1-1-1985

IRS Computer Data Bank Searches: An Infringement of the Fourth Amendment Search and Seizure Clause

Robert Messick

Follow this and additional works at: http://digitalcommons.law.scu.edu/lawreview

Part of the Law Commons

Recommended Citation
Available at: http://digitalcommons.law.scu.edu/lawreview/vol25/iss1/6

This Comment is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara Law Review by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
IRS COMPUTER DATA BANK SEARCHES: AN INFRINGEMENT OF THE FOURTH AMENDMENT SEARCH AND SEIZURE CLAUSE

I. INTRODUCTION

In recent years the Internal Revenue Service has faced increasing difficulty in enforcing the internal revenue laws. Studies suggest that nearly twenty-five percent of all income earners evade income taxes. Although there has always been a certain element of society unwilling to comply with revenue laws, the dramatic increase in noncompliance deeply concerns the Internal Revenue Service and Congress. An obvious solution, recently instituted by the IRS, is to implement state-of-the-art computer technology. With the ability to

© 1985 by Robert Messick


The greatest portion of uncollected taxes is attributable to the "underground economy," defined by the General Accounting Office (GAO) as "the aggregate of unrecorded cash activity and that activity which escapes economic measurement and tax assessment. This includes the actual exchange of goods or services for cash or for value of other goods or services; that is, bartering." Underground Economy, 1979: Hearings on H. 781-42 Before the Subcomm. on Oversight of the Comm. on Ways and Means, 96th Cong., 1st Sess. 3 (statement of Allen R. Voss, Dir., Gen. Gov't Div., GAO). The "underground economy" is defined by the IRS as including both legal and illegal income. Coates, supra note 2, at 100.

For the calendar year 1981, the IRS estimated a "tax gap" of about $90 billion in uncollected taxes. The tax gap represents the uncollected taxes resulting from overstated deductions and underreported income, including unreported interest, dividends, tips, and earnings of independent contractors from the legal sector; and income derived from organized crime, such as drugs, gambling, and prostitution.

The IRS estimates that individual taxpayers who do file tax returns are the largest source of unpaid taxes, totaling nearly $66 billion, while individual nonfilers represent an estimated loss of only $3 billion in uncollected taxes. Surprisingly, according to IRS estimates, illegal sector income represents only $9 billion, or 10% of uncollected taxes for 1981. The balance of the deficit is represented by corporations, trusts and exempt organizations. Coates, supra note 2, at 101.

3. As part of its ambitious computer matching plan, the IRS in 1983 implemented the Automated Collection System (ACS). ACS is a fully computerized network system for tracking
search thousands of computer data banks throughout the country containing hundreds of millions of records on the personal affairs of citizens, the IRS can tap this wealth of information to track down noncomplying citizens.

Indiscriminate IRS searches through data files raise serious issues concerning the fundamental rights of an orderly society—the right of privacy, freedom of association, and the right to be free from unlawful searches and seizures. The use of computers to ferret out tax evaders represents a much more serious threat to an individual's civil liberties than do manual searches through file cabinets. The insuperable manual task of matching billions of bits of information scattered across the nation has been conquered by the computer. Using a common form of identity such as a social security number, information from diverse sources can be pieced together to provide a more complete profile of data bank subjects. The ease with which matching functions may be performed, and the cost effectiveness of such functions provide an incentive to apply computer technology

down delinquent taxpayers. The network consists of 30 computer systems in IRS service centers nationwide and is continuously updated with such information as delinquent taxpayers' most recent telephone numbers and addresses. At a cost of $300 million, ACS is expected to collect between $1.5 and $1.7 billion during its first six years of operation. GENERAL ACCOUNTING OFFICE STUDY, [Gov't Pub. No. GGD-83-103] COMPUTER TECHNOLOGY AT IRS: PRESENT AND PLANNED 127-29 (1983) [hereinafter cited as COMPUTER TECHNOLOGY AT IRS]. See New Computerized Taxpayer Compliance Pilot Program, Milwaukee Sentinel, May 11, 1983, at 1, col. 3 (implementation of ACS in Chicago and St. Louis).

4. See infra notes 41-52 and accompanying text for a discussion of the right to privacy, notes 53-56 for a discussion of the right of freedom of association, and notes 93-190 for a discussion of the right to be free from unlawful searches and seizures.

5. A data bank subject refers to an individual who is the subject of a computer data file containing personalized information specific to the individual's affairs.

Justice Douglas aptly described the revealing consequences of laying bare one's bank records:

The records of checks—now available to the investigators—are highly useful. In a sense a person is defined by the checks he writes. By examining them the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on ad infinitum. These are all tied to one's social security number; and now that we have the data banks, these other items will enrich that storehouse and make it possible for a bureaucrat—by pushing one button—to get in an instant the names of the 190 million Americans who are subversives or potential and likely candidates.


"Computers facilitate the composition of lists of people connected with various types of activities and institutions from widely scattered data that probably could not be brought together manually, enabling previously unknown relationships to be revealed or inferred from seemingly disparate information." A. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 202 (1971).
against taxpayers. This comment will first examine the threats posed to civil liberties by present and planned IRS use of governmental agency and private data banks. Second, the inadequacies of the first and fifth amendments as constitutional protections, and the ineffectiveness of the Privacy Act of 1974 as a statutory restraint upon IRS searches will be discussed. Finally, this comment will focus on the fourth amendment search and seizure clause as a possible means of providing protection to citizens against IRS computer searches of data banks. This comment concludes that such a search is a general search prohibited by the fourth amendment, and further, any particularized search of an individual’s records contained on data banks requires a warrant based upon probable cause.

II. INTERNAL REVENUE SERVICE DATA BANK SEARCHES

With more than twenty-five percent of its budget and manpower dedicated to computer operations, the IRS is one of the largest nondefense users of computers in the federal government. The Service presently has in force over forty mainframe computers at ten IRS service centers and the National Computer Center. Beginning in 1974, the Internal Revenue Service applied its computer resources to the task of matching information returns filed by income payors

6. The costs of computer functions has decreased from a 1950 high of $1.26 per 100,000 calculations to only $0.0025 per 100,000 in 1980. OFFICE OF TECHNOLOGY ASSESSMENT [Pub. No. OTA-CIT-146] COMPUTER-BASED NATIONAL INFORMATION SYSTEMS: TECHNOLOGY AND PUBLIC POLICY ISSUES 4 (1981) [hereinafter cited as COMPUTER-BASED NATIONAL INFORMATION SYSTEMS].

The IRS has stated that it costs $400 to process 100,000 documents submitted on magnetic media as opposed to $20,000 to manually process the same amount of information from paper documents. Hearings Before the Comm. on Commerce, Consumers, and Monetary Affairs, A Subcomm. of the Comm. on Gov't Operations, 96th Cong., 1st Sess. 3 (1979) (testimony of Richard L. Fogel, Assoc. Dir., Gen. Govt. Div., GAO) [hereinafter cited as Fogel]. For this reason, the IRS has aggressively promoted that taxpayers submit information documents on magnetic tape. As a result, the number of documents submitted on magnetic tape has increased from 48 million in 1968 to about 435 million in 1978—representing 87% of the total number of documents submitted that year. Id. at 80.

7. COMPUTER TECHNOLOGY AT IRS, supra note 3, at 1.

8. Id. The National Computer Center (NCC), located in Martinsburg, West Virginia, is the centralized computer center for the IRS. NCC contains the Master File of 145.9 million individuals and businesses on 1,800 reels of magnetic tape. NCC's library contains a total of over 178,000 reels of magnetic tape and almost 2,600 computer programs. Id. at 1, 14, 24, and 25.

9. Information returns are transmittals to the IRS describing the nature and amount of payments to recipients. See I.R.C. §§ 6041-59 for a list of sources of income which require payors to submit an information return. Section 6041 requires that:

All persons engaged in a trade or business and making payment in the course of
with tax returns filed by recipients of the income. During the early years of this program only about fifty percent of all information returns submitted were actually matched against tax returns. The majority of the matched information returns were on magnetic computer tape generated from the payors' in-house computer record systems. The remaining fifty percent of the information returns, most of which were submitted on paper, were typically discarded by the IRS because of the massive effort required to transfer the information to magnetic tapes for computer use. More recently, nearly eighty percent of all information returns filed have been matched against tax returns. Consequently, the IRS has attained the ability to match tax returns filed with nearly all information returns submitted, and thereby generate a list of all persons underreporting income or failing to file tax returns.

such trade or business to another person, of rent, salaries, wages, premiums, annuities, compensations, remunerations, emoluments, or other fixed or determinable gains, profits, and income. . . of $600 or more in any taxable year. . . shall render a true and accurate return to the Secretary. . . setting forth the amount of such gains, profits, and income, and the name and address of the recipient of such payment.


The IRS expects to receive nearly one billion information returns for the tax year 1984. WALL STREET J., Feb. 22, 1984, at 1, col. 5. However, with the enactment of I.R.C. § 60501 in the Tax Reform Act of 1984, the information returns required to be filed for the year 1985 could easily exceed 5 billion in number. Section 60501 requires any person engaged in a trade or business who receives, in the course of that trade or business, more than $10,000 in cash or foreign currency in one or more related transactions, to report the receipt of the money to the IRS and to provide a statement to the payor. I.R.C. § 60501 (West Supp. 1985). Transactions subject to the reporting requirements of § 60501 include, but are not limited to, “a sale of goods or services; a sale of real property; a sale of intangible property; a rental of real or personal property; an exchange of cash for other cash; the establishment or maintenance of or contribution to a custodial, trust, or escrow arrangement; a payment of a preexisting debt; a conversion of cash to a negotiable instrument; or the making or repayment of a loan.” 50 Fed. Reg. 21,239 (1985) (to be codified at 26 C.F.R. pt. 1, § 1.60501-1 (T)) (proposed May 23, 1985). Section 60501 also encompasses transactions with dealers in precious metals, stones or jewels, pawnbrokers, loan or finance companies, insurance companies, and travel agencies. H.R. REP. No. 861, supra note 2. The penalty for failure to file the necessary information returns is $50 per failure, subject to a maximum of $50,000 per calendar year. I.R.C. §§ 6652, 6678 (1984).


11. Id.

12. Id.

The effectiveness of the matching system has not been satisfactory. The IRS has concluded that because nearly half of all nonfilers identified by a computer match are not required to file a return, pursuit of all nonfilers without further differentiation would be unproductive.

Realizing the need for more comprehensive computer matching, the IRS has developed a predictive model which takes into account other sources of information and determines what group of persons is least likely to comply with the revenue laws. In order to implement its ambitious plan to track down noncompliers by computer, the Internal Revenue Service expects to spend nearly two billion dollars over the next six to eight years on state-of-the-art computer technology. With the combination of massive computer systems and access

14. IRS received over 588 million information documents of all types for tax year 1981. For cases generated in prior years and completed in fiscal year 1981, document matching resulted in additional tax assessments totaling about $500 million - less than 1% of the total tax gap. IRS NON-COMPLIANCE STUDY, supra note 13. See also Fogel, supra note 6, at 78-81, criticizing the IRS for ineffective handling of the compliance program; suggesting that "payors are not submitting all required information documents," "many documents submitted are not used," "[m]ore income could be subjected to matching," and "[a] management information system is needed for proper program planning and evaluation."

15. An IRS study for the year 1976 concluded that nonfilers are predominately of a low income status with 52% having incomes of $5,000 or less. Nonfilers account for only about 16% of lost revenues. Kurtz, supra note 10, at 7.

16. IRS has calculated that the greatest return of revenue per hours of examination (audit) time is naturally from the highest generators of income - the top 1,200 to 1,300 corporations. Thereafter, as the income level drops, so does the return on examinations. Therefore, examinations of nonfilers in the lowest earning category, which yield the lowest return on examination, can only be justified by the need to maintain an IRS "presence" among all strata of taxpayers. Id. at 4-19.

17. During hearings before the Committee on Government Operations, Commissioner Kurtz stated:

We are trying to improve our methodology for selecting nonfiler cases by developing a predictive model to detect nonfilers. The concept here is to design a more objective, scientifically designed scoring system that will identify the most productive nonfiler cases. We need such a system because we anticipate a backlog of 700,000 uncompleted nonfiler investigations by the end of 1980 and must select those cases to which we will devote our limited resources.

Id. at 7.

In response, Congressman Joel Deckard querrated Commissioner Kurtz whether the IRS was using a profile of typical nonfiler or tax-avoidance persons as a basis for random selection of audits. The commissioner replied that the IRS does have such a profile system which is used in conjunction with various commercial data banks capable of selecting persons from particular professions or cities. Kurtz, supra note 10, at 34.

18. See generally COMPUTER TECHNOLOGY AT IRS, supra note 3. The IRS originally proposed, at a cost of $1.8 billion, a "Tax Administration System" (TAS). TAS would have been a nationwide network of computers hooked together by telecommunications with the NCC (National Computer Center) functioning as a taxpayer directory and providing national reports while continuing to process and match information returns. Conservative dissent.
to thousands of data banks from which to draw personal information on millions of individuals, the IRS will have the capacity to conduct thorough computer searches of most citizens.

A. Internal Revenue Service Access to Government Data Banks

Notwithstanding the Privacy Act of 1974,19 the IRS has authority to gain access to interagency data banks for the purpose of enforcing criminal laws. The intended purpose of the Privacy Act is to restrict access to, and transfers or disclosures of, personal information stored on government data banks. Section (j)(2) of the Privacy Act exempts from its prohibition against disclosure those agencies which have as their principal function any activity pertaining to the enforcement of criminal laws.20 Because one of the functions of the IRS is enforcement of the criminal provisions of the Internal Revenue Code,21 the IRS appears to be exempt from section (j)(2).

With such broad discretion the IRS may acquire information of a personal nature from thousands of government data banks. By 1971 the federal government maintained 5,961 computers.22 On the state level, the Law Enforcement Assistance Administration reported that in 1976 over 4,000 criminal justice data banks were available for nationwide transfer of information from state data banks.23 In addition, state law enforcement agencies can access the Federal Bureau of Investigation National Crime Information Center (NCIC) which maintains records on persons, vehicles, license plates, articles, guns, securities, and boats - all for the purpose of identifying stolen property and wanted criminals.24 The FBI also maintains "narrative

sal due to concern over the substantial threat of invasion of privacy. The Office of Technology Assessment likewise expressed fears over the proposal. Id. at 61. Congress subsequently approved a repackaged proposal effectively requesting a system with the same capabilities as TAS. Id. at 61.

19. The Privacy Act of 1974, 5 U.S.C. § 552a (1982), was enacted to protect individual privacy interests from government misuse of federal records containing personal information. For further discussion of the Privacy Act, see infra notes 59-92 and accompanying text.

20. 5 U.S.C § 552a(j)(2).

21. Internal Revenue Code § 7608 grants to Criminal Investigation Division Agents of the IRS the authority to execute and to serve search and arrest warrants, to make arrests based upon probable cause without warrant, and to seize property to enforce the criminal provisions of the IRS code.

22. A. Westin, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING AND PRIVACY 29 (1972) [hereinafter cited as DATABANKS IN A FREE SOCIETY].

23. 1 U.S. DEPT. OF JUSTICE, LAW ENFORCEMENT ASSISTANCE ADMIN., DIRECTORY OF AUTOMATED CRIMINAL JUSTICE INFORMATION SYSTEMS (1976). The Law Enforcement Assistance Administration of the Department of Justice is required to promulgate privacy and security regulations covering federally-funded criminal justice information systems.

24. DATABANKS IN A FREE SOCIETY, supra note 22, at 50.
files" which contain applications for federal jobs, special investigations conducted by the FBI, credit-checks, reports of agent interviews, documentary materials, informant reports, and "technical informant" data including wiretapping and bugging information. The files contain both verified and "raw" unconfirmed material.

During the 1960's, the United States Army Intelligence actively collected personal data on lawful political organizations and their members including the American Civil Liberties Union (ACLU), the National Association for the Advancement of Colored People (NAACP), the Southern Christian Leadership Conference (SCLC), and the Women's Strike for Peace. The IRS could conceivably use this information with the assumption that "politically subversive" individuals are more likely to violate the tax laws.

In the early 1970's, the IRS conducted research on the relationship between a taxpayer's political affiliation and his or her propensity toward tax evasion. In the process of its research and surveillance, the IRS collected a considerable quantity of information on many individuals and businesses. After Senate oversight hearings on the matter, the program was disbanded.

Because of the tremendous amount of information that government agencies collect for various reasons, the federal government has amassed an incredible array of data banks. In addition to govern-

25. Id.
26. Id.
29. The Internal Revenue Service program, known as the Special Service Staff (SSS), compiled political intelligence data on at least 11,000 individuals and organizations deemed to be "activists, . . . ideological, militant, subversive, radical." Id.
30. As of 1974, over 850 federal data bank systems existed. Id. at 14. The following is a partial list of federal agency data banks accessible to the IRS:
   Social Security Admin.
   U.S. Customs Service, Financial Law Enforcement Center
   Dep't of Health and Human Services (formerly HEW)
   Dep't of Justice (Nat'l Crim Justice Info & Statistical Service)
   Federal Bureau of Investigation
   Veterans Admin.
   Nat'l Aeronautics & Space Admin.
   Office of Naval Intelligence
   U.S. Postal Inspector's Office
   Bureau of Narcotics and Dangerous Drugs
   Immigration and Naturalization Service
   Dep't of Defense
   Dep't of Labor
ment files, the Internal Revenue Service also has access to thousands of private data banks, most notably those belonging to banks, credit reporting agencies and commercial mailing list companies.

B. **Internal Revenue Service Access to Private Data Banks**

Commercial bank computer data files typically contain information supplied by applications for new accounts, credit requests, and subsequent banking transactions.\(^{31}\) Credit reporting agencies possess information from a myriad of sources, including property records, landlords, employers, banks, credit references, court records, newspapers, trade periodicals, and bulletins from protective agencies han-

---

Secret Service Comm'n  
U.S. Coast Guard  
Dep't of Treasury  
Dep't of the Interior  
Office of Personnel Mgmt.  
Selective Service Admin.  
Army and Air Force Exchange Serv.  
Federal Deposit Insurance Corp.  
Trials Interagency Litigation Systems (TRIALS)  
Bureau of Personnel Investigations, Civil Service Comm'n  
Defense Logistics Agency  
Dep't of Commerce (Bureau of Economic Analysis)  
Illustrative of the scope of information retained in government agency data banks is the following NASA employee file listing:

- birth date; social security number; home address and telephone number; marital status; references; veteran preference, tenure, handicap; position description, past and present salaries; payroll deductions, leave; letters of commendation and reprimand; adverse actions, charges and decisions on charges; notice of reduction-in-force; personnel actions, including but not limited to, appointment, reassignment, demotion, detail, promotion, transfer and separation, minority group; records relating to life insurance, health and retirement benefits; designation of beneficiary; training; performance ratings; physical examinations; criminal matters; data documenting the reasons for personnel actions or decisions made about an individual; awards; and other information relating to the status of the individual.

In addition to the internal uses of the information contained in this system of records, the following are routine uses outside of NASA for information maintained on . . . employees only: (1) Provide information in accordance with legal or policy directives and regulations to the Internal Revenue Service . . . .


31. **DATABANKS IN A FREE SOCIETY**, supra note 22, at 121. Bank records and other third party records are not available to the IRS without an administrative summons. I.R.C. § 7609 (1982). Under § 7609, except in unusual circumstances, the IRS is required to provide a bank customer 23 days notice when it issues an administrative summons to review records at a bank. After receiving notice, the customer has a right to object to enforcement of the summons before a U.S. district court. An individual is also entitled to notice before the IRS issues an administrative summons on third-party recordkeepers such as credit unions, consumer reporting agencies, credit card companies, brokers, attorneys and accountants.
The scope of the information encompasses such matters as "age, marital status, dependencies, residential history, occupation, financial resources, bank references, manner of payment of accounts, loans and other credit extensions in the trade and lending institutions, and litigation history, if any." Credit bureaus may pry even deeper into matters so personal as an applicant's reputation, character, and morals. Since credit agencies are in the business of selling information, they are just as willing to sell their information to the IRS as to any other buyer.

The mailing list industry is another source of personal information maintained on data banks. Mailing lists are data compilations predominately gathered from public sources, including "official records, telephone books, city directories, membership lists, news clippings, customer lists, lists of contest participants, door-to-door canvassing, and convention rosters." Government sources include lists of pilots, boat owners, ham-radio operators, veterans, and motor vehicle owners. Information is also purchased from commercial sources such as credit card customer accounts and publishers.

Mailing list data banks contain information on an individual's business connections, marital status, occupation, place of employment, telephone number, and status as a renter or homeowner. Continuous updating of changes in address, employment, subscription offers accepted, purchase clubs joined, and retail store transactions reflect many buying preferences and habits. With access to

33. Id. at 9-10.
34. Fair Credit Reporting Act, 15 U.S.C. § 1681 (1982), permits the IRS to obtain identifying data from a credit agency's data banks. In United States v. Davey, 426 F.2d 842 (2nd Cir. 1970), Credit Data Corporation, a nationwide credit agency, challenged IRS summonses seeking credit records in the company's data bank, asserting that the IRS sought to use Credit Data Corporation as a vast private databank for its own investigatory purposes and that the IRS summonses were unreasonable searches and seizures. In response, the federal district court held that "[t]he government has the right to require the production of relevant information wherever it may be lodged and regardless of the form in which it is kept and the manner in which it may be retrieved, so long as it pays its reasonable share of the costs of retrieval." Id. at 845.
35. Databanks in a Free Society, supra note 22, at 154-55.
36. Id.
37. Id.
38. Id. at 155.
39. Id. at 157. Retail store point-of-sale terminals collect such information on customers as name, items purchased, exact time and location of purchase, and financial status as it relates to credit transactions. Computer-Based National Information Systems, supra note 6, at 76.
such comprehensive information drawn from diverse sources, the Internal Revenue Service can readily construct a complete dossier on an individual and map out his or her past, present and anticipated transactions. Under no other circumstances than by computer matching of data banks can the IRS so readily discover one's personal reputation, morals, preferences, habits and day-to-day transactions in business and private lives.

Despite the fact that a significant portion of private data bank information is derived from public sources, the compilation and assimilation of such data from all avenues of life threatens normal societal expectations of privacy.40 These important societal interests in privacy and noninterference by government have traditionally been protected by such constitutional and statutory provisions as the first, fourth and fifth amendment, and the Privacy Act of 1974. Nevertheless, these provisions have their shortcomings as applied to IRS computer data bank searches. The inadequacies of each of these provisions and the potential strength of the fourth amendment as a protection against IRS data bank searches are discussed in the following sections of this article.

III. INADEQUACIES OF CONSTITUTIONAL AND STATUTORY PROTECTIONS AGAINST IRS COMPUTER SEARCHES

A. Constitutionally Protected Rights

The constitution protects certain basic privacy rights from government intermeddling. Although the concept of a constitutional right of privacy is somewhat ephemeral, the right of privacy assumes at least three forms. "The first is the right of the individual to be free in his private affairs from governmental surveillance and intrusion. The second is the right of an individual not to have his private affairs made public by the government. The third is the right of an individual to be free in action, thought, experience, and belief from governmental compulsion."41 The right to be free from governmental surveillance and intrusion is grounded in the fourth amendment.42 The other two rights are grounded in, among other constitutional

40. See infra note 61. In Whalen v. Roe, 429 U.S. 589 (1977), the Supreme Court stated: "We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." 429 U.S. at 605.
42. Whalen v. Roe, 429 U.S. at 599 n.24.
provisions, the first and fifth amendments.\(^{43}\)

1. The Right of Privacy

The constitutionally protected right of privacy emanating from the first and fifth amendments create a protected zone of privacy encompassing "only [those] personal rights that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty.'"\(^{44}\) The activities ordinarily embraced by this zone of privacy relate to the intimate facets of an individual's personal life - marriage, procreation, contraception, family relationships, and child rearing and education.\(^{46}\)

In *Jaffess v. Secretary of HEW*, \(^{48}\) a federal district court refused to extend privacy rights to federal interagency transfers of data for computer cross-checking of veterans' benefits. More recently, though, the Fifth Circuit held that the constitutionally guarded "zone of privacy" encompasses an individual's interest in avoiding disclosure of personal matters.\(^{47}\)

The United States Supreme Court, in *Whalen v. Roe*, \(^{48}\) similarly construed the constitutional right of privacy as protecting against governmental disclosure of personal matters. The Court suggested that when the government maintains on computer data banks personal information concerning an individual's medical history, the government has a duty to safeguard against public disclosure of the confidential information.\(^{49}\) The Court, however, expressed no opinion as to whether privacy rights may prevent interagency transfers of such information.\(^{50}\)

Lower courts in applying *Whalen* have taken divergent ap-

\(^{43}\) Id.


\(^{45}\) Paul v. Davis, 424 U.S. 693, 713 (1976); Eisenstadt v. Baird, 405 U.S. 438 (1972). "If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child." 405 U.S. at 453 (emphasis in original).


\(^{47}\) Johnson v. IRS, 700 F.2d 971, 976 (5th Cir. 1983).

\(^{48}\) 429 U.S. at 599-600.

\(^{49}\) Id. at 599.

\(^{50}\) Cf. Jaffess v. Secretary of HEW, 393 F. Supp. 626, 629 (S.D.N.Y. 1975) (dissemination of personal information within the government not offensive to constitutional privacy).
approaches. While some courts only protect the confidentiality of traditional zones of privacy within the context of the home or family,51 other courts protect confidential information when the potential harm to an individual exceeds the benefits gained by the government.52 The lack of certainty among the courts as to the boundaries of an individual’s zone of privacy provides a data bank search subject with little assurance that traditional notions of privacy will prevent IRS computer searches.

2. The Right of Freedom of Association

Another protected interest, not within the zone of privacy, but encompassed by the first amendment, is the right of freedom of association. A restrictive reading of the right of association disfavors data bank search subjects. Based on the Supreme Court decision in *NAACP v. Alabama,*53 it may be argued that IRS data bank searches violate first amendment rights of freedom of association by selectively prosecuting individuals solely on the grounds of their association to a specific organization.

For example, if the IRS’ profile predictive model54 were to suggest that Libertarians constitute a large percentage of tax evaders, and on that assumption the IRS were to seek the records listing all followers of that belief, then the Libertarians’ associational rights may be violated. In practicality, no violation of associational rights has occurred when the information sought is necessary to protect a legitimate government interest.55 In all likelihood, application of the

---


52. See Doe v. Webster, 606 F.2d 1226, 1238 n.49 (D.C. Cir. 1979) (constitutional right to privacy limits the government’s ability to disseminate information about individual’s criminal records). See also Nixon v. Administrator of Gen. Serv., 433 U.S. 425, 458 (1977) (President’s primary interest in personal communications outweighed by government’s need for administrative information); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980) (employee’s privacy interest in medical records outweighed by government’s need for administrative information).

53. 357 U.S. 449 (1958). In this case, the Alabama State Attorney General sought disclosure of the Association’s membership list. The Supreme Court reversed the state court disclosure order, holding: “The immunity . . . is here so related to the rights of the members to pursue their lawful private interests privately and to associate freely with others in so doing as to come within the protection of the Fourteenth Amendment.” Id. at 466.

54. See *supra* notes 17, 28.

55. Baird v. Arizona, 401 U.S. 1, 6-7 (1971) (state inquiry into applicant’s past associations is a legitimate concern for admission to state bar); cf. Gibson v. Florida Legislative Investigating Comm., 372 U.S. 539, 546 (1963) (“an essential prerequisite to the validity of an investigation which intrudes into the area of constitutionally protected rights of speech, press, association and petition is that the State convincingly show a substantial relation between the
freedom of association test to IRS data bank searches would probably balance in favor of the government in recognition of the need to maintain 'fiscal responsibility.' The inadequacies of these constitutional provisions in restraining IRS computer data bank searches leaves an individual exposed to the vagaries of equally inadequate statutory provisions for protecting privacy.

B. Statutory Protections

While one may disparage the lack of definitive support amplifying constitutional civil rights for data bank subjects, no greater relief is to be found in statutory provisions. Even though there are numerous statutes tangentially related to data bank protections, the absence of a national policy or statutory scheme for dealing effectively with governmental transfer and disclosure of data leaves the data bank subject sorely in need of protection. One statute designed to grant some relief is the Privacy Act of 1974.


58. As one commentator observed:

An information disclosure policy of the federal government simply does not exist. The current diversity of federal agencies' policies regarding the handling of private information grew without statutory rhyme or reason. The lack of direction contributes to a suspicion which renders the collection and use of private sector information more difficult for all federal agencies. The suspicion could be significantly alleviated by a uniform federal policy on disclosure standards.

O'Reilly, Who's on First?: The Role of the Office of Management and Budget in Federal Information Policy, 10 J. OF LEGIS. 95, 133 (1983).
1. Privacy Act of 1974

One of the more important statutes intended to provide protection for data bank subjects is the Privacy Act of 1974 (the Privacy Act).\(^{59}\) Hurriedly enacted at the close of the 93rd Congress, the Privacy Act is the result of unreconciled Senate and House bills on privacy, later amended by a compromise bill developed by staff and members.\(^{60}\)

The preamble to the Privacy Act proclaims its purpose to be "to safeguard individual privacy from the misuse of federal records, to provide that individuals be granted access to records concerning them which are maintained by federal agencies, to establish a Privacy Protection Commission, and other purposes."\(^{61}\) The Privacy Act, however, has proven to be ineffective in curbing federal agency deprivations of civil rights.\(^{62}\)


60. The only record of the compromise amendment is a staff memo inserted into the Congressional Record. Many of the provisions of the Privacy Act are not explained in Committee reports. For a compilation of the legislative history, see the Privacy Act of 1974, Pub L. No. 93-579, 1974 U.S. CODE CONG. & AD. NEWS 6916-99.

61. Section 2(a) of the Privacy Act reiterates the congressional findings:

Sec.2.(a) The Congress finds that -

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.


62. The Privacy Protection Study Commission, established by § 5 of the Privacy Act, supra note 61, to study the issues raised by the legislation, concluded in its July 1977 report that the Privacy Act needs "significant modification and change if it is to accomplish its objective within the Federal government." PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 498 (1977). Similar conclusions were reached in the COMMISSION OF FEDERAL PAPERWORK, CONFIDENTIALITY AND PRIVACY 163 (1977).

At the first congressional oversight hearing of the Privacy Act since the law's enactment in 1974, the House Subcommittee on Government Information, Justice and Agriculture examined the Office of Management and Budget implementation and enforcement of the Privacy Act. Subcommittee Chairman Glenn English complained that "no one seems to consider any more
a. General Requirements of the Privacy Act

The primary principle underlining the Privacy Act is that the data subject should have a right to control access to information about himself and to prevent its use, without his consent, for purposes wholly unrelated to those for which it was collected. This principle is incorporated into the Privacy Act by restricting agency disclosures of personal data, and by requiring accountings of record disclosures. In addition, the Privacy Act provides that agencies must adhere to standards for the collection and maintenance of data in an accurate manner, as well as notice in the federal register of the existence and uses of such data. The Privacy Act also places restrictions on records relating to the data subject's exercise of his or her First Amendment rights. Both civil and criminal remedies are authorized for violations of the Privacy Act.

b. Exemptions from the Privacy Act

The Privacy Act provides for both general and specific exemptions from the restrictions on disclosures and transfers of data. The general exemption covers records maintained by the Central Intelligence Agency and other criminal law enforcement agencies. The whether the Privacy Act prohibits a particular use of information. As long as an agency publishes a routine use notice in the Federal Register it can do pretty much anything it wants with the information. Administration’s Fiscal Year Proposals: Hearings Before the Subcomm. on Gov’t Information, Justice and Agriculture, 98th Cong., 1st Sess. 115 (1983).

63. 5 U.S.C. § 552a(b).
64. 5 U.S.C. § 552a(c).
65. 5 U.S.C. § 552a(e). Agencies are under an affirmative duty to maintain accurate, relevant, timely and complete records under § (e)(5). Fiorella v. HEW, 2 G.D.S. ¶ 81,363 (W.D. Wash. 1981). The duty is not brought about merely by an individual's request to amend his records.

Publication requirements in the federal register are delineated at 5 U.S.C. § 552a(e)(11).
66. Subsection 552a(e)(7) states:
   Each agency that maintains a system of records shall maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.

67. 5 U.S.C. §§ 552a(g), (i). For further discussion on remedies under the Privacy Act, see infra notes 74-82 and accompanying text.
68. 5 U.S.C. § 552a(j). To qualify under the law enforcement exemption, an agency must have as its "principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities." § 5 U.S.C. 552a(j)(2). This provision allows for broad statutory interpretation. Although the
specific exemptions apply to classified records, law enforcement material not covered by the general exemption, Secret Service records concerning protection of government officials, statistical records, and certain personnel records.\textsuperscript{66} An additional exemption permits transfers of data "compiled in reasonable anticipation of a civil action or proceeding."\textsuperscript{70}

The general and specific exemptions stated above are not self-executing and may not be asserted by an agency in a particular case unless the agency has issued published regulations declaring it is exempt under the provisions. Therefore, most agencies issue regulations in order to take advantage of the Privacy Act's exemption requirements.

The Internal Revenue Service may satisfy the general law enforcement agency exemption since it enforces both civil and criminal laws governing the collection of revenue. A separate division of the Service, the Criminal Investigation Division (CID), is the most likely candidate to qualify under the law enforcement exemption, thus permitting the IRS to gain access to other agency data banks. Most likely, the IRS would liberally construe the specific exemption permitting transfers of information compiled in anticipation of civil actions.

A major exception to the prohibition against interagency transfers of information is the "routine use" exception.\textsuperscript{71} Information may be transferred to another agency if the data is declared a "routine use;" that is, if the information will be used "for a purpose which is compatible with the purpose for which it was collected."\textsuperscript{72} Because many agencies invoke the routine use exception without restraint due to ineffective supervision by the Office of Management and Budget, the routine use exception has proven to be an ineffective restriction on interagency transfers of data banks.\textsuperscript{73}

---

principal function of the IRS may not be criminal law enforcement, IRS agents are authorized to enforce the criminal provisions of the internal revenue laws. See supra note 21. Furthermore, as in other areas of law, the effectiveness of the IRS in collecting revenue depends to a large degree on the threat of enforcement of criminal laws.

69. 5 U.S.C. § 552a(k).
70. 5 U.S.C. § 552a(d)(5).
71. 5 U.S.C. § 552a(b).
73. As part of the Privacy Act, the Office of Management and Budget (OMB) was assigned the duty to "(1) develop guidelines and regulations for the use of agencies in implementing the provisions of [the Act] . . . ; and (2) provide continuing assistance to and oversight of the implementation of [the Privacy Act] . . . ." 5 U.S.C. § 552a.

The duty was reiterated in the Paperwork Reduction Act of 1980 (PRA), 44 U.S.C. §§ 3401-3420, requiring OMB to continue to monitor agency compliance with the Privacy Act.
c. **Remedies under the Privacy Act**

The remedial provisions of the Privacy Act contain both criminal penalties for violations by officers and employees and a civil remedial scheme for agency violations of the Privacy Act. The remedial scheme has been criticized as ineffective.

Different remedies are available for violation of different provisions of the Privacy Act. If a data subject is denied access to and amendment of his data file, a district court may enjoin the offending agency and order such amendment. If an agency intentionally or willfully fails to comply with the provisions of the Privacy Act in such a way as to have an adverse effect on a data subject, the court may award damages of not less than $1,000.

In one of the few cases granting damages for willful violations, the Fifth Circuit in *Johnson v. Department of the Treasury* upheld an award of the minimum $1,000 damages against the IRS for fail-

---

74. 5 U.S.C. § 552a(i)(1).
75. 5 U.S.C. § 552a(g)(1).
77. Agency conduct subject to civil action is identified at 5 U.S.C. §§ 552a(g)(1)(A)-(D), with remedies specified in subsections (g)(2)-(4).
78. 5 U.S.C. §§ 552a(g)(1)(A), (g)(3)(A).

80. 700 F.2d 971 (5th Cir. 1983).
ing to collect information, to the greatest extent practicable, directly from the subject of a tax violation investigation. The court also remanded the matter for further findings of fact to determine appropriate damages for mental anguish and physical injuries. This decision appears to have limited application to a challenge of IRS computer matching since the IRS has express authority under the law enforcement exemption to gather information directly from other agencies' data banks.

Injunctive relief under the Privacy Act is available only in instances where a request to gain access to records or to amend records has been denied. To redress other violations of the Privacy Act, such as unauthorized interagency transfers of data, the data bank subject is limited to filing a damages action.

d. Overall Ineffectiveness of the Privacy Act

Far from attaining the law's proclaimed purpose, the Privacy Act has proven to be ineffective in protecting data bank subjects from interagency transfers and disclosures of data. At the first Congressional oversight hearing on the Privacy Act since its enactment in 1974, the House Subcommittee on Government Information, Justice and Agriculture reviewed the Office of Management and Budget (OMB) implementation of the Privacy Act. During the hearings the Subcommittee Chairman expressed dismay over the dearth of OMB guidance to agencies in recent years, the failure to meet statutory deadlines for reports to Congress, and the growing abuse of the "routine use" exception in computer matching programs. Despite these shortcomings, the OMB Director of Information and Regulatory Affairs asserted that "the Act is working well for the most part," and stated that he did not "see any evidence [that application of the routine use exemption] is running roughshod over the Privacy Act." The Director did, however, acknowledge the vagueness of OMB's 1975 guidelines which require only a "programmatic nexus" between the use of the data proposed by one agency and the original reason asserted by another agency for collecting data from a

81. See supra note 78 and accompanying text.
82. Edison v. Department of Army, 672 F.2d 840, 846 (11th Cir. 1982); Parks v. IRS, 618 F.2d 677, 684 (10th Cir. 1980).
83. Oversight of the Privacy Act of 1974, Subcomm. on Gov't Information, Justice, and Agriculture, 98th Cong., 1st Sess. 98 (1983) [hereinafter cited as Oversight of Privacy Act].
84. Id. at 81-93 (statement by Glen English, Subcomm. Chairman).
85. Id. at 60-61, 118 (testimony by Christopher DeMuth, OMB Dir. of Information and Regulation Affairs).
Earlier, in hearings before the Subcommittee on Oversight of Government Management, a stark narrative of the ineffectiveness of the Privacy Act was presented. As compared to the 1979 OMB guidelines on federal computer matching programs, the 1982 guidelines contain no requirements or limitations on computer matching with regard to certain fundamental areas of concern. For instance, all data bank information is subject to matching, no matter how personal or sensitive the material. The new guidelines do not require that an agency assure due process of law to a data bank subject once the computer match makes a "hit.

Furthermore, agencies are no longer required to submit cost-benefit analyses and reports for computer matching programs. With such lax requirements, it is not surprising that OMB has approved every computer matching program since the inception of the Privacy Act. For these reasons, one of the speakers at the hearings stated that "it is difficult not to conclude that computer matching is a totally unregulated business. . . ." Consequently, the ineffectiveness of the Privacy Act leaves the fourth amendment as the sole potential protection against IRS data bank searches.

IV. FOURTH AMENDMENT SEARCH AND SEIZURE PROTECTIONS

In the absence of effective legislative protections, and given the uncertainty of other constitutional protections available to data bank subjects, the fourth amendment may be the last source of protection against IRS computer data bank searches. The fourth amendment has long served as a protective device against overambitious law enforcement. The Supreme Court, in G.M. Leasing Corp. v. United

86. Id. at 90, 94.
88. Id. at 275-76.
91. Oversight of the Privacy Act, supra note 83, at 113.
93. "Where Congress has authorized [government] inspection [of personal records] but made no rules governing the procedure that inspectors must follow, the Fourth Amendment and its various restrictive rules apply." Colonade Catering Corp. v. United States, 397 U.S. 72, 77 (1970); See v. City of Seattle, 387 U.S. 541, 543-46 (1967); United States v. Deak-
States, declared that "...one of the primary evils intended to be eliminated by the Fourth Amendment was the massive intrusion on privacy undertaken in the collection of taxes [during colonial times] pursuant to general warrants and writs of assistance." The Internal Revenue Service in the furtherance of tax enforcement is not licensed to disregard the fourth amendment.

Modern day matching of computer data banks by the IRS in the hope of finding a tax violator may very well constitute a general search in contravention of the fourth amendment. Since the primary purpose of the fourth amendment is to protect personal privacy and dignity against unwarranted government intrusion, IRS computer matching of data banks arguably violates one of the fundamental rights of a free society. To invoke protection of the fourth amendment search and seizure clause, the victim must establish that the government unreasonably intruded upon matters over which the victim has a reasonable expectation of privacy.

A. Expectations of Privacy in Private Data Banks

The fourth amendment prohibits unreasonable searches and seizures, and requires that a warrant be based upon probable cause,


The fourth amendment to the Constitution provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. Amend. IV.

94. 429 U.S. 338 (1977). In G.M. Leasing Corp., in order to satisfy a tax assessment against a taxpayer, IRS agents made warrantless searches and seizures of the taxpayer's records and documents, along with his levied automobiles. The Court held that intrusions into taxpayer's privacy without a warrant for the purpose of collecting taxes violated the fourth amendment. 429 U.S. 338.

95. Id. at 355 (citing T. Taylor, Two Studies in Constitutional Interpretation 35-41 (1969); N. Lasson, The History and Development of the Fourth Amendment to the United States Constitution 51-78 (1937); J. Landynski, Search and Seizure and the Supreme Court 30-42 (1966)). One of the early causes of the American Revolution was disdain for general writs of assistance. Cave v. Superior Court, 267 Cal. App. 2d 517, 521, 73 Cal. Rptr. 167, 170 (1968). During Colonial times, a writ of assistance specified only the object of the search—goods on which colonists had evaded paying taxes. With carte blanche authority, British customs officials were "completely free to search any place where they believed such goods might be." Steagald v. United States, 451 U.S. 204, 220 (1981).

96. 429 U.S. at 355.

97. See infra notes 155-170 and accompanying text.


99. See infra notes 102-108 and accompanying text.
particularly describing the place to be searched and the persons or things to be seized. A search in the context of the fourth amendment is defined as an exploratory investigation, quest, or invasion into places either concealed or intended to be private. Thus, a search encompasses governmental intrusions into matters over which one has a justifiable expectation of privacy. Intrusion into, or observation of that which a person knowingly exposes to the public, even in his own home or office, is not a search. However, intrusion into what a person seeks to preserve as private, even in an area open to the public, may be a search subject to restrictions by the fourth amendment.

The “subjective expectation of privacy” test is a two-prong test set forth in Justice Harlan’s concurring opinion in Katz v. United States: “First . . . a person [must] have an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’” Recently, the second prong of the Katz test has been the focus of the Court’s analysis. The objectivity element of the second prong attempts to balance the individual’s interest in conducting his affairs in private against the public’s interest in thwarting criminal activity by intensive investigation. Despite repeated protests by dissenting Supreme Court justices, this test does not recognize an absolute immunity from searches of highly personal matters.

100. U.S. Const. Amend. IV. See supra note 93.


102. Katz v. United States, 389 U.S. 347, 351-52 (1967) (Harlan, J., concurring). The majority opinion, authored by Justice Stewart, does not refer to a subjective analysis. It states that the government conduct directed at Katz “violated the privacy upon which he justifiably relied.” Id. at 353.

103. Terry v. Ohio, 392 U.S. 1 (1968) (“wherever an individual may harbor a reasonable ‘expectation of privacy’ . . . he is entitled to be free from unreasonable governmental intrusion.”); Vreeken v. Davis, 718 F.2d 343, 347 (10th Cir. 1983).

104. Id. at 361 (Harlan, J., concurring). The majority opinion, authored by Justice Stewart, does not refer to a subjective analysis. It states that the government conduct directed at Katz “violated the privacy upon which he justifiably relied.” Id. at 353.

105. Id. at 361.


107. Justice Douglas, dissenting in Warden v. Hayden, 387 U.S. 294 (1967), asserted that the Constitution “creates a zone of privacy that may not be invaded by the police through
Traditionally, the Supreme Court has limited an individual's "constitutionally protected areas" to those enumerated in the fourth amendment: persons, houses, papers, and personal effects. In *Katz*, it appeared that the Supreme Court was prepared to extend an individual's zone of privacy beyond traditional limits. More recently, though, the Court has favored "effective law enforcement," indicating that one's zone of privacy does not insulate all personal activities and possessions. Today, no clear rule exists as to what constitutes a "reasonable expectation of privacy." The United States Supreme Court has yet to rule on the applicability of the fourth amendment to computer data bank searches.

In the area of personal banking records, the Supreme Court held in *United States v. Miller* that a defendant had no justified expectation of privacy in his financial records held by his bank since his records were not "private papers." The Court found the de-
defendant to have no legitimate expectation of privacy because the bank checks were negotiable instruments used in commerce, and because the documents contained information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. The Court concluded that copies of defendant's checks, deposit slips, financial statements and monthly statements were the business records of the bank, thus conveying property rights to the bank, not to the defendant bank customer. 118

Despite the doctrinal basis of *Katz* which abandoned the notion of property rights as a necessary element of privacy, 119 the *Miller* court asserted that an individual with "neither ownership nor possession" 120 in his records has no protected fourth amendment interest. This conclusion is contrary to the reasoning of *Katz* and *Jones v. United States*, 121 which "explicitly did away with the requirement that to establish standing one must show legal possession or ownership of the searched premises. . . ." 122 Furthermore, the Court's presupposition that the banking customer consented to the search because he assumed the risk of disclosure by the bank to government authorities conflicts with the Court's earlier decisions in *Bumper v. North Carolina*, 123 and *Mancusi v. DeForte*. 124

because it did not provide notice to depositors upon issuance of a subpoena for records. The Court dispelled this argument on the grounds that plaintiff was prematurely asserting an injury when the Service had yet to subpoena its records from the bank. Although that issue was left unresolved, the Right to Financial Privacy Act of 1978 later corrected this infirmity. See *infra* note 127 and accompanying text.

118. 425 U.S. at 440.

119. "*Katz v. United States* [389 U.S. 347] makes it clear that capacity to claim the protection of the [fourth] Amendment depends not upon a property right in the invaded place but upon whether the area was one in which there was a reasonable expectation of freedom from governmental intrusion." *Mancusi v. DeForte*, 392 U.S. 364, 368 (1968).

120. 425 U.S. at 440.


123. 391 U.S. 543 (1968). In *Bumper*, the Court recognized that although a third person may own and possess the incriminating material being sought, the search victim is nevertheless entitled to fourth amendment protections for the reason that the victim is the "one against whom the search [is] directed." 391 U.S. at 548, quoting *Jones v. United States*, 362 U.S. at 261. Therefore, even though the search victim in *Bumper* may have assumed the risk that his grandmother would consent to a search of her home for the alleged murder weapon (a rifle which the grandmother owned), the search victim retained standing to challenge the validity of the search. 391 U.S. at 548.

124. 392 U.S. 364 (1968). In *Mancusi* the Court held that plaintiff, by voluntarily exposing his books and records to other occupants of his office, did not thereby grant consent to a search of such materials by state officials. Plaintiff held a reasonable expectation of privacy in the books and records despite the fact that the materials were subject to scrutiny by co-occupants of plaintiff's shared office space.
Nevertheless, the facts in *Miller* are distinguishable from the circumstances surrounding an IRS computer search. *Miller* involved a search of defendant’s checks voluntarily placed into the public stream of commerce, whereas an IRS computer search of taxpayer information retained by government agencies involves a search of information obtained by the government through compulsion.\(^{126}\) Most information held by government agencies is demanded in exchange for licenses and benefits, the denial of which would frustrate a citizen’s ability to function in today’s society.

The *Miller* Court acknowledged this distinction between obtaining information by compulsion, and by free will. However, rather than finding the distinction persuasive, the Court instead proceeded to distinguish *Burrows v. Superior Court*,\(^{126}\) a California Supreme Court case which held that the defendant had a reasonable expectation of privacy in his bank records worthy of fourth amendment protection against searches without legal process.\(^{127}\)

---

125. Compulsory production of one’s books and records to be used in a criminal or penal proceeding is restricted by the fourth amendment. Boyd v. United States, 116 U.S. 616 (1886). See also Schmerber v. California, 384 U.S. 757, 767-68 (1966) (compulsory production of blood sample for testing of alcoholic content restricted by fourth amendment considerations).

126. 13 Cal. 3d 238, 529 P.2d 590, 118 Cal. Rptr. 166 (1974) (bank records obtained by sheriff and prosecutor without legal process but with consent of a bank was held an illegal search and seizure), cited in *Miller*, 425 U.S. at 445 n.7.

127. 13 Cal. 3d at 247, 529 P.2d at 596, 118 Cal. Rptr. at 172.

Justice Mosk of the California Supreme Court advised:

To permit a police officer access to these records merely upon his request, without any judicial control as to relevancy or other traditional requirements of legal process, and to allow the evidence to be used in any subsequent criminal prosecution against a defendant, opens the door to a vast and unlimited range of very real abuses of police power.

*Id.* at 247, 529 P.2d at 596, 118 Cal. Rptr. at 172.


Justice Brennan, in full agreement with the California Supreme Court analysis, asserted in his dissent in *Miller* that lack of notice to a bank customer upon disclosure of his records to the government was a “fatal constitutional defect” to fourth amendment rights. 425 U.S. at 448 n.2. Interestingly, Congress subsequently enacted the Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-22 (1982) which require that a copy of any federal subpoena or summons for financial records be served on the customer with full notice of his right to challenge the subpoena or summons in court prior to its execution 10 days hence, unless a “protective order” is obtained upon a showing that such notice would jeopardize the investigation.
In *Smith v. Maryland*, a case involving the government’s use of a “pen register” to record the numbers dialed from an individual’s telephone, the United States Supreme Court held that an individual has no legitimate expectation of privacy in his telephone records. As in *Miller*, the Court based its decision on the theory that defendant telephone subscriber *voluntarily* conveyed the dialing numbers to the telephone company in the ordinary course of business, thereby implicitly consenting to interception by the government pen register.

When the California Supreme Court was faced with nearly the same facts in *People v. Blair*, it held contrary to the United States Supreme Court based upon its interpretation of the California Constitution - that an individual does have a reasonable expectation of privacy in his telephone records. Unlike the *Smith* Court’s contention that telephone subscribers assume the risk that the telephone company will automatically reveal telephone records to police, Justice Mosk of the California Supreme Court expressed the belief that telephone subscribers justifiably expect that use of their records will be limited to necessary internal telephone company accounting functions. Likewise, the New Jersey Supreme Court refuted the *Smith* rationale, and instead interpreted the New Jersey Constitution in *State v. Hunt* in a manner consistent with the California Su-

---

129. A pen register is an electronic device attached to a telephone line which intercepts telephone calls and records the numbers dialed. See 1 W. LaFave, *Search and Seizure* § 2.7(b) (1978).
131. 442 U.S. at 743. The Court explained:

> Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.

*Id.*

133. 25 Cal. 3d at 653, 602 P.2d at 746, 159 Cal. Rptr. at 826.
134. *State v. Hunt*, 91 N.J. 338, 450 A.2d 952 (N.J. Sup. Ct. 1982) (telephone toll billing records seized without judicial sanction or proceeding). Despite the court’s recognition of prior Supreme Court decisions disallowing fourth amendment protections for telephone toll records, Justice Scheiber of the New Jersey Supreme Court nonetheless asserted:

> The telephone caller is entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. [*Katz v. United States,*] 389 U.S. at 352 (1967). Similarly, he is entitled to assume that the numbers he dials in the privacy of his home will be recorded solely for the telephone company’s
preme Court's reasoning in Blair.

The California Constitution135 and the New Jersey Constitution136 contain language virtually identical to that found in the fourth amendment. Yet the divergence of opinions between Smith, on the one hand, and Blair and Hunt on the other, suggests that the United States Supreme Court is granting greater deference to law enforcement than are state courts. The divergence of opinions appears most acute in cases involving searches which employ contemporary technology.

While the United States Supreme Court denies an expectation of privacy once the information or records leave the hands or lips of the individual, the state forums maintain that privacy rights continue to exist beyond the point of collection of information by the third party. The state courts imply societal expectations of privacy demanding third party recipients to adhere to a fiduciary duty respecting the confidentiality of the information obtained. The United States Supreme Court, on the other hand, asserts that privacy expectations end because the defendant has assumed the risk that information revealed to third parties will be transferred to others.137

The United States Supreme Court finds solace in believing that the individual has the option whether or not to release information through conduits of communication and channels of commerce. For example, the Smith court draws no distinction between impairment to privacy when personally dialing telephone calls and when placing calls through an operator.Positing that central computer switching equipment for telephone operations is the modern counterpart of operators, the Smith court dismissed defendant's claim that the computerized equipment actually assures a greater expectation of privacy. Yet computers do assure greater privacy protection if guarantees exist to prevent government officials from tapping into the data banks.

Computer data banks theoretically serve to enhance data pri-

---

135. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable seizures and searches, shall not be violated. . . ." CAL. CONST. art. I, § 13.

136. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no warrant shall issue except upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the papers and things to be seized." N. J. CONST. art. I, par. 7.

137. The lack of protections availed by federal law suggests that a complaint couched in terms of state law assures greater chances of obtaining protection. See, e.g., Pruneyard Shopping Center v. Robins, 447 U.S. 74 (1980) (California Constitution conferring greater rights and protections than United States Constitution).
vacy by confining the information to densely packed electromagnetic files; access to the files is restricted to those persons having a valid password. With a computer, there is no need for human contact with specific data except at the initial stage of inputting it into the system. Thereafter, the data in each file retains anonymity until matched with identifying names or numbers in association with an individual, or when retrieved for viewing upon a screen or printer. Nevertheless, if mismanaged or abused, computer data banks pose a serious threat to privacy.

The ability to electromagnetically search or sort through massive arrays of data files is a distinctive feature of computers. When a computer search becomes a dragnet combing through data files to match incriminating evidence, the technological advantage of computers seriously impinges on legitimate expectations of privacy.

B. Expectations of Privacy in Government Data Banks

Statutory restrictions, custom and private remedies serve to create or reinforce societal expectations of privacy. Notwithstanding

138. For the purpose of securing the privacy of tax return information held on all individuals by the IRS, only IRS personnel with personal passwords may review the files of tax information on IRS data banks. The amount of information available for perusal varies with the level of entry authorized. The security system also monitors on a daily basis all individuals who have accessed data. COMPUTER TECHNOLOGY AT IRS, supra note 3, at 54-55.

The cursory nature of governmental handling of individual records provides government employees with little opportunity to inspect the personal data. The tremendous volume of records simply does not physically permit it. Therefore, government contact with the information during the inputting stage is minimal.

139. To be sure, the Constitution and Bill of Rights are not to be read as covering only the technology known in the 18th century. Otherwise its concept of "commerce" would be hopeless when it comes to the management of modern affairs. At the same time the concepts of privacy which the Founders enshrined in the Fourth Amendment vanish completely when we slavishly allow an all-powerful government, proclaiming law and order, efficiency, and other benign purposes, to penetrate all the walls and doors which men need to shield them from the pressures of a turbulent life around them and give them the health and strength to carry on.


140. With the advent of telecommunications, data files can be dispursed or published in a matter of seconds throughout the world. See generally COMPUTER-BASED NATIONAL INFORMATION SYSTEMS, supra note 6, at 137-38.

141. "The computer storage and easy accessibility of computerized data vastly increases the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology." Whalen v. Roe, 429 U.S. 589, 609 (1977) (Brennan, J. concurring).

142. "Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present." United States v.
the fact that the Privacy Act of 1974 and other legislation fail to safeguard privacy interests in government maintained data banks,143 the purported purpose of the legislation does serve to raise expectations of statutory protection over privacy interests in such data.144 But for poor drafting by Congress and incompetent oversight and regulation by the Office of Management and Budget, the Privacy Act would have extended some degree of protection against IRS computer data bank searches. Legitimate societal expectations of privacy simply should not be compromised by infirm legislation.

The Freedom of Information Act (the FOIA),146 unlike the Privacy Act, was enacted to facilitate the release of information from the


144. The Tax Reform Act of 1976 extends some privacy protection to data held on individuals by the Internal Revenue Service. The Act reverses the former status of non-confidentiality of individual tax returns and return information. Formerly the law stated that tax returns were public, with certain exceptions. Under the Tax Reform Act, returns are confidential, with certain exceptions. Returns may be disclosed with the consent of the taxpayer, upon written request of state tax authorities or estate administrator, to committees of Congress, to the Dept. of Justice or Treasury for tax investigations, for statistical surveys and to locate parents failing to meet their child support obligations. I.R.C. § 6103.

In Rodgers v. United States, 697 F.2d 899, 906 (10th Cir. 1983), even though the taxpayer in litigating issues in his tax return caused the return to become a matter of public record, the court held that an IRS agent's disclosure to a third person of the tax information in the return was unlawful. The IRS agent argued that there can be no reasonable expectation of privacy with respect to matters of public record. The court disagreed, but on different grounds, stating that "[t]he issue . . . [does not involve] the loss of 'confidentiality' or 'privacy,' but, rather, . . . [the existence of] an unauthorized disclosure of tax return information in violation of § 6103. . . . Even assuming the loss of confidentiality in the context of the statements, we hold that the . . . disclosure was clearly unauthorized." 697 F.2d at 906. However, the court failed to recognize that, in enacting I.R.C. § 6103, Congress placed great weight on the importance of preserving expectations of privacy and confidentiality in tax return information. See H.R. REP. NO. 658, 94th Cong., 2d Sess. 1, 316-17, reprinted in 1976 U.S. CODE CONG. & AD. NEWS 2897, 3746-47.

145. 5 U.S.C. § 552.
Equally important, though, the FOIA contains nine prohibitions against disclosure of government-maintained information, the most significant prohibition being the non-disclosure of "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." The FOIA recognizes that society demands a certain degree of privacy protection in government-maintained data banks. Furthermore, the FOIA clearly acknowledges that privacy rights remain affixed to personal data files even after the government comes into possession of the data. The Supreme Court likewise acknowledged the personal nature of private information held by the government and exempted under the FOIA.

In *United States v. Deak-Perera & Co.*, the District of Columbia district court held that a general sharing of information concerning a taxpayer, even if shared intra-agency, is prohibited if it would violate the subject's legitimate expectation of privacy. Similarly, in *United States v. Sells Engineering, Inc.*, the Supreme Court held that in the absence of a court order the Department of Justice may not transfer grand jury materials from its criminal to its civil division. The Court sought to protect the legitimate expectation of privacy in testimony compelled from witnesses, and to quell fears that the testimony would be used in other governmental civil litigation and administrative actions. Based on these statutorily and ju-
dially created expectations of privacy, an individual may assert a legitimate expectation of privacy in government-maintained files containing personal information, and thereby challenge the validity of the computer data bank search as a general search unsupported by probable cause in violation of the fourth amendment.164

C. General Searches

Computer matching of data banks by the IRS exhibit many of the indicia of a general exploratory search typical of general writs of assistance prohibited by the fourth amendment.168 Dreading general writs of assistance which invaded the privacy of American colonists, the Constitution’s framers drafted the fourth amendment with the intention of preventing overambitious government officials from searching and seizing what they might please.166

In order to limit the scope of a search and to verify its lawfulness, the fourth amendment requires that a magistrate issue a warrant upon oath or affidavit of an officer particularly describing the person or place to be searched.167 Full-blown searches, dragnets, wholesale rummaging through possessions, or “fishing expeditions” in search of potential evidence are prohibited by the fourth amendment; such exploratory searches cannot be undertaken by the govern-

another would “threat[en] the willingness of witnesses to come forward and to testify fully and candidly. If a witness knows or fears that his testimony before the grand jury will be routinely available for use in governmental civil litigation or administrative actions, he may well be less willing to speak for fear that he will get himself into trouble in some other forum.” 103 S. Ct. at 3142.

The Court also expressed its concern for the unfair advantage the government would gain by obtaining access to private materials, stating that “the limitations imposed on investigation and discovery exist for sound reasons—ranging from fundamental fairness to concern about burdensomeness and intrusiveness.” 103 S. Ct. at 3142-43.

154. Recent polls reflect an increasing societal concern over privacy of data banks and expectations of restraints on use of government and private data banks. COMPUTER-BASED NATIONAL INFORMATION SYSTEMS, supra note 6, at 78, (citing The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy (1979)).

See infra notes 155-170 and accompanying text for an analysis of general searches and notes 171-190 and accompanying text for an analysis of probable cause.


156. Stanford v. Texas, 379 U.S. 476. Justice Stewart, concurring in Stanley v. Georgia, 394 U.S. 557 (1969), stated that: “The purpose of [the fourth amendment] was to guarantee to the people of this Nation that they should forever be secure from the general searches and unrestrained seizures that had been a hated hallmark of colonial rule under the notorious writs of assistance of the British Crown.” 394 U. S. at 569 (quoting Stanford v. Texas, 379 U.S. at 481).

ment with or without a warrant. Likewise, it is arguable that a
generalized search through computer data banks constitutes a mas-
sive dragnet into the private affairs of substantial numbers of
persons.

Search techniques which indiscriminately pry into society's
zones of privacy are inherently unlawful unless restricted to narrow
applications. For example, trained narcotics-detecting police dogs,
if used indiscriminately, represent an invasion of one's expectation of
privacy. Similarly, 'wholesale frisking' of the general public with
magnetic scanners in order to locate weapons and to prevent future
crimes is not justified. Random detentive searches of large num-
bers of persons without objective facts giving rise to a suspicion of
illegality are impermissible, unless an officer can point to an indi-
vidualized, articulable suspicion of the persons searched.

An unlimited search of all of an individual's personal financial
records held by a third party is impermissible. Indeed, the Su-
preme Court's decision in *United States v. Miller* justified, in part,
the search and seizure of a depositor's financial records held by a
bank on grounds that the Government had exercised its investigative
powers under the legal restraints of a narrowly defined subpoena
duces tecum. Had the search in *Miller* been a general search
through all records, the requirements of the administrative sum-
mons—the typical IRS procedure for obtaining information con-
cerning a taxpayer—would not have been satisfied.

---

F.2d 418 (9th Cir. 1978).
159. Marron v. United States, 275 U.S. 192 (1927); VonderAHE v. Howland, 508 F.2d
364 (9th Cir. 1974).
160. "The increasing use of dogs, in airports and elsewhere, to detect contraband exem-
plifies the 'powerful hydraulic pressures' to 'water down constitutional guarantees.'" United
States v. Beale, 674 F.2d 1327, 1331 n.5 (9th Cir. 1982) (quoting Terry v. Ohio, 392 U.S. 1
(1968) (Douglas, J., dissenting)), rev'd on remand, 736 F.2d 1289 (1984), in light of, United
States v. Place, 103 S. Ct. 2637, 2644 (1983) (holding that a search does not occur when
travelers' luggage in an airport is sniffed by a narcotics detection dog).
161. United States v. Davis, 482 F.2d 893, 908 (9th Cir. 1973). "There is an obvious
danger . . . that the screening of passengers and explosives will be subverted into a general
search for evidence of crime." 482 F.2d at 909.
162. International Ladies' Garment Workers' Union v. Sureck, 681 F.2d 624, 639 (9th
Cir. 1982).
F.2d 1147 (9th Cir. 1980).
165. United States v. Miller, 425 U.S. at 446 n.6.
167. Baldwin v. C.I.R., 648 F.2d 483, 488 (8th Cir. 1981) ("overbroad IRS informa-
tional probe may infringe upon constitutionally protected rights"); United States v. Life Sci-
seem reasonable to expect that since legislatively prescribed administrative summonses must be limited in scope to relevant materials, an IRS computer search of data banks should likewise be limited in scope to less than a general search.

Administrative summons procedures also require that the data subject receive notice within three days of the issuance of the summons to a third-party record-keeper. Conversely, a data bank subject receives no notice of IRS computer data bank searches. Under the Privacy Act, an agency is required to publish in the federal register the scope and use of data banks; however, the federal register notice requirement does not apply to criminal law enforcement searches. Therefore, IRS computer searches, lacking the specificity of a warrant or notice, proceed under the guise of criminal investigation unrestrained by legal process. Without satisfying the restrictions of the fourth amendment, the IRS is at liberty to conduct a full-blown search of data banks—from A to Z, numbers 1 to 250,000,000—to discover any possible evidence of wrongdoing. This is clearly a general search.

D. Probable Cause

A general search by computer is instituted in the absence of any pre-existing evidence to justify suspicion of wrongdoing by the data bank subjects. Since a general search by computer is not even premised on "mere suspicion," the fourth amendment requirement of probable cause is not met. The fourth amendment requires that searches intruding upon an individual's privacy be justified by probable cause, as determined by a neutral and detached magistrate. If probable cause is found, then the warrant must particularize the items sought so as to prevent a general search.

Probable cause for a search exists when known facts and circumstances are sufficient to warrant a reasonably prudent person to

---

168. I.R.C. § 7609(a).
169. See supra note 65.
170. 5 U.S.C. § 552a(j). See also supra note 66.
172. Brinegar v. United States, 338 U.S. 160, 176-77 (1949) (probable cause for a search warrant requires "less than evidence which would justify . . . conviction," yet "more than mere suspicion.").
believe that criminally-related objects or incriminating evidence will be found in the place which the warrant authorizes to be searched.\textsuperscript{178} The actual level of proof required is subject to dispute and difficult to quantify. A significantly lower quanta of proof is required to establish probable cause than guilt;\textsuperscript{179} nevertheless, there must be some objective facts to raise suspicions that criminal activity is occurring.\textsuperscript{177} Mere suspicion or expectation that an item may incriminate a defendant is not sufficient.\textsuperscript{178}

Courts typically analyze probable cause in terms of weighing the need to search against the invasion of privacy.\textsuperscript{178} In practical application, though, courts more typically deal with probable cause in terms of probabilities—that it was more probable than not that a certain person committed an offense.\textsuperscript{180}

The probability that one among many data bank subjects is violating the internal revenue laws is so remote, at least on a statistical basis, that probable cause is not satisfied.\textsuperscript{181} Yet when dealing with over two hundred million potential suspects, the only sensible way to analyze probable cause appears to be on a statistical basis. The IRS reports that the noncompliance rate for persons not voluntarily re-

\begin{itemize}
  \item \textsuperscript{175} Zucher v. Stanford Daily, 436 U.S. 547, 556-57 n.6 (1978) (citing with approval Amsterdam, \textit{Perspectives on the Fourth Amendment}, 58 Minn. L. Rev. (1974)).
  \item \textsuperscript{176} United States v. Davis, 458 F.2d 819, 821 (D.C. Cir. 1972) (the standard of probable cause required to arrest). It appears that the quanta of evidence required for a search is the same as that for an arrest. See Zucher v. Stanford Daily, 436 U.S. 557 n.6 (citing with approval Comment, 28 U. Chi. L. Rev. 664, 687 (1961)).
  \item \textsuperscript{177} United States v. Cortez, 449 U.S. 411, 417 (1981) (the standard of probable cause required for an investigatory stop); International Ladies' Garment Workers' Union v. Sureck, 681 F.2d at 635.
  \item \textsuperscript{178} United States v. Dichiarinte, 445 F.2d 126, 129 n.2 (7th Cir. 1971).
  \item \textsuperscript{180} Brinegar v. United States, 338 U.S. at 175 ("In dealing with probable cause . . . as the very name implies, we deal with probabilities."); Illinois v. Gates, 103 S. Ct. 2317, 2328 (1983).
  \item \textsuperscript{181} See generally Coates, supra note 2; IRS NON-COMPLIANCE STUDY, supra note 13.
\end{itemize}
porting income is about ten percent. Of the roughly two hundred million persons listed as subjects in agency data banks, the noncompliers would represent five to eight percent. Therefore, the optimum "hit" rate, or probability of identifying a tax evader through computer searches, is at best eight percent, or less than one in ten. It would seem fallacious to conclude that it is more probable than not that each data bank subject is violating the internal revenue laws.

With respect to whether any crime has in fact occurred, courts typically require a higher level of probability for identifying unknown criminal activity than for identifying specific perpetrators of known criminal activity. This position is justifiable since the limited activity of identifying the perpetrator of a known criminal offense is far less offensive to expectations of privacy than is the operation of attempting to identify a suspected yet unknown criminal offense; the latter is the function of IRS computer data bank searches.

Under conventional methods of identifying unknown perpetrators of suspected unlawful activity, the IRS must abide by the requirements of a "John Doe" summons. The IRS may serve a John Doe summons only if it can prove in an *ex parte* petition to a district court judge that:

1. the summons relates to the investigation of a particular person or ascertainable group or class;
2. that there is a reasonable basis for believing that the person or group may fail or has failed to comply with a tax law; and
3. that the information sought, as well as the identity of the person or persons to which the information relates, is not readily available from other sources.

The stringent requirements of a "John Doe" summons are intended to prevent the IRS from using such summonses to engage in "fishing expeditions." Computer searches by the IRS seem to be precisely the type of fishing expedition which Congress intended to prohibit. At the very least, the IRS should be required to adhere to the con-

182. Coates, supra note 2.
183. "I am not yet ready to agree that America is so possessed with evil that we must level all constitutional barriers to give our civil authorities the tools to catch criminals." California Bankers' Assoc. v. Shultz, 416 U.S. 21, 86 (1974) (Douglas, J., dissenting).
184. See 1 W. LaFAVE, SEARCH AND SEIZURE § 3.2 (Supp. 1984).
186. 712 F.2d at 1345 (emphasis added).
187. Id. at 1346 (quoting In re Tax Liabilities of John Does, 688 F.2d 144, 149 (2d. Cir. 1982)).
straints of a John Doe summons before commencing its computer searches.

When the Constitution's framers enacted the fourth amendment, hoping to eliminate the "primary evil" of intrusive tax collection, they understood the necessity of restraining searches with the requirements of specificity and probability. Current administrative summons provisions which attempt to curb IRS fishing expeditions also incorporate essential elements of the fourth amendment. Present day computer searches of data banks, contrariwise, circumvent the essential elements of probability and specificity embodied in the fourth amendment and administrative summonses. Until the Internal Revenue Service complies with the essentials of the fourth amendment, an invasion of a data bank subject's expectation of privacy in data concerning his or her personal affairs should justify a cause of action under the fourth amendment's search and seizure clause.

V. Conclusion

With the dramatic increase in taxpayer noncompliance, the Internal Revenue Service perceives a justification for utilizing computer searches of data banks to identify tax evaders. Having access to thousands of data banks, including those of government agencies networked throughout the country by the latest in computer technology, the IRS can hunt through millions of records concerning the most intimate details of citizens' lives. Surreptitious searches of data bank subjects by the IRS without restraint raises possible violations of constitutional protections. Yet case law relating to possible invasions of an individual's privacy and associational rights do not supply necessary protections to a data bank subject. Nor do numerous statutory provisions, such as the Privacy Act of 1974, afford the individual any substantive protection.

In light of the absence of effective constitutional and statutory protections against IRS computer data bank searches, the fourth amendment may be the only restraint on the IRS against such searches. Because an individual possesses a legitimate expectation of privacy in his personal data maintained in computer data banks, the

188. See supra notes 94-95 and accompanying text.
190. See supra notes 155-170 and accompanying text for a discussion of the specificity requirement against general searches and notes 171-189 and accompanying text for a discussion of the probability element of probable cause.
fourth amendment constraints apply.

While the fourth amendment typically does not protect matters knowingly exposed to the public, information compulsorily gained by the government from an individual in return for licenses and benefits is deserving of protection. Similarly, in order to function in today’s society, an individual must rely upon the goods and services of third parties who, in the ordinary course of business, require information concerning the individual’s private affairs. Society does retain some expectation of privacy in this material despite the fact that it is “voluntarily” relinquished to third persons.

Nevertheless, the United States Supreme Court has been unwilling to recognize a “reasonable” expectation of privacy in third-party records such as bank records concerning an individual’s financial transactions. However, the Court has yet to rule on the applicability of the fourth amendment as a restraint on computer data bank searches. Notwithstanding the United States Supreme Court’s position, contrary state supreme court decisions granting greater deference to privacy expectations, statutory provisions purporting to extend protections—yet failing to do so—and societal expressions of fear for computer matches, all suggest that data bank subjects truly deserve recognition of their reasonable expectations of privacy under the fourth amendment.

Searches within an individual’s zone of privacy are prohibited except by a warrant based on probable cause particularizing the items or information sought. To substantiate probable cause, the official seeking authority to search must demonstrate that the search subject more probably than not has violated a law. Bare suspicion alone is not sufficient to justify a search. A computer search, initiated without any suspicion of wrongdoing by individual data bank subjects, is a massive dragnet combing through millions of data files with an eye toward generating “suspects.” Therefore, general computer data bank searches by the IRS—void of both probable cause and particularity—derogate the requirements of the fourth amendment.

In the words of Justice Mosk of the California Supreme Court: “Cases are legion that condemn violent searches and invasions of an individual’s right to the privacy of his dwelling. . . . Development of . . . electronic computers . . . have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently, judicial interpretations of the reach of the constitutional protections of individual privacy must keep pace with the perils created by these
new devices." So too, federal courts must keep pace with the perils created by IRS computer data bank searches.

Robert Messick
