEC's reading rooms, or by paying the fees set by the commercial vendors.

The same kind of situation in which electronic dissemination of government information was established with the agency and commercial users in mind can be seen in other agencies. Even when the government itself maintains a database for the explicit purpose of making information widely available to the public, access to such databases can be much costlier than if the FOIA had been used.[196]

---

193. 50 Fed. Reg. 52,730 (1985) (final Dec. 12, 1985).

194. The controversy with respect to OMB's Circular A-130 and its emphasis on privatization of information dissemination policy is more fully discussed in T. MCINTOSH, *supra* note 34, at 19-33, and Berman, *The Right To Know: Public Access to Electronic Public Information,* 3 SOFTWARE L.J. 491 (1989).

195. *See Sellers of Government Data Thrive,* N.Y. Times, Dec. 26, 1991, at C2.

196. 1989 HOUSING HEARINGS *supra* note 30, at 460 (testimony of Joseph E. Clark, Deputy Director, National Technical Information Service). The case of the MEDLARS database, *infra* at notes 205-211 and accompanying text, provides further support for this position.

Hence, one result of the commercial emphasis in electronic dissemination of government information has been the development of a disparity between the "haves" and "have-nots" in electronic government information. Commercial interests can cause information to become quite expensive,[197] and even beyond the reach of students and other non-commercial researchers.[198]

A proposal by the Federal Maritime Commission to charge access fees for computerized government tariff data has highlighted this problem.[199] The agency's plan, endorsed by some government officials as a revenue-generating measure, would allow the agency to charge a fee each time the data are used, including each time the data are accessed through commercial services. Such a "user fee" would in effect give the agency a copyright-like royalty each time the information is used. The proposal is being strongly opposed by press and information industry groups.

As explained by one critic of this trend, Jerry J. Berman, Director of the ACLU's Information Technology Project:

> [A]s we observe [the] emerging world of electronic Government data bases, it's apparent that the benefits are not being equitably shared and widely shared by the public at large. The major users of electronic information are government, business, and the scientific community. Most of the major developments in the Federal Government of electronic data systems are occurring in the regulatory and business area, Trademark Office, Federal Communications Commission, Securities and Exchange Commission.
>
> [T]here are no similar developments at HUD, HHS, Justice Department, and even EPA has only one example, the TRI data base.[200]

Berman attributes this disparity to the emphasis in the Reagan administration on disseminating information in the least costly means, at the expense of maximizing public access to information.[201] This creates "a

197. *See* 1989 HOUSING HEARINGS *supra* note 30, at 198 (statement of Dr. Alan F. Westin, President, Reference Point Foundation, and Professor of Public Law and Government, Columbia University).

198. *1989 House Hearings, supra* note 30, at 313 (testimony of Nancy C. Kranich, director of public and administrative services, New York University Libraries, on behalf of the American Library Association); *Id.* at 368 (testimony of Nicholas E. Mercury, director information services, System Planning Corporation on behalf of the Special Library Ass'n).

199. *See* Newlin, *Communications: Whose Information Is It, Anyway,* NAT'L J. 1892 (July 27, 1991).

200. *1989 House Hearings, supra* note 30, at 105.

201. *Id.*

tendency . . . to encourage the development of electronic dissemination systems only when they're commercially viable, since commercial firms will not undertake the investment unless they have a market for their product."[202] This policy "exacerbates inequities between the information rich and the information poor."[203] Another long-time observer of the federal information policy, Alan Westin, Professor of Public Law and Government at Columbia University, notes that "the United States is in great danger of becoming an information autocracy," with business, science, government, and the media becoming the new "lords of the new information age" and the public at large becoming "information peasants."[204]

Troublesome issues may result not only from commercial involvement in information computerization and distribution, but also from government development of commercially valuable databases. Many government agencies have assembled information databases containing commercially valuable articles or data. Large access fees, which are designed with commercial users in mind, are often imposed for these databases.

In one instance, a litigant raised the conflict between the FOIA fee provisions and the higher fees set by the agency that developed a commercially valuable database.[205] The Department of Health and Human Services established the Medical Literature Analysis And Retrieval System (MEDLARS), a databank of articles on medical and scientific topics. The agency spent $10 million to prepare the database, and offered it on a subscription basis for $50,000. At that price, the agency had no takers. However, one firm made a FOIA request for the database, and offered to pay a $500 fee to cover the cost of copying and producing the MEDLARS computer tapes.[206] The agency resisted, holding out for its $50,000 charge. At the time, FOIA did not contain any exceptions to its normal fee schedule.[207]

The requester sued, and a decision was ultimately rendered by the U.S. Court of Appeals for the Ninth Circuit in *SDC Development Corp. v. Mathews*.[208] Judge (now Justice) Kennedy wrote the Ninth Circuit's decision in *SDC Development*, and upheld the agency's refusal to pro-

202. *Id.* at 106.

203. *Id.*

204. *1989 House Hearings, supra* note 30, at 179.

205. SDC Development Corp. v. Mathews, 542 F.2d 1116 (9th Cir. 1976).

206. *Id.* at 1118.

207. Subsequently, Congress amended FOIA to provide that FOIA fee provisions do not override statutes setting specific fees for specific records. 5 U.S.C. §552(a)(4)(A)(vi) (1988).

208. 542 F.2d 1116 (9th Cir. 1976).

duce the records.[209] The decision skirted entirely FOIA's applicability to the MEDLARS database, concluding that FOIA was primarily concerned with government records "which dealt with the structure, operation, and decision-making procedure[s] of the various government agencies."[210] Since in the MEDLARS case the agency "is seeking to protect not its information, but rather a system for delivering that information," disclosure under the FOIA would hamper rather than enhance the agency's information gathering and dissemination function, the court reasoned.[211]

This FOIA-avoidance reasoning of *SDC Development* is unpersuasive and has not been followed by other courts. Indeed, even Judge Kennedy's other FOIA decisions, *Long I*[212] and *Long IV*,[213] acknowledge that FOIA was meant to cover all government records, unless they are covered by specific exception.

The MEDLARS issue was ultimately resolved when Congress acted to allow override of FOIA fee provisions in cases of specific statutes setting fees for specific records.[214] Such exceptions to the standard FOIA fee provisions, however, must be monitored closely so that they are not misused. Special fee statutes, potentially, could seriously impair the news media's access to information, under the guise of a scheme that allows commercial users (who get great economic benefit from the information) and general interest media users (who do not), access to the information at equally high prices.[215]

The cost problems associated with commercial involvement in computerization and distribution of existing government records are different from the MEDLARS situation, in which an altogether new database was created. In cases of computerization of existing records, high commercial fees for information are not justifiable. In these cases, the fees represent not so much the essential fees that must be imposed if the database is to exist, (as with MEDLARS) as an attempt to shift the costs to users of upgrading government records — an upgrading that would be done in any event. If the SEC contracts with private parties for the EDGAR

209. *Id.* at 1121.

210. *Id.* at 1119.

211. *Id.* at 1120.

212. 596 F.2d 362 (9th Cir. 1979).

213. 825 F.2d 225 (9th Cir. 1987).

214. 5 U.S.C. § 552(a)(4)(A)(vi) (1988).

215. *Cf.* A. FRANCE, CRAINQUEBILLE (1901) ("The law, in its majestic equality, forbids the rich as well as the poor to sleep under bridges, to beg in the streets, and to steal bread," *quoted in,* Griffin v. Illinois, 351 U.S. 12, 23 (1956) (Frankurter, J. concurring)).

system, for example, the SEC is simply attempting to avoid some of the costs it would incur if it directly handled its own computerization. This process of involving commercial users in computerizing government records makes sense to the agency and some of its public constituents. The agency benefits from having its records computerized. Its commercial constituents also benefit from the computerization since some public users will pay access fees that will allow the agency to recoup its costs and make a profit. And, the users who can pay the commercial fees are also satisfied with this system.

But, this cozy picture of the benefits of privatization leaves out some key interests: those of public users, non-commercial users, and media users. Such users do not receive the same direct commercial benefit as industry information users, and thus, are not willing to pay the high fees geared to industry users. Because access to government information is a *right* of democracy, not a mere commodity of the free market, public users should not be forced to pay such artificially high fees, and should be permitted access at standard FOIA fees.

Although agencies will argue this is a burden, it really should not be. After all, agencies that accomplish computerization with the assistance of commercial firms are really, by that means, avoiding much of their own computerization costs (and usually shifting them on to their willing industry constituents). These savings will more than offset the additional costs of making the new computer records available to public and media users at standard, non-commercial FOIA fees.

8. Copyright Barriers to Access to Government Electronic Information

Under the Copyright Act of 1976, federal government information cannot be copyrighted.[216] However, in some cases, where commercial services supply government records to the public in computerized form, those services have been able to copyright certain aspects of the format, organization, and classification of information.

For example, Dialog, a commercially available data base which distributes the Agriculture Department's "Agribusiness" data base, claims copyright in the data base.[217] Although commercial services are justified in copyrighting the added value they give to government informa-

216. 17 U.S.C. §105 (1988).

217. *1989 House Hearings, supra* note 30, at 315-16 (testimony of Nancy C. Kranich, Director of Public and Administrative Services, New York University Libraries on behalf of American Libraries Ass'n).

tion,[218] it is often particularly difficult for users "to separate the proprietary component of a data base, which is copyrighted, from the public information, which is not copyrighted."[219] Hence, when a commercial service acts as an intermediary in the dissemination of government information to the public, researchers and other public users may be inhibited in downloading and analyzing data that is in the public domain.[220]

Software can be copyrighted and in many cases government agencies use privately developed (and copyrighted) software in their normal operations. In such cases, agencies may argue that they cannot disclose software without violating copyright protection. This argument would not apply in cases of software developed by the agency itself, since copyright protection would be unavailable for that federal government created material.[221] Private software, however, might be withheld on this ground, although the better view is that even privately copyrighted materials must be disclosed if the materials constitute non-exempt agency records.[222]

Privately developed software might have to be disclosed for other reasons, as well. If, for example, only a portion of the software need be disclosed, and only for a limited purpose, such disclosure might be allowable under the copyright law as "fair use."[223] Or, if the software itself was a specially developed product developed with extensive governmental input and actively used by the government agency as a substantive government record (such as a computer-driven drug smuggler profile), the record might, on the whole, be considered a non-copyrightable federal government work even though a private concern actually implemented it.

---

218. Callaghan v. Myers, 128 U.S. 617, 650 (1888).

219. *1989 House Hearings, supra* note 28, at 315-16.

220. *Id.* at 321.

221. 17 U.S.C. § 105 (1988). Even in these cases, however, agencies often still resist disclosure of software, claiming the software is an internal agency record exempt under FOIA. *E.g.*, Windels, Marx, Davies & Ives v. Department of Commerce, 576 F. Supp. 405, 411-14 (D.D.C. 1983); *see generally* T. MCINTOSH, *supra* note 34, at 102-103.

222. FOIA does not provide any specific exemption for copyrighted materials, and the Copyright Act does not operate through 5 U.S.C. §552(b)(3) (the catch-all exemption) to exempt disclosure of copyrighted materials. *See* National Parks and Conservation Ass'n v. Kleppe, 547 F.2d 673, 686 (D.C. Cir. 1976); M.A. Schapiro & Co. v. SEC, 339 F. Supp. 467, 470 (D.C. Cir. 1972); *see also* St. Paul's Benevolent Educational & Missionary Institute v. United States, 506 F. Supp. 822, 830 (N.D. Ga. 1980) (affirming an agency ruling).

223. 17 U.S.C. §107 (1988).

9. Agencies' Duties To Create or Preserve Electronic Records

One of the unique characteristics of electronic records is that, in many cases, large quantities of records can be deleted or destroyed quite easily. "A single keystroke does what a night or two nights of shredding or carrying out burn bags would otherwise do."[224]

This capability raises the issue of whether agencies should have a special duty to preserve electronic records. So far, relying on the analogy to paper records, courts have held that FOIA is a disclosure statute only and imposes no requirements on agencies regarding the creation or destruction of particular records.

In *Armstrong v. Bush*,[225] the Executive Director of the National Security Archive sought an order requiring White House officials to preserve the contents of the White House electronic mail system.[226] This system was used extensively by Oliver North and other White House officials involved in planning and carrying out the Reagan Administration diversion of proceeds from arms sales to Iran to the Contra movement in Nicaragua.[227] The National Security Archive argued that under both FOIA and two federal records preservation acts these records should be preserved, and not destroyed on the last day of the Reagan Administration as planned.[228]

The district court expressly refused to order the records preserved based on FOIA. The court held that FOIA "is a disclosure statute, and a disclosure statute only; it imposes no obligations and provides no guidelines for the creation or disposal of particular records."[229] The appeals court in *Armstrong* held that plaintiffs could obtain review only of the adequacy of agency procedures pursuant to the two records preservation acts and the adequacy of the agency's compliance with its own procedures.[230]

Once again, this result is probably correct under the literal interpretation of the statutes, but probably incorrect as a matter of sound policy.

---

224. *1989 House Hearings, supra* note 30, at 411-12 (testimony of Scott Armstrong, Director, National Security Archive).

225. 924 F.2d 282 (D.C. Cir. 1991).

226. 721 F. Supp. 343, 344 (D.D.C. 1989), *aff'd in part, rev'd in part,* 924 F.2d 282 (D.C. Cir. 1991).

227. *Id.* at 345, n.1.

228. *Id.* at 347.

229. *Id.* at 345.

230. 924 F.2d at 291-97. The particular statutes involved were the Federal Records Act of 1950, 44 U.S.C. § 2901 (1988) and the Presidential Records Act of 1978, 44 U.S.C. § 2201-09 (1988).

Although FOIA *is* primarily a disclosure statute, an effective disclosure policy must be supported by prohibitions against destruction of records for the purpose of defeating disclosure. This is particularly important given the nature of electronic mail systems, which are unlikely to be backed up by full or complete paper records. Therefore, anti-destruction laws are necessary in order to make disclosure effective. Of course, these laws can recognize legitimate agency needs, and permit routine and normal destruction while prohibiting wholesale and unwarranted destruction of records.

Notably, while records acts do not provide any *legal* barrier to destruction of computer records, the nature of computer records provides some *practical* obstacles to their destruction. Operators often believe they have deleted computer-stored documents when they have not. In most systems, the "delete" command merely instructs the computer to delete the document from file indexes; the information remains on the tape or disk until eventually erased when that storage space is needed for new data. In several recent cases, including the Iran-Contra prosecution of Oliver North and the 1991 Los Angeles police brutality investigation, investigators have been able to retrieve electronic messages thought by the original operators to have been deleted. Hence, an agency's use of computer records may in some cases effectively expand the quantity of records that are preserved. Courts, therefore, may soon confront the issue of whether an FOIA requester is entitled to computer records thought to have been deleted, but actually still in existence and capable of retrieval.

C. *Non-Statutory Access Rights*

Although statutory rights of access, such as FOIA, are the prime avenues of access to government information, they are not the only ones. Particularly with respect to the judicial branch, common law and first amendment rights of access may also exist. This access right also needs policies specifically recognizing the nature of electronic records and the needs of parties to have full and effective access.

The first amendment and common law right of access to judicial proceedings is now well recognized. This right includes the right of the press and the public to attend trials,[231] a prohibition against mandatory closure of judicial proceedings,[232] the right to attend voir dire,[233] and

231. Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980).
232. Globe Newspaper Co. v. Superior Court, 457 U.S. 596 (1982).
233. Press-Enterprise Co. v. Superior Court, 464 U.S. 501 (1984).

the right to attend preliminary hearings in criminal cases.[234] This right of access to criminal proceedings generally extends to all proceedings in which there is a history of openness and a need for access to inform the public about these important governmental proceedings.[235]

Moreover, the right of access to judicial proceedings has been extended in many cases beyond the traditional right to attend a trial in open court. It embraces a right of access to all sorts of things that did not exist in common law, including pre-sentence investigatory reports,[236] probable cause affidavits in criminal cases,[237] videotapes and audio tapes used at trial,[238] an airplane crash site controlled by the National Transportation Safety Board,[239] audiovisual information at a medical examiner's inquest,[240] television representatives in White House press "pool,"[241] and many other non-traditional areas.

In many areas of government, particularly involving the judicial branch, this common law right of access may provide a legal rationale for disclosure of electronic records equal to or stronger than FOIA. For example, electronic court records may be viewed as the electronic equivalent of paper records which have long been available to the press and the public. In this case, courts should be required to produce the records in electronic form, just as executive agencies have been required to produce their electronic records under FOIA. Similarly, discovery material that is susceptible to inspection by the public under the first amendment and common law right of access should be available in electronic form when it is maintained in that form. This could be a major boon to the press in class action, mass disaster, environmental, toxic tort, civil rights, and similar cases where newsworthy information is contained in discovery materials that have been produced or assembled in electronic form.

In addition, although the first amendment or common law right of

---

234. Press-Enterprise Co. v. Superior Court, 478 U.S. 1 (1986).

235. *Id.* at 8-9.

236. Seattle Times v. United States District Court, 845 F.2d 1513, 15 Media L. Rptr. 1273 (9th Cir. 1988).

237. Vermont v. Tallman, 537 A.2d 422, 15 Media L. Rptr. 1344 (Vt. 1987) (right attaches only after the affidavit is viewed by the court).

238. *In re* Application of National Broadcasting Co., 648 F.2d 814 (3rd Cir. 1981).

239. Westinghouse Broadcasting Co. v. National Transportation Safety Board, 8 Media L. Rptr. 1177 (BNA) (D. Mass. 1982).

240. Wisconsin Freedom of Information Council v. Hill, 7 Media L. Rptr. 2061 (BNA) (Wisc. Cir. Ct. 1981).

241. Cable News Network v. ABC, 518 F. Supp. 1239 (N.D. Ga. 1981) (attempt by the White House to exclude television media from such events unsuccessful).

access has primarily been developed in connection with judicial records, it may be equally applicable to other government records which have been traditionally open to the public, such as motor vehicle records, vital statistics, election records, real estate assessment records, and similar records. Reporters and other researchers may find the common law right of access a weighty tool for disclosure of electronic records in these areas.

VI. POLICIES AND CONCERNS RELATING TO ACCESS TO COMPUTER RECORDS

Cases involving new technology, like "great cases," can make bad law.[242] In computer record access cases, both reasoning and outcomes may be affected by stated and unstated judicial assumptions regarding the appropriate policies governing computer records and their use. These assumptions and policies deserve to be fully scrutinized and discussed.

A. *General Fears of New Technology*

Courts often address new technology arguments by assuming that the effect of the new technology will be qualitatively different, and often severely detrimental. Many judges feared, for example, that allowing television in the courtrooms would not only intrude, but also dramatically change both courtroom conduct by sensationalizing it, and public perception and understanding of courts by trivializing it.[243] The experience of experimental cameras-in-the-courtroom programs eased these fears when it became apparent that courtroom conduct and public understanding actually improved with un-intrusive television coverage.[244] Moreover, a focus on potential misuse of information is unwarranted because it is well established that, in evaluating access laws and their exemptions, courts should not inquire into the requester's purpose.[245]

B. *Fear of Unfair Advantages*

Calculators, typewriters, computers and other machines that stream-

242. Northern Securities Co. v. United States, 193 U.S. 197, 400 (1904) (Holmes, J., dissenting) ("Great cases like hard cases make bad law.").

243. Sheppard v. Maxwell, 384 U.S. 333 (1966).

244. Chandler v. Florida, 449 U.S. 560 (1981).

245. State Employees Association v. Dep't. of Management and Budget, 404 N.W.2d 606, 614 (Mich. 1987). *See also* Kronman, *The Privacy Exemption to the Freedom of Information Act,* 9 J. LEGAL STUD. 727, 743 (1980); Davis, *The Information Act: A Preliminary Analysis,* 34 U. CHI. L. REV. 761, 765-66 (1967).

line and ease mechanical tasks often seem initially to give unfair advantage to those who use them. Some courts have expressed concern that allowing access to data banks that were organized at considerable effort and cost gives the accessing party a "free ride."[246] Experience and understanding of the new technology are necessary to overcome this fear.

C. *The Print Analogy*

New communications technologies[247] are usually analyzed, at least initially, by analogy to the familiar print medium. Different regulatory approaches (*e.g.*, tighter government controls on broadcasting) are based on perceived differences (*e.g.*, spectrum scarcity) from the bench-mark print medium. Hence, legal doctrines based on experience with the print media are almost always the starting point of analysis.[248] While the analogy generally is useful for application of first amendment protections to new technologies, over-reliance on the analogy tends to limit the protections for new technologies to those characteristics in which they are most like print.[249] Therefore, often it is better to initiate such analysis using principles such as the need for meaningful access to information and the impropriety of government controls over information or expression.

D. *Privacy Concerns and Fear of Improper Use*

One of the greatest concerns about computer information is that it will allow or cause invasions of personal privacy. The concern, in essence, is that the power and efficiency of new technology (computers) will have a synergetic effect on information. A computer can take one seemingly innocuous fact in one database and match it with an equally innocuous fact in another database thereby producing a piece of highly significant information. Fearing such uses, privacy advocates often take extreme positions, such as labeling these uses as improper or urging that all personal information should be kept out of reach of the public.[250]

---

246. SDC Development Corp. v. Mathews, 542 F.2d 1116, 1120 (1976).

247. Such new technologies include: motion pictures, radio, and television; along with new and television technologies like pay-per-view, cable, direct broadcast satellite services, and videotext.

248. *See* POOL, TECHNOLOGIES OF FREEDOM 1-10, 116-19, 244-51 (1983).

249. *Id.* at 149-50.

250. For example, in Schwaner v. Department of the Air Force, 698 F. Supp. 4 (D.D.C. 1988), *rev'd* 898 F.2d 793 (D.C. Cir. 1990), the district court turned down an FOIA applicant's request for a computer print-out of certain Air Force personnel stationed at a particular base. The district court held the information to be unrelated to significant public interests, based on the assumption that the usefulness of the

A good example of this view of computer information as qualitatively different is found in the Michigan Supreme Court's decision in *Kestenbaum v. Michigan State University*.[251] In the course of upholding an agency's refusal to release information on magnetic tape that had already been published in printed form, the court plurality proclaimed that "the computer era . . . is fraught with potential dangers to our notions of individual autonomy" and there can be no doubt that computers have led to "an ever-increasing erosion of personal privacy."[252] Reasoning from these abstract and fearful prophecies, the court plurality readily distinguished between the release of information in printed and electronic form — thus basing legal doctrine solely on generalized fears of new technology. Justice James L. Ryan, writing for the dissenters, dismissed the plurality's fear that disclosure of electronically stored names and addresses was a serious and qualitatively new threat to personal liberties:

> It is hard to take seriously the assertion that the advent of the modern computer era poses a significant threat to the secrecy of one's name and address. In the days of our forefathers, one's name and address

---

information to some commercial users was outweighed by unspecified "normal considerations of individual privacy" for the government employees:

> If [the public interest in the information] is accepted, then as electronic filing expands to create ever larger reservoirs of miscellaneous personal data, a wealth of personal information will be placed at hazard and normal considerations of individual privacy will be jeopardized. In order to target its mailings and phone calls in ever more precise and intrusive ways using the highly sophisticated tactics of modern marketing, the creative FOIA requester will tap into the vast data-banks of government computers. Perhaps, after obtaining data from FOIA requests, they will sell their lists to other merchants interested in the military or civil service markets. While this threat to personal liberties is far from fatal, the government should not be put to the cumulating expense of processing the requests of merchants, nor should FOIA be interpreted as requiring this intrusion of the privacy of government employees.

Id. at 6. The underlying rationale of this passage is unrelated to computers and simply reflects a feeling — directly contrary to the policy of the FOIA — that disclosure of non-exempt government information may somehow be harmful or "threatening." The circuit court reversed, holding that the information clearly was not exempt. Nevertheless, the appeals court gratuitously noted its disapproval for the commercial objectives of the requester: "Repugnant as it may seem to order disclosure to an insurance agent who seeks only a pool in which to fish for commissions, . . . only by allowing Schwaner's claim can we keep exemption 2 [of FOIA] within its proper confines." Schwaner v. Air Force, 898 F.2d 793, 798 (D.C. Cir. 1990).

251. 327 N.W.2d 783 (1981).

252. *Id.* at 789.

> were a matter of general public knowledge. An individual's home may still be a "castle" into which "not even the king may enter," . . . ; but nothing prevents the king or anyone else from telling others whose castle it is, particularly when the castle-dweller himself has voluntarily released that information to the general public.[253]

Justice Ryan also noted that the plurality's fear of the potential misuse of computer-stored information was an inappropriate basis for a distinction between computer and non-computer information, since every bit of information released under FOIA, electronic or non-electronic, has the potential for misuse or abuse.[254]

As Justice Ryan's analysis explains, computers have not really contributed anything new in substance. This same kind of gathering, sorting, and matching of information can be done without a computer. Oedipus never used a computer to learn that he had killed his father and married his mother. All it took was a dogged pursuit of the truth. The difference is that a computer conducts information gathering, sorting and matching with incredible speed and relative ease. The opportunities for useful analysis are enhanced. This change is one of degree, not kind.[255] The computer does not change the way we look at informa-

---

253. *Id.* at 796 n.18.

254. *Id.* at 799 n.26.

255. The parallels with the printing press are striking. Books existed before the invention of movable type. What the printing press did was to change the speed and ease with which books could be created. And, once books became generally available, government and the church became concerned with the "misuse" of this invention. It became easy to spread "dangerous" ideas that might cause confusion and anarchy. Censorship, a sport that enjoyed amateur standing in the Greek and Roman civilizations, achieved professional stature after Gutenberg. Ultimately, however, it became clear that censorship was a far worse cure than the ill it was intended to prevent. It was also futile; censorship, in essence, is an attempt to repeal change.

As Justice Ryan explained in his *Kestenbaum* dissent, it makes little sense to criticize information in a certain form merely because it is *useful:*

> [T]o equate usefulness with intrusiveness is to turn the FOIA on its head. A public body should not be allowed to thwart legitimate uses of public information by releasing the information in a format difficult or expensive to use. Releasing the requested names and addresses in handwritten form would make it even more difficult to read and use the information; surely that does not mean that a person requesting a printed copy can be given a handwritten copy because the latter is less usable and therefore less "intrusive"? Following that rationale would encourage a public body to meet its FOIA requests with the response that the actual public document or "writing" cannot be copied, but the agency will gladly produce the same "information" in a "less intrusive" form such as a foreign language, Morse Code, or hieroglyphics.

tion. It only changes the time it takes to do the analysis.

Oddly, one of the major objections often made by opponents of electronic release of government files is that files containing address lists can be used for commercial mailings, often disparagingly called "junk mail." One must question the extent to which dislike of junk mail should determine information access policy. Several courts that have specifically addressed this point have concluded that fear of junk mail should not override the right of access to government information.[256] Moreover, to the extent unsolicited mailings or other information disclosed under access laws present serious concerns, these concerns can be dealt with by less restrictive means than a total ban on disclosing the information.[257]

Indeed, although the talismanic word "privacy" seems to strike a natural chord of sympathy in most persons, few have any but the vaguest fears regarding misuse of information. For example, many citizens instinctively rebel at the thought of their drivers' license records being public. But such records have long been public in most states, and there are few documented instances of misuse. Moreover, hearings have shown that the few inchoate fears of misuse of these records are dwarfed by their many legitimate uses.[258]

Journalists and others who need access to government computer

---

327 N.W.2d at 802.

256. Disabled Officers Ass'n v. Rumsfeld, 428 F. Supp. 454 (D.D.C. 1977) (upholding release of list of names and addresses of disabled officers, and rejecting objection that requester would use list for unsolicited mailings); Lamont v. Commissioner of Motor Vehicles, 269 F. Supp. 880, 883 (S.D.N.Y.), *aff'd,* 386 F.2d 449 (2d Cir. 1967), *cert. denied,* 391 U.S. 515 (1968) (refusing to enjoin state from selling a list of automobile owners). "The short, though regular, journey from mail box to trash can . . . is an acceptable burden, at least so far as the Constitution is concerned." 269 F. Supp. at 883.

257. For example, if unsolicited mailings of a sexually explicit nature are the feared result, those who do not wish to receive the mailings can give notice under 39 U.S.C. § 3008 (1988), thereby prohibiting future mailings. In other situations, notice or "opt-out" opportunities are afforded to persons listed in advance of the disclosure of the lists. *See* Kestenbaum v. Michigan State University, 327 N.W.2d 783, 800 (Mich. 1981) (Ryan, J., dissenting) (explaining methods by which university students could prevent release of their names and consequent receipt of unsolicited junk mail).

258. For example, in hearings before the Kansas State Senate in March 1992, groups testifying against a bill that would have made drivers' license records exempt from disclosure included a state social service agency (which had been using the records to track down fathers delinquent in child support payments), a state utility (which used the records to assess the driving records of its prospective and current drivers), as well as traditional information-dependent groups such as private investigators, trial lawyers, researchers, and directory publishers.

records must allay concerns regarding improper use and demonstrate to policy makers that a similar potential for abuse existed even before computers. Additionally, responsible researchers should attempt to show that adequate safeguards against misuse exist, and that they will act responsibly.

E. *Benefits of Access*

While courts and legislators are often receptive to fears of what may occur with full access to computer records (i.e. privacy invasions), it is equally important to consider what may happen if access is *not* allowed.[259]

If information is denied to the press and the public because of privacy, or restricted in *how it is disclosed* to the press and public (but not *how it is maintained* by the government), the government becomes the sole possessor of information and the means of effectively using it. That is, government controls not only the information, but also the means of analysis. This is hardly an ideal result from the standpoint of civil libertarians. The press, at a disadvantage in investigating the government before the advent of computers, will be completely overshadowed. Government will have both the exclusive use of "private" information and the computers to manipulate that information.

If the government, for example, reports that its computer analysis indicates that doctors are not abusing Medicare, who can check? Not the press, if the press cannot obtain Medicare reimbursement information, or cannot obtain it in a form that permits effective analysis. There is no public interest served in keeping secret the amount paid to doctors who serve in the clinic. In fact, just the opposite is true. Unless the public knows how its money is being spent, public accountability is lost.

A vigorous public debate is essential to a democratic society, as many courts and commentators have long acknowledged. So is a *well*

---

259. In his dissent in *Kestenbaum,* Justice Ryan noted that the court's plurality ruling, which stressed fears of potential misuse of computer-stored information, ignored the *benefits* of disclosing information in electronic form:

> By failing to mention beneficial uses to which *some* members of the public might put the information, and emphasizing the dangers of a "computerized dossier" that *some* members of the public might create, our brother's conclusion is foreordained . . .
>
> We think the public benefits of voter registration and political campaigning contemplated in this case clearly outweigh any minimal invasion of privacy. The fundamental importance of voter registration and political communication in a democracy cannot be overestimated.

327 N.W.2d at 799-800 (footnotes omitted).

informed public. Overemphasis on privacy can give individuals or groups a tool to stifle information essential to public discussion and debate.

VII. CONCLUSION

Control and release of government computer-stored information is too important an issue to be left to the haphazard pattern of statutes and case law that has governed it to date. In addition to the inconsistencies and uncertainties in the law as it has developed so far, many of the existing decisions overemphasize general fears of the new electronic information-storage technology, and understate or ignore the great potential benefits of access to such information to the public.[260]

Many states and the federal government are currently reviewing their records laws to update them to take account of the widespread use of computer records. It will take more than a few amendments recognizing coverage of electronic records, however, to adequately update access laws. New information disclosure laws and policies directly governing access to computer-stored information need to be developed.[261] And, not only information specialists, but also persons cognizant of the usefulness of that information to the press and the public need to participate in the development of these laws and policies.

---

260. Though government has been relatively quick to take to the benefits of computerized information, government laws and policies have been slow to realize the impact of electronically maintained government information on access laws. As Jerry J. Berman, Director of the American Civil Liberties Union's information technology project, has observed:

> Enacted prior to extensive government computerization and before the PC revolution brought computing power to most citizens, federal information laws from the Printing Act to the Freedom of Information Act to the Paperwork Reduction Act, established a public right of access to printed government information, including print outs from government computer files, but uncertain public access rights to electronic public information.
>
> This uncertain status, instead of enhancing the public's right to know through the use of new technology is instead creating new barriers to public access, new inequities and new dislocations.

1989 House Hearings, supra note 30, at 104.

261. As Jane E. Kirtley, Executive Director of the Reporters' Committee for Freedom of the Press, stated,

> [E]lectronic data bases are in fact the file cabinets of the present as well as the future. If meaningful rights of access to government information are to be maintained, it is essential that workable policies for insuring requestor retrieval of electronically stored information be established. The access has to be timely, not prohibitive in cost, and it has to be user friendly.

1989 House Hearings, supra note 30, at 35.

A bill submitted by Senator Patrick Leahy of Vermont in the 102nd Congress, the proposed Electronic Freedom of Information Improvement Act of 1991, tackles some of the most pressing problems.[262] It would explicitly put to rest the discredited but still influential *Dismukes* precedent, by specifically requiring agencies (a) to make records available in the requester's format of choice, if records exist in that format, and (b) to "make reasonable efforts to provide records in an electronic form requested by any person, even where such records are not usually maintained in that form."[263] The bill would include electronic information of all sorts in the FOIA's definition of "record" and would address the "programming" issue by defining "search" broadly as "a manual or automated examination to locate records."[264] It also would specifically provide for computer redaction of exempt information, although it does not address the issue of data rearrangement.[265] Finally, the bill would also require agencies to publish indexes of information stored electronically, and would establish incentives and penalties designed to avoid delays in processing FOIA requests.[266]

This bill as introduced takes a big and long overdue first step at addressing the inadequacies of current access law with respect to computer records. To truly bring access laws into the computer age, however, lawmakers will have to address as well such important and recurring issues as data rearrangement, reasonable fees, and the preservation of electronic records.

In developing standards that specifically address computer records, as amendments to the federal FOIA and as state information access laws, the following points should be included:

- Computer records should be explicitly recognized as subject to disclosure to the same extent as paper, microform, and other more traditional documentary records.
- Access to computer records should be permitted in the most efficient and direct manner. Just as government agencies are not allowed to ignore the photocopy machine and insist that the public copy documents by hand, so also must they be required to produce electronic records in suitable convenient electronic form.
- Search responsibilities with respect to electronic records should

262. S. 1940, 102d Cong., 1st Sess. (1991); *See* 137 Cong. Rec. 16, 213-44 (1991) (statements of Sen. Leahy and Sen. Brown).

263. S. 1940, 102d Cong., 1st Sess. § 3 (1991).

264. *Id.* § 7.

265. *Id.* § 6.

266. *Id.* §§ 3, 4.

include all reasonable and ordinary means of searching electronic records, including preparation and modification of search programs. In particular, agencies should be required to utilize searching capabilities and other computer programming techniques to delete or redact confidential or exempt information, and hence allow greater disclosure of non-exempt information.

- Fees for access to computer records should be reasonable. Reasonable fees could be based on actual marginal costs to the agency, subject to appropriate statutory fee waivers or reductions.
- Fees should *not* be determined based on the value to commercial users, or calculations designed to recover capital costs of government computerization.
- Arrangements between commercial information agencies and government agencies should not be allowed to interfere with or restrict the agencies' responsibilities under access laws to produce information directly to the public in the most convenient format.
- Computer capabilities for rearranging data to avoid disclosure of sensitive and confidential material should be fully available to the press and public, under provisions for appropriate allocation of cost and programming responsibility. That is, data rearrangement such as those urged by the plaintiff in *Yaeger v. Drug Enforcement Administration* should be permitted, but with the direct costs involved placed on the requester, since those techniques go beyond the agency's normal responsibility to prepare search programming.
- Adequate provisions should be made for requiring preservation of electronic information and data communications systems such as electronic mail, so that such information is not lost to researchers and interested public users.

Codifying these policies in FOIA will not end all problems in this field. As technology advances, new hitherto unforeseen issues will undoubtedly arise and require even more changes. But the time is overdue for a bold first step to bring information access laws into step with modern technological realities.