California Western Law Review

Volume 39 | Number 2 Article 8

2003

Will the Privacy Act of 1974 Still Hold Up in 2004? How Advancing Technology Has Created a Need for Change in the "System of Records" Analysis

Julianne M. Sullivan

WILL THE PRIVACY ACT OF 1974 STILL HOLD UP IN 2004? HOW ADVANCING TECHNOLOGY HAS CREATED A NEED FOR CHANGE IN THE "SYSTEM OF RECORDS" ANALYSIS

INTRODUCTION

The notion of privacy is one central to the values and principles of the United States.[1] Ever since the publication of the famous law review article by Brandeis and Warren in 1890,[2] the courts have been cluttered with cases attempting to define the reaches and the limits of privacy guarantees.[3] In their article, Brandeis and Warren laid out the principle of privacy law, particularly with respect to privacy torts, and since then, the notion has been all but unstoppable.[4] The article was a reaction to the times: to the advent of tabloid journalism,[5] to attacks of the press, and some say, to the prying eyes of journalists into the private lives of the authors.[6] Regardless of the authors' motivations, their article was the tremor that started the avalanche of privacy claims, defenses, and disagreements.

At the same time privacy notions developed in the public's mind, a certain lack of familiarity to the everyday interactions between people and or-

1. Although not expressly guaranteed by the U.S. Constitution, the Supreme Court has held that privacy is implied in the Bill of Rights, because the "penumbras" of the various amendments create "zones of privacy." Griswold v. Connecticut, 381 U.S. 479, 484 (1965). Along with the ideals of individual freedoms and the interests of the founders of this country in independence, the notion of privacy is essentially the desire of citizens to be left alone. At common law, privacy has been broken down into four main categories: public disclosure, intrusion, appropriation, and false light. The Privacy Act of 1974 deals primarily with the first and second categories. The Privacy Act of 1974, 5 U.S.C. § 552a (2000).

2. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

3. *See, e.g.*, *Griswold*, 381 U.S. at 479; Galella v. Onassis, 487 F.2d 986 (2nd Cir. 1973); Cantrell v. Forest City Publ'g Co., 419 U.S. 245 (1974).

4. Consider the escalation in privacy tort suits throughout the twentieth century and the courts' increasing acceptance of them, along with the wider recognition that there are boundaries the press should not be allowed to cross. Of course, this might not have become an issue if the press had not *tried* to cross more boundaries. In the past, the press respected the private lives of public officials, such as President Roosevelt's confinement to a wheelchair, and did not attempt to publish intrusive articles. Today, even the lives of private citizens are at risk of exposure if they happen to find themselves involved in some public event or scandal.

5. Amazingly, tabloid journalism had already gotten its start by the end of the nineteenth century. While the articles were hardly on par with the bizarre stories seen in our supermarket check out lines today, they did provide entertainment with society articles and similar pieces.

6. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

ganizations also arose. No longer can one count on being remembered by local shopkeepers as a recent or even a long-time customer.[7] As society and the federal government have grown in size and complexity, the number of records maintained on individuals has also grown.[8] Like many things in today's world, the quantity and detail of information the government maintains on its citizens would astound someone from the last century, as it would most likely amaze citizens of today, too.

The idea of statutory protection for citizens against the records maintained by the government grew out of this increase in recordkeeping.[9] Yet even as Congress has attempted to provide protection and assurances for citizens, technology has advanced to outstrip its efforts. Consider the remarkable advances in data storage just in the past ten years. What used to fill tape drives now fits on the laptops seen in every classroom and coffee shop across the country.[10] So how are members of the public to know what files the government has on them? How are individuals to ensure that their records are correct? How are agencies to know what files they may or may not disclose and who they must allow to access those files? These are the very concerns that the Privacy Act of 1974 was intended to address.[11] Yet, as will become clear in this Comment, there are significant problems with at least one aspect of this Act, and thus problems with answering these questions, as the Act is applied today.

The first section of this Comment will provide background about the Act, the historical and social setting in which it was written, and the intentions of the Congress that passed it. Background will also be provided on the evolution of the problems with the system of records analysis. It will then go on to provide the current state of the analysis and the precedent set by the

---

7. Today, with online ordering and delivery services available for everything from groceries to books and movies to gourmet dinners, a person could go months without even setting foot inside a store. How inconceivable that would have been just fifty years ago, or even twenty. Though local shops do still exist, the small towns where the owners knew everyone in the neighborhood are few—and thus we are left with the ever-increasing computerization of our lives and our life stories.

8. Consider how many government forms every citizen fills out: tax returns, vehicle registrations, voter registrations, census surveys; then add all of the specialized forms: patent applications, farm quota assessments, employment applications. The number of forms has gotten so large that most government agencies have their forms identified by a serial number or form code, printed on each form so that it can later be identified and matched with its intended purpose. The next time you fill out a government form look in the corner for the official Government Printing Office (GPO) number.

9. OFFICE OF INFO. AND PRIVACY, FREEDOM OF INFORMATION ACT GUIDE & PRIVACY ACT OVERVIEW 779 (2002).

10. Just ten years ago, 40 gigabytes (GB) of data on a single personal computer's hard drive was unthinkable. Six years ago, a two GB hard drive was considered perfectly reasonable. Today, two GB can be filled by just the operating system and pre-installed software. Not to mention the increases in processing speeds and the advent of Ethernet as a replacement for modem speeds.

11. The Privacy Act of 1974, 5 U.S.C. § 552a (2000).

D.C. Circuit Court in *Henke v. United States Department of Commerce*.[12] The second section will introduce the conflict that has arisen between the current interpretations of the Privacy Act and the advances in technology. Part III will illustrate the sources of the problem with the system of records analysis that developed as a result of the decision in *Henke*. The fourth section of this Comment will analyze the problem and discuss two possible avenues that can be taken in response to the conflict. It will consider the possible repercussions of either approach, for although the current Act may have flaws, any solution may create other problems that far exceed those solved. In conclusion, this Comment suggests that reforms must be undertaken. While they should be done cautiously, they must be done without delay, for to wait is to find ourselves falling further and further behind the onslaught of technology.

I. BACKGROUND

The Privacy Act must be considered in light of its historical basis, just as the problems it currently faces cannot be understood without an appreciation of the technological advances in recent years, and the interpretations of the Privacy Act by courts. Specifically, interpretations of the term "system of records," by which courts responded to those technological changes, are central to understanding the different types of problems encountered between the Privacy Act and advancing technology.

A. Brief History of the Privacy Act

The Privacy Act of 1974 was passed on December 31, 1974, and went into effect on September 27, 1975.[13] It serves the dual purpose of protecting individuals' private information from disclosure by those government agencies who have collected it,[14] and of enabling individuals to determine what information has been collected and to verify its accuracy.[15] The Act also provides a mechanism for individuals to challenge their records and request corrections of the data stored by an agency,[16] and a remedy against those who do not comply.[17] The Privacy Act specifically applies to government agencies, such as the Executive branch, the military, and federal depart-

12. Henke v. United States Dep't of Commerce, 83 F.3d 1453 (D.C. Cir. 1996).

13. The Privacy Act of 1974, 5 U.S.C. § 552a (2000). Although this may seem like a long delay since the original 1890 article, the primary focus of privacy law in early part of the century related more to privacy torts between individuals. It was not until later, when the volume of information stored by the government increased, that privacy concerns of this kind arose.

14. *Id.* § 552a(b).

15. *Id.* § 552a(d), (f).

16. *Id.* § 552a(d).

17. *Id.* § 552a(g), (i).

ments.[18] Similar statutes have been passed that cover other types of organizations, providing additional rights and remedies.[19]

Because the Privacy Act was passed quickly, and at the end of the ninety-third Congress, its legislative history has not always been helpful in determining the original intent of the legislature or in interpreting the language.[20] The bills passed by the House and the Senate were not identical, and no conference committee was convened, therefore there is no official committee report and the early Congressional reports do not necessarily correspond to the statute that was actually enacted.[21] The Act has been amended several times since its original enactment, but none of the amendments have directly addressed the changes in technology that have occurred since 1974.[22] The changes have been dramatic in the way information is now stored and retrieved,[23] which plays a significant role in the classification of records under the Privacy Act.[24] In a movement away from the paper or microfiche systems of the past, electronic storage of data has become the widespread means of keeping records.[25]

A basic requirement to show that the Privacy Act applies is that the records are contained within a "system of records."[26] Under the Act, an agency will only grant an individual access to records which are stored in a "system of records."[27] All government agencies are required to report the systems of records that they maintain and to describe in detail the information collected, the purpose for which it was collected, and the person or office to which re-

18. *Id.* § 552a(a)(1), (e), (f).

19. *See, e.g.*, Family Education Rights and Privacy Act (FERPA) of 1974, 20 U.S.C. § 1232 (2000); Electronic Communications Privacy Act (Privacy Act of 1986), 18 U.S.C. §§ 2510-2521 (2000).

20. OFFICE OF INFO. AND PRIVACY, FREEDOM OF INFORMATION ACT GUIDE & PRIVACY ACT OVERVIEW 777 (2002).

21. *Id.*

22. 5 U.S.C.S. § 552a (Bender 2002).

23. Printed or handwritten data that once filled volumes can now be stored on a microchip. Entire encyclopedias are stored on just a few CD-ROMs. Computer search engines can find a single use of a word within a file. All of these advancements make data storage easier, smaller, and faster, but they also make the Privacy Act harder to use.

24. *See* Henke v. United States Dep't of Commerce, 83 F.3d 1453 (D.C. Cir. 1996); Baker v. Dep't of the Navy, 814 F.2d 1381 (9th Cir. 1987).

25. OFFICE OF INFO. AND PRIVACY, FREEDOM OF INFORMATION ACT GUIDE & PRIVACY ACT OVERVIEW 779 (Pamela Maida ed., 2002).

26. *See* 5 U.S.C. 552a(b), (d), (f); *see also* Office and Management and Budget's (OMB) Privacy Act Guidelines, 40 Fed. Reg. 56,741, 56,741-43 (1975).

27. 5 U.S.C. § 552a(d) (2000). It is interesting to note that in contrast to the policies of the Freedom of Information Act (FOIA), the sister to the Privacy Act, here only the individuals about whom the records are kept may access those records. However, under FOIA, members of the general public may request documents, but only limited information must be released and substantial sections may be redacted based on the privileges allowed. The Freedom of Information Act, 5 U.S.C. § 552 (2000). No such privileges exist under the Privacy Act, thus when someone is entitled to access to his record, he would typically be allowed access to the *entire* record, much to the dismay of many agencies.

quests for records should be sent.[28] Agencies are also required to go through an approval process prior to establishing a new system of records. All of the information about each system of records is then published by the Office of Management and Budget (OMB) on paper in the Federal Register as well as on the Federal Register website.[29] Thus the process appears to be quite clear, until you consider the problem of determining which groups of records in which agencies qualify as "systems of records."

The term "system of records" is an artificial distinction, legislatively created to identify those groups of records to which the Privacy Act applies, and those to which it does not apply.[30] According to the Privacy Act: "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[31] The "system of records" analysis involves examining the actual retrieval methods used by an agency to determine if the records fit into the definition, that is, if the records are retrieved by an individual's name or identifying code (such as a Social Security number).[32] However, with today's databases, this analysis is breaking down. Agencies have the capability of searching based on virtually any word or number contained in their systems.[33] This capability leads to the question of how many actual retrievals of information using someone's name are sufficient to create a system of records.[34] It is here that the Privacy Act begins to show that it has not kept up with technology and where it is most in need of clarification.

B. Current System of Records Analysis

1. Interpretation in Henke v. United States Department of Commerce

Henke v. United States Department of Commerce is the leading authority on the system of records analysis,[35] and has been widely accepted by

28. 5 U.S.C. § 552a(e) (2000).

29. Privacy Act Issuances, *at* http://www.access.gpo.gov/su_docs/aces/ PrivacyAct.shtml (last visited Jan. 29, 2003).

30. The definition provided by the Privacy Act is not based on the ordinary, plain meaning of the words "system of records," but is in fact a very specific type of system, with very particular rules. This distinction likely arose out of the need to create some kind of distinction between groups of records that should be accessible and those that should not.

31. 5 U.S.C. § 552a(a)(5) (2000).

32. *Henke*, 83 F.3d at 1459-60.

33. All one has to do is press SHIFT-F on most computers, regardless of the program, and a dialog box for a word search will appear. Depending on the sophistication of the program, different parameters can be set, but the basic search will simply look at each word in the document, compare it to the one typed into the search field, and return the matches.

34. *Cf. Henke*, 83 F.3d at 1461 (noting that when records are compiled for investigatory purposes, even a few retrievals might be sufficient to create a system of records).

35. *Id.*

courts.[36] This case reinforced a distinction between the capability to retrieve records by individuals' names and the practice of actual retrieval by names that was set out in the OMB Guidelines.[37] The appellant, a scientist, president, and co-owner of a company that develops earthquake technology, claimed that the Privacy Act had been violated when she was denied access to records from the U.S. Department of Commerce (DOC) and the National Science Foundation (NSF).[38] The records had been submitted by her company in an application to the DOC's Advanced Technology Program (ATP) for a grant, which was denied.[39] The appellant's name had been used as the "contact name" for the company; however, the records were not indexed by contact name, nor were they actually retrieved in practice by contact name, despite the ATP's capability to do so.[40] The court held that *mere capability* was not sufficient to create a system of records.[41]

The court considered three primary factors in its decision, which have become the basis for the current system of records analysis. Initially, the court looked at whether or not the agency had a practice of retrieving records by the contact name.[42] To meet the standard, an individual would have to show that the agency not only had the capability of retrieving records by the individual's name, but that they *in practice* used that capability.[43] Here, although the agency retrieved records using the appellant's name at her request to prove that they had the capability, because they did not do so as a general practice, the court held that this did not constitute the necessary type of retrievals.[44]

The court went on to consider the record-keeping agency's function and why the information was gathered.[45] The names were collected as points of contact between the DOC and companies filing applications with it.[46] The court pointed out that collection of the names was not strictly necessary to the function of the DOC, it was merely a convenience.[47] A phone or fax

---

36. *See e.g.*, Fisher v. Nat'l Inst. Health, 934 F. Supp. 464 (D.C. Cir. 1996); Alexander v. FBI, 193 F.R.D. 1, 6-8 (D.D.C. 2000). *But see* Williams v. Virginia, 104 F.3d 670, 674-77 & n.4 (4th Cir. 1997).

37. *Henke*, 83 F.3d at 1461 n.12.

38. *Id.* at 1455. The DOC and NSF were co-defendants in this suit, however, it was unclear the exact participation of the NSF in this litigation because the court specifically noted that the NSF did have a system of records that they had properly identified with a systems notice.

39. *Id.* at 1457. The ATP was a program within the DOC's National Institute of Standards and Technology.

40. *Id.* at 1456.

41. *Id.*

42. *Id.* at 1457-58.

43. *Id.* at 1460.

44. *Id.* at 1461-62.

45. *Id.* at 1461.

46. *Id.*

47. *Id.* at 1462.

number alone would have served its purposes.[48] The court also indicated that certain purposes, such as investigations, would allow a much more lenient analysis and "even a few retrievals of information, keyed to individuals' names" would suffice for a system of records to exist.[49]

The final point the court considered was whether the records were actually about the individuals named, regardless of the retrieval capability and usage.[50] If the records were not about the individuals named, then the Act would not apply and the application would be invalid.[51] For an individual to retrieve records under the Privacy Act, the records have to actually be about that individual—it is not enough that the individual is mentioned in the records.[52] Here, the court determined that these records were not actually about the appellant, thus she was not entitled to the records under the Privacy Act.[53]

2. *Comparison of* Henke *With Other Holdings*

Fisher v. National Institutes of Health was decided the same year as *Henke* and strictly applied the *Henke* holding to a claim where investigation files were indexed by institution name, rather than by individual name.[54] The court determined that despite the investigatory purpose of the files, the fact that the files were not retrieved by name barred the finding of a system of records.[55] This opinion also emphasized the concept that the system of records had to be in existence at the time of the alleged wrongdoing.[56] The court did not find it persuasive that the agency later created a system of records, published a systems notice, and used names of individuals to locate files.[57]

In *Baker v. Department of the Navy*, the court held that even when the records were collected specifically for investigation of the individual seeking the records, if there is no retrieval capability or use under her name, then the request may be denied.[58] In *Baker*, the requestor was the subject of an investigation, but the records were filed under the name of the individual who instigated the investigation and no cross-referencing occurred, thus there was no Privacy Act claim.[59] The court notes that the system of records analysis is

48. *Id.*
49. *Id.* at 1461.
50. *Id.* at 1462.
51. *Id.*; *see also* 5 U.S.C. § 552a(d) (2000).
52. OMB's Privacy Act Guidelines, 40 Fed. Reg. 28,948, 28,957 (1975).
53. *Henke*, 83 F.3d at 1462.
54. Fisher v. Nat'l Inst. of Health, 934 F. Supp. 464, 474 (D.C. Cir. 1996).
55. *Id.* at 473.
56. *Id.*
57. *Id.*
58. Baker v. Dep't of the Navy, 814 F.2d 1381, 1385 (9th Cir. 1987).
59. *Id.* at 1382.

the one aspect of the Privacy Act where a record is judged not on its content, but on its method of retrieval. Interestingly, *Baker* was actually decided years before *Henke* or *Fisher*.[60] It does not appear to be in conflict with either of those decisions, but its position seems to make it harder to establish a system of records. However, when *Henke* says that "even a few retrievals, keyed to individuals' names" would suffice for a system of records to exist, that indicates that investigatory purposes is not enough alone either.[61]

3. Summary of Overall Scheme

Generally, there must be retrievals of some kind, in some number, for there to be a system of records.[62] If there are many such retrievals, then a system of records is established and the analysis ends.[63] If there are relatively few retrievals, then the other factors, such as purpose of collection, must be considered.[64] However, this leaves substantial gaps in the analysis due to the changing way data is stored.

II. OVERVIEW OF THE CONTROVERSY

If retrievability is the key issue here, then the manner of retrieval should give great insight into the problem. However, it is not as clear as it used to be. In the past, paper or microfiche files were the standard and they were accompanied by an index of some form so that one could locate the particular files one needed. By examining the index and comparing it to the order in which the files were stored, it was fairly easy to determine whether a group of records was indexed according to name, Social Security number, or some other identifier, and thus fell under the Privacy Act.

Today, however, this is not how data storage works. Groups of records that are stored in computer databases do not require a separate index, which makes it more difficult to determine how the data is indexed or catalogued. Those groups of records that are still maintained on paper or microfiche, but which now have a computerized index, also no longer fit the original analysis. The computerized "index" is not an index in the ordinary sense of the word. It does not require that one have the same type of information that a paper indexing system would require to find the needed record. Instead, any information about the record at all will usually be sufficient.[65] Thus, the en-

60. Baker was decided in 1987, nine years before either *Henke* or *Fisher* in 1996 and thirteen years after the original version of the Privacy Act was passed.

61. *Henke*, 83 F.3d at 1461, *see supra* note 49.

62. *Supra* Part I.B.1.

63. *Id.*

64. *Id.*

65. Granted, some types of information may be more effective or more efficient than others at narrowing down the possible files to find the one you want, but the record will still be retrieved.

tire analysis has broken down. One can no longer look at a group of records and determine whether the Privacy Act applies, one must go through the analysis of how the system is used and how retrievals are done, as laid out in *Henke*. Yet even *Henke* does not provide an answer for the most modern groups of records, as discussed in the following section.

III. CREATION OF THE PROBLEM

A. Computer Databases

Computer databases are used to store millions of records throughout the government for virtually every agency at federal, state, and local levels.[66] From property taxes to employment data to Medicare claims, everything is stored in some type of database.[67] Because of these databases, actual retrieval is no longer an indication that the records were filed or indexed according to the individuals' names. Retrieval is easily done without that kind of filing system or index.[68] Files are accessible by name or any other piece of data within a record; a computer database does not need to be indexed by a particular field in order for it to find a record containing that data. Although it may be easier to retrieve records when indexed this way (easier for the user, not necessarily the computer), it really does not matter. A computer can simply do a textual search of all of its records and whenever the searched-for word appears, it will flag the record, regardless of whether the word is in the expected field.[69]

Modern database software such as Microsoft® Access and Lotus Notes™ are the real source of this problem.[70] As agencies converted their old mainframe databases to these newer, more user-friendly versions, they changed the way users are able to interact with the stored data. Where the

---

66. *See* OFFICE OF INFO. AND PRIVACY, FREEDOM OF INFORMATION ACT GUIDE & PRIVACY ACT OVERVIEW 777 (2002).

67. *See e.g.*, John Eckhouse, *Why Nothing's Secret Anymore*, SAN FRANCISCO CHRON., Mar. 15, 1993 at E1 (discussing the variety and accessibility of information stored in computer databases). The number of files and records has become so large that for federal agencies as well as state and local ones, it would be impracticable to try to maintain non-computerized files. *See supra* notes 8 and 23.

68. *See supra* note 33.

69. Following a text search of this kind, any records containing the searched word will be flagged (usually by listing in the dialog box), and can be accessed without any reference to or knowledge of the record number or other identifying information (i.e. the information by which the records was *actually* indexed). Note, however, that one can achieve the effect of a paper index with a more advanced search (typical that it takes *more* technology to simulate the old-fashioned searches), by limiting the search to only a specific field in the records. Thus, when you go to the library and look up "Shakespeare" as "Author", it will not return the many books written by others *about* Shakespeare, where his name is in the title or keywords, it will only return those books where he is listed as author.

70. No, this is not another harangue against Bill Gates, just an observation about how this all got started.

older mainframe databases only allowed searches on particular fields, and had to be specifically programmed to do those searches, the new software allows a straight text search on every bit of information entered into a database, regardless of where it is located within a given record. The difference in search capabilities between the old and new databases is why, despite the fact that records have been stored on computers for decades, the problem with accessibility of records has just emerged.

Consider a hypothetical system of records indexed by the names of investigating officers. One officer's name is Michael Jones. There is a record listed under *another* officer's name containing an investigation on Sally Michaels. If one wanted to know what Michael Jones was working on and so searched the database for 'Michael', not only would all of Michael Jones' cases show up, but so would Sally Michaels' investigation.[71] If Sally then came looking for a copy of her records, how would this be treated under the current system? This was an actual retrieval, but the records were not indexed according to subjects' names. Further, the search retrieved her file, but the searcher was not trying to do that; he was looking for an entirely different set of files. This situation presents the problem of finding a system of records in existence when analyzing it using one name and finding that it does not exist when using a different name. Thus, the system of records analysis appears variable. While the above situation would be considered a system of records with respect to the investigator, it is not considered a system of records *as applied to the subject of an investigation*, simply because her name was not used to file the records. How can a group of records be a system of records in one case but not in another?

Not only does this present a logical paradox, it also creates a legal one. Agencies are required to identify and disclose their systems of records to the public through the OMB. If a particular group of records can be seen as either a system of records or not, how is the agency to determine if it needs to disclose those records? Are agencies expected to disclose all records that have even the potential to be a system of records? Somehow that seems a waste of time, money, and resources without substantial benefit to the public.

B. Computer Stored Records in Comparison with Computer Indexed Records

There is another area of uncertainty within the system of records analysis in the cases where an organization still maintains paper files, filed by case number, but maintains a searchable computer database that indexes the

71. Most searches will find all instances of the particular combination of letters, thus a search for "Michael" would also return "Michaels," "Michaelson," and so on. Here is a frightening test: run a search for the word "the" on a document. What you will find is that large numbers of results are returned for even a short document because "the," "them," "then," "their," "theater," etc. are all returned.

paper files.[72] In these situations, a great deal depends on how much and what type of information is put into the index. If it is in a modern database system and set up with certain key fields,[73] but also provides a space for a description of the file, to help identify the particular case from other similar ones, then any word in that textual description could be found in a search, even though it was not being used as a key field for the index.

How does this type of record storage fit into the analysis? A significant issue, of course, is whether or not the organization actually searches its database using individuals' names. If it does not, then *Henke* applies, the analysis ends, and there is no system of records.[74] If the organization does search by name, it is not actually retrieving the individuals' *records* by its search, it is just obtaining the case numbers and file location or whatever other identifying information was input into the system. Perhaps a court would consider the database a system of records separate from the paper records themselves, but more likely the entire system, computer index and paper files, comprise a system of records. Unfortunately, until a case presents this issue, the analysis changes, or it is decided in some other way, neither the public, nor government agencies can be sure.

C. Evolution into a System of Records

As described above, the Privacy Act and the OMB require that all governmental agencies get approval for and publish a systems notice when they are creating a new system of records.[75] The Guidelines provide instructions for setting up these new systems, but do not explain what must be done to convert an existing filing system into a system of records when the system simply changed over the years, rather than changing as a result of a specific new policy or procedure.[76] There are filing systems that have been in existence for many years, and in some cases the systems have been modified such that they should be listed as systems of records. For these systems, advancements in technology transformed the systems over time and it is difficult to pinpoint the date when the filing system became a system of records.

---

72. This is likely the case when an agency is maintaining handwritten field reports and other non-typewritten records, such as photographs, chemical or other laboratory test results, or even physical evidence itself. In the case of photographs or non-physical evidence, though technology makes it possible to store all of this on computer, every agency may not have that ability or may not have implemented those activities. Thus, some agencies have adopted these combination systems, so that they can still find information quickly, but the computer only provides the location, not the actual data.

73. Key fields for this type of index might include the case or identifying number, the name of the case, if any, and any other specific information regarding the location of the physical file (such as a room number, or storage cabinet number, etc.).

74. *Henke*, 83 F.3d at 1461.

75. 5 U.S.C. § 552a(e) (2000); OMB's Privacy Act Guidelines, 40 Fed. Reg. 28,948, 28,962-63 (1975).

76. OMB's Privacy Act Guidelines, 40 Fed. Reg. 28,948, 28,963 (1975).

Agencies do not have guidance for many of the issues surrounding conversion of older groups of records into systems of records.

Consider the following questions that would arise if an agency decides to publish a systems notice for an existing system. Does publishing a notice mean that *all records* filed in the system would be available under the Privacy Act, even those that were collected well before the records evolved into a system of records? What about records that were collected after the system of records evolved, but before it was officially recognized, i.e. before the systems notice was published? Generally ex post facto regulations or statutes are disfavored; is that not what creating such a rule would be? Why should agencies be required to hand over records that were collected prior to the time when the systems notice goes into effect?

IV. ANALYSIS

The new reality of how agencies store and retrieve their records presents two possible futures for the Privacy Act. If the Privacy Act remains unchanged, then we must accept that the current application of the *Henke* analysis has broadened the accessibility of records to the public beyond the original scope of the Act. Alternatively, if the Privacy Act is amended to overrule *Henke* and change or clarify the system of records analysis, the majority of the original limitations could remain intact.[77]

A. Accepting the Broadened Access

The combination of the *Henke* analysis with extensive computerization of records has resulted in a widening of the range of records accessible under the Privacy Act. When an agency upgrades its databases to be fully computerized, the new systems provide search functions that do not rely upon the method of indexing.[78] Thus, when looking for a particular record, it is often easiest to search on a particular word or name within that record, even if the record is not otherwise about the search term, rather than searching for the case number or the report title or other official identifier.[79] As a result, the

77. *See* OFFICE OF INFO. AND PRIVACY, FREEDOM OF INFORMATION ACT GUIDE & PRIVACY ACT OVERVIEW 795-97 (2002).

78. Meaning the use of newer database software, such as Microsoft® Access or Lotus Notes™, that allows for full text searches.

79. This is particularly true when the indexing method or the case name, etc. has many duplications. For instance, consider a *Fisher*-type situation, where the NIH indexes according to the name of the institution or organization, except in this case the files are completely computerized and the staff makes use of the search functions. If one were to do a search for Abbott Laboratories (a large biotech company), there would likely be thousands or records resulting. However, if one recalled that someone named Alice Smith gave a statement regarding the particular case, it would be far easier to search using her name, because it would likely show up in far fewer records and it would be easy to determine which were the needed records.

agency has performed *actual retrievals* using individuals' names and therefore the major factor in the *Henke* analysis is met. The added retrievability has broadened the extent of the records considered to be in a system of records, and along the way, the public's access to those records.

An argument in response to this apparent broadening of accessibility is that requests under the Privacy Act where searches are done as described above would not be granted. They would legitimately be denied because the records would not be about the requestor and thus the Privacy Act would not apply. However, this is not necessarily the case. There may be agencies where records are maintained that are arguably "about" a particular requestor, yet *but for* the computerized searching those records would not be accessible because they were not indexed by a personal identifier.[80]

In those instances, it may seem that allowing access would be preferable because access would conform to the spirit of the law: giving an individual access to files stored by the government that are *about that individual.* However, there may be legitimate and important reasons for maintaining the files in such a way as to avoid granting access, such as national security. In *Fisher*, the court did not require such critical reasons or interests of the agency at all.[81] The fact that the NIH had always maintained their files in that way was sufficient for the court to hold that there should be no access, even without a showing of particular reasons why it was necessary for the NIH to use that filing method.[82]

There is also the possibility that a different interpretation of *Henke* might evolve in the courts, upon presentation of a different set of facts. Although it may not be clear at the present time what facts a court might find sufficiently distinct from *Henke* and *Fisher* to produce a different result, there is certainly room for courts to limit the *Henke* holding. Not only would judicial constriction of the *Henke* holding likely provide a more palatable result than simply accepting the situation as it is, it would also be an easier process than amendment of the Act.

Does all of this really mean that allowing the scope of the Privacy Act to broaden is a bad decision? After all, was the Act not written to protect the public from use and misuse of records by the government? Although it does seem to be a logical conclusion that allowing a broader application of the Privacy Act would further its original purpose, the carefully struck balance between private concerns and government interests might ultimately be destroyed.

---

80. Consider Fisher v. NIH, the case where an investigation record was denied to a requestor because the records were indexed based on the individual initiating the investigation and the institution at which the person worked, rather than the subject of the investigation, and likely, the record.

81. *Id.* at 473.

82. *Id.*

B. Amending to Retain the Intended Access

An amendment to the Privacy Act could both clarify the system of records analysis and help to maintain and re-establish the original intent and limitations of the Act. Any amendment passed to the Privacy Act would have to reconcile the differences between the holding of *Henke* and the current computerized methods of data storage and the purpose of the Act itself. Here we must look to the specific wording of the Act and its legislative history, as well as the reality of the computerized world. Right now, advances in technology appear to have shifted somewhat, with the focus on making storage bigger and speeds faster, not on altering the basic concept and structure underlying the machines. Thus, it is probably an ideal time to consider such an amendment. Now that so many government agencies' records are stored in *today's* databases, when future advances arrive, agencies will probably switch over slowly, and only after the new technology has been well proven in the private sector.[83]

It could be argued that changing the Privacy Act by amendment may create more problems than it solves.[84] Or it could create an entirely new set of unforeseen effects with their own problems. It may be that leaving the Act alone will result in the least conflict; there is no way to know in advance either way. Other than just leaving the Privacy Act as it currently stands, the Act could be repealed entirely and new legislation put into place. This, however, seems too draconian a solution for a problem that exists only in one section of the Act. Although other sections of the Act may also benefit from updating, eliminating them entirely is not likely to help solve any problems. Unfortunately, if left without any changes, the Privacy Act may become so outdated in the future that eliminating it and starting over may be the only solution. Thus, an amendment now, though complicated, may save even more work later.

An amendment would need to address three specific areas of the Privacy Act to be fully effective. First, it would need to establish exactly what a system of records is and how one is created, i.e. what combination of organization and retrievals is necessary to qualify. Importantly, the retrieval factor should not be keyed to a particular number of retrievals, since this would vary from agency to agency, and what might be a full year's worth of retrievals for one agency, might be only a week's to another. Perhaps a solution would be to consider the percentage of the total retrievals that are done by individuals' names as a minimum standard. Although many legal solutions involve applying a standard of reasonableness, that is essentially what

---

83. Karen Kaplan, *Bringing the IRS into the 21st Century*, L.A. TIMES, June 27, 1999, at C1 (describing the long-awaited upgrade of the IRS computer system into a comprehensive, modern database system).

84. For example, requiring excessive court involvement or supervision or creating high costs of system renovation and maintenance for the OMB might be problems created by an amendment.

was established by *Henke*, where the court said that a reasonable number of retrievals for the circumstances would suffice to show that a system of records existed.[85] This is the very standard that has not worked so far, thus a more specific measure should be implemented here.

Second, the amendment would need to address the procedures for systems that have evolved into systems of records, including a timeline of which records are accessible under the Privacy Act. If the amendment allows information collected before the system of records developed to remain inaccessible, agencies will need to know how to publish their systems notices to identify information collected as part of a system of records, while exempting information that does not qualify. Also important would be an explanation of this change in policy for the public. The easiest means of achieving this would be to have the OMB provide an explanation of accessibility, and the way agencies determine accessibility, along with its published systems notices. Because individuals generally go through the OMB to find information about systems of records, they would find out about the new policies at the same time.[86]

Finally, the amendment should make allowances for future changes in technology, to the best that today's predictions can establish. This last area would likely be the most difficult to do successfully; however, it could be done by simply including a statement that future disagreements are to be resolved to conform with the original intent of the Act. The amendment could also recommend or require that the technology situation be reevaluated at regular intervals, in order to keep the processes current and to avoid a significant overhaul of the data and procedures in the future.

Alternatively, instead of providing substantive changes to the analysis, the amendment could simply restate the original intent of the Privacy Act or some narrowed intent. Then the amendment could direct that all future construction of the Act merely conform with that explained intent. This restated intent should take into account concerns of national security or whatever other interests Congress deems relevant in today's world. If Congress takes this approach and decides to avoid making specific substantive changes, then the interpretation of the Privacy Act will ultimately end up in the courts again. In that case, the courts will have a lot of leeway in deciding how best to interpret the new language, but at least they would be bound to the express intent of Congress. This may not be the ideal solution, but it would be an improvement over the current situation.

---

85. *Henke*, 83 F.3d at 1461.

86. Sometimes individuals are sent privacy notices by agencies maintaining records on them and use those notices as their sole source of information. However, when notices are not sent directly or when an individual wants to access all systems notices, that individual would have to go through the OMB, because to access the notices through the agencies themselves (more accurately, through their websites) would usually require an internal computer logon and password. Even those agencies with public websites (ones that do not require passwords) that make their systems notices available online merely do so by providing links that point to the notices as published on the Federal Register's website. *See supra* Part I.A and note 29.

The critical focus of an amendment should be upon the Privacy Act's definition of "system of records" itself.[87] It is in this definition that the most effective change could be made, because all of the other provisions of the Act depend upon the current definition.[88] In each case, by updating the definition, the individual sections would be correspondingly revised. Although an exceptionally long and detailed definition would probably only create greater opportunities for disagreements and court interpretations, a definition that recognizes the indexing method and computer database form, supported by a clear Congressional record, would provide the necessary changes. Likely a change to this section would necessitate changes at the level of the OMB Guidelines as well, which would provide an additional opportunity for clarification and detail.

The other section that would benefit from revision is the "agency requirement" section, which provides the steps an agency must take to set up a new system of records, properly identify it, and publish the systems notice.[89] Depending on the approach taken in the amendment with regard to paper files with computerized indices and to records that have evolved into systems of records, it may be necessary for the new systems notices to include information such as applicable dates or categories of individuals who may obtain the records.[90] A danger in these situations is that by identifying records that the Privacy Act does not cover, an agency practically invites disputes. However, if the amendment is sufficiently clear and the agency follows the statute, then the problems should be minimized.

The Privacy Act is ultimately a balancing of interests between the government agencies storing the records and the individuals about whom the records are kept. Currently the balance is wavering, and depending on the next steps taken, it may shift so that the government agencies' interests have virtually no protections under the Act. While the notion of the government keeping secrets from the citizens of the United States does not sit well with anyone, there can be legitimate reasons why an individual should not have access to a particular record. Do we really want to eliminate all of the protections agencies have? Remember that the Privacy Act does not allow for exceptions or redactions of the record in most cases, thus agencies are required to turn over entire records, including material generally protected from disclosure requirements.[91] Do we really trust them so little and believe that their decisions regarding access to records are unjustified? An amendment is nec-

87. 5 U.S.C. § 552a(a)(5) (2000); *see supra* Part I.A for current full definition.

88. *See supra* Part I.A and note 23.

89. 5 U.S.C. § 552a(e) (2000).

90. With regard to the categories of people who may access the records, an example using the *Henke* case: if the appellant had applied for the grant *personally*, rather than as a company with her name listed as a contact, then she might have had success under this approach.

91. For example, there is no general exception for attorney work product or for privileged attorney-client communications. While these privileges may apply in other situations, they are not recognized under the Privacy Act. 5 U.S.C. § 552a(j), (k) (2000).

essary to rebalance this process. Consider also those agencies that think they may have records that have evolved into systems of records, but are unsure what to do about it. In those cases, an amendment clarifying these procedures would actually *increase* the access of the public. Overall, an amendment will serve both the government agencies and the public, and will save the Privacy Act from falling further and further behind technology.

CONCLUSION

One theory in life is that if something is not broken, we should not try to fix it. Although that may be true of toaster ovens and VCRs, it does not apply here. The Privacy Act is *mostly* working; it is not shooting off sparks and threatening to burn down anyone's kitchen. For the most part, agencies publish their systems notices and individuals request and receive the information they need. However, the Act is also creating a great deal of confusion for both members of the public seeking access to their records, and for the agencies who are maintaining those records. Perhaps this is the equivalent of burned toast; not a fire hazard, but not exactly good either. Therefore, something needs to be done to clarify the situation. A decision needs to be made. On the one hand, the OMB could simply issue a policy instructing agencies to comply with the *Henke* holding and leave it at that. At the very least, that would eliminate some of the confusion with regard to the duties that agencies owe to the public. However, it would still leave substantial questions unanswered, such as what to do with those existing systems that have evolved into systems of records, and what about systems where only the index is computerized and searchable. On the other hand, the OMB could take a more proactive approach and redefine the system of records analysis within its own published Guidelines. These Guidelines do not have the weight of a statutory amendment, but as the official policies of the federal department that oversees the Privacy Act, they would likely gain the compliance of other governmental agencies.

Another problem with leaving the Act as it stands now is that technology is not likely to stand still. Huge advances in technology created this issue in the first place. Though most people cannot predict what is ahead, it is that very unpredictability that suggests changes need to be made now. If nothing is done now, how much worse will the situation be in ten, twenty, or thirty years? How much farther from the original intent of the Privacy Act will technology have led us? In the past, most of the files collected, maintained, and requested were written or printed documents. Video and audio cassettes simply took up too much space to store them on a regular basis, in the ordinary course of business. Each cassette could only hold a certain amount of data, and finding any particular information required listening to or viewing the entire tape. Today, video and audio files are digitized and now they can be stored as easily as any text file. A CD-ROM can be used to store digital files that would replace volumes of printed material or audio

and video data that would have taken up many cassettes.[92] With the advances in voice recognition, the computer does the searching for information within files. In these days of heightened national security and increasing surveillance technology capabilities, audio and video files may become more common in the government's files. How is the Privacy Act going to be applied? How are the public's concerns over this kind of intrusion going to be addressed?

We need an amendment to bring the Privacy Act up to date. We cannot expect a convenient case will present itself to the courts in a timely fashion to resolve this problem, and the problem will only grow with time. Although this may not seem to be a priority in the public's mind, it is in everyone's best interest that an amendment be passed. By the time most people become truly interested in the workings of the Privacy Act, it is usually too late. At that point, they are probably attempting to retrieve records from agencies that have complied with the technical rules of the Privacy Act and the OMB Guidelines, but have missed the intent of the Act. Or, they are dealing with agencies that do not have the answers to the questions discussed here, have not determined what they need to do, and thus cannot give access to their records. By the time people have gotten to this stage, it is too late to amend the Privacy Act to give agencies more guidance and clearer rules. They will have discovered that the Privacy Act is *not* really working, and does need to be fixed. Thus, a timely amendment is in everyone's interest.

Julianne M. Sullivan[*]

92. Even the military has made this switch: their Official Military Personnel Files (OMPF) are now stored on CD-ROM. The switch was made from the past microfiche system because of the impracticality of microfiche and difficulty in ensuring a microfiche reader would be available where needed, coupled with the ease of use of the CD-ROMs and the fact that CD-ROM drives are found in virtually every computer made today.

* California Western School of Law, J.D. candidate, 2004; Northwestern University, B.S. Biomedical Engineering, 2000; Thank you to my mother, Cathy, for all of her help and support.