Should Disclosure of Information Always Destroy Privacy of Information?

Keywords
anonymity, anonymous, anonymously, association, bank, confidential, confidentiality, constitutional, content, disclose, disclosure, e-mail, First Amendment, Fourth Amendment, fiduciary, freedom, garbage, government, identification, information, Internet, intimate, law, letter, letters, library, Miller, personal, privacy, private, professional, right, rights, risk, screen name, search query, Smith v. Maryland, speech, telephone, third-party, trustworthy, United States, U.S., USA, user, users, White

Table of Contents

Introduction

The U.S. Supreme Court, in *U.S. v. Miller* (1974) and *Smith v. Maryland* (1979) held that disclosure of confidential information destroyed the confidentiality of (or destroyed the reasonable expectation of privacy in) that information. This essay reviews those two cases, explains the historical origin of this rule of law, and criticizes the holding.

This topic is relevant to many issues in privacy law, such as the privacy of allegedly anonymous screen names or user identification on the Internet, the privacy of search engine queries on the Internet, the privacy of library records, and privacy of some information sought by government surveillance. These issues are discussed later in this essay, with the exception of surveillance, which is discussed in my separate essay at http://www.rbs2.com/NSL.pdf .

The present essay considers *only* federal law in the USA. State statutes, or state common law, *may* give people privacy rights not found in federal law.

I have decided not to include in this essay the cases[1] involving disclosure of allegedly confidential information from an accountant to the Internal Revenue Service. Federal statutes and IRS regulations *require* disclosure of information about income and deductions on tax returns, which complicates any discussion of privacy. Furthermore, if the client attempted to use the accountant's services to perpetrate a fraud on the IRS, then not even the stronger attorney-client privilege would protect the confidentiality of such services.[2]

This essay presents general information about an interesting topic in law, but is *not* legal advice for your specific problem. See my disclaimer at http://www.rbs2.com/disclaim.htm .

I list the cases in chronological order in this essay, so the reader can easily follow the historical development of a national phenomenon. If I were writing a legal brief, then I would use the conventional citation order given in the *Bluebook.*

---

[1] See, e.g., *Couch v. U.S.,* 409 U.S. 322 (1973); *Fisher v. U.S.,* 425 U.S. 391 (1976).

[2] For cases on the crime-fraud exception to attorney-client privilege, see, e.g., *U.S. v. Zolin,* 491 U.S. 554 (1989); *In re BankAmerica Corp. Securities Litigation,* 270 F.3d 639 (8thCir. 2001).

Miller v. U.S.

Miller was convicted of operating an unlicensed still for production of whisky and failure to pay taxes on income from the sale of the whisky. During the investigation of Miller, the government used a defective subpoena to obtain copies of Miller's checks, deposit slips, and monthly statements from two banks where Miller had accounts. Neither the government nor the bank informed Miller of the subpoena. The U.S. Court of Appeals reversed Miller's conviction and ordered "a new trial, free from the taint of evidence improperly required."[3]

> The Supreme Court determined almost 90 years ago that 'a compulsory production of a man's private papers to establish a criminal charge against him . . . is within the scope of the Fourth Amendment . . ..' *Boyd v. United States,* 1886, 116 U.S. 616, 622, 6 S.Ct. 524, 528, 29 L.Ed. 746. The venerable *Boyd* doctrine still retains its vitality; [footnote omitted] the government may not cavalierly circumvent *Boyd's* precious protection by first requiring a third party bank to copy all of its depositors' personal checks and then, with an improper invocation of legal process, calling upon the bank to allow inspection and reproduction of those copies. In upholding the Bank Secrecy Act the divided *California Bankers* Court determined that the government could take the first of those steps without exceeding constitutional limits. The Court, however, did not choose to abandon 90 years of precedent by proclaiming open season on personal bank records. Indeed, in rejecting the Fourth Amendment claims of bank depositor plaintiffs, the *California Bankers* majority, in an opinion by Justice Rehnquist, relied heavily upon the proposition that depositors have adequate legal protection from improper government access to their records:
>
> > We see nothing in the Act which violates the Fourth Amendment rights of any of these plaintiffs. Neither the provisions of Title I (Recordkeeping Requirements) nor the implementing regulations require that any information contained in the records be disclosed to the Government; both the legislative history and the regulations make specific reference to the fact that access to the records is to be controlled by existing legal process.
>
> [*California Bankers Ass'n v. Shultz,*] 416 U.S. at 52, 94 S.Ct. at 1513, 39 L.Ed.2d at 835. [footnote omitted] Surely a purported grand jury subpoena, issued not by the court or by the grand jury, but by the United States Attorney's office, for a date when no grand jury was in session, and which in effect compelled broad disclosure of Miller's financial records to the government, does not constitute sufficient 'legal process' within the meaning of the majority opinion.[4] [FN6]
>
> > FN6. A separate opinion filed by two members of the six Justice majority in the *California Bankers* case provides additional support for this proposition. Justice Powell, for himself and Justice Blackmun, joined the majority opinion, but entered a separate concurring opinion to note his concern over the scope of the reporting provisions of the Act, which confer broad authority on the Secretary of the Treasury to require financial institutions to file reports of domestic monetary transactions. Limiting his approval of these requirements to

---

[3] *U.S. v. Miller,* 500 F.2d at 758.

[4] The subsequent U.S. Supreme Court opinion did *not* consider the defective subpoena, because the Court disposed of the case on grounds of no Fourth Amendment protection. *Miller v. U.S.,* 425 U.S. 435, 440 and n. 2 (1976).

> the boundaries of the current implementing regulations — transactions in currency of more than $10,000, 31 C.F.R. § 103.22 (1973) — Justice Powell warned that significant extension of the government's power to compel disclosure of financial transactions would pose substantial constitutional difficulties:
>
> > Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy. Moreover, the potential for abuse is particularly acute where, as here, the legislative scheme permits access to this information without invocation of the judicial process. In such instances, the important responsibility for balancing societal and individual interests is left to unreviewed executive discretion, rather than the scrutiny of a neutral magistrate. [citation omitted by Court of Appeals]
>
> [*California Bankers Ass'n v. Shultz,*] 416 U.S. at 78[-79], 94 S.Ct. at 1526, 39 L.Ed.2d at 850-851 (Powell, J. concurring). A governmental order to disclose copies of a bank depositor's checks is at least as obnoxious to constitutional principles when exercised, as here, without sanction in statute or regulation as it would be under authority of an extended legislative scheme.

U.S. v. Miller, 500 F.2d 751, 757-758 (5thCir. 1974).

The U.S. Supreme Court, in a 7-to-2 decision, reversed the Court of Appeals.

> On their face, the documents subpoenaed here are not respondent's "private papers." Unlike the claimant in Boyd, respondent can assert neither ownership nor possession. Instead, these are the business records of the banks. As we said in *California Bankers Assn. v. Shultz,* supra, 416 U.S., at 48-49, 94 S.Ct., at 1511, 39 L.Ed.2d, at 833, "(b)anks are . . . not . . . neutrals in transactions involving negotiable instruments, but parties to the instruments with a substantial stake in their continued availability and acceptance." The records of respondent's accounts, like "all of the records (which are required to be kept pursuant to the Bank Secrecy Act,) pertain to transactions to which the bank was itself a party." *Id.,* at 52, 94 S.Ct., at 1513, 39 L.Ed.2d, at 835.

Miller v. U.S., 425 U.S. 435, 440-441 (1976).

This paragraph seems strange to me, because the bank's customer *purchases* checks (typically through the bank itself), so the checks are the property of the customer. Prior to about 1990, it was common practice for the bank to return the paid checks to the customer along with the monthly statement. The bank retained copies of the deposit slips and paid checks, as evidence that the bank had properly accounted for all of its customer's money. Modern practice is for the bank to discard all of the paper and only keep copies in either microfilm or digital format.

Later in its opinion, the Supreme Court rejected the privacy argument:

> Respondent urges that he has a Fourth Amendment interest in the records kept by the banks because they are merely copies of personal records that were made available to the banks for a limited purpose and in which he has a reasonable expectation of privacy. He relies on this Court's statement in *Katz v. United States,* 389 U.S. 347, 353, 88 S.Ct. 507, 512, 19 L.Ed.2d 576, 583 (1967), quoting *Warden v. Hayden,* 387 U.S. 294, 304, 87 S.Ct. 1642, 1648, 18 L.Ed.2d 782, 790 (1967), that "we have . . . departed from the narrow view" that " 'property interests control the right of the Government to search and seize,' " and that a "search and seizure" become unreasonable when the Government's activities violate "the privacy upon which (a person) justifiably relie(s)." But in *Katz* the Court also stressed that "(w)hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection." 389 U.S., at 351, 88 S.Ct., at 511, 19 L.Ed.2d, at 582. We must examine the nature of the particular documents sought to be protected in order to determine whether there

> is a legitimate "expectation of privacy" concerning their contents. Cf. *Couch v. United States,* 409 U.S. 322, 335, 93 S.Ct. 611, 34 L.Ed.2d 548, 558, 619 (1973).
>
> Even if we direct our attention to the original checks and deposit slips, rather than to the microfilm copies actually viewed and obtained by means of the subpoena, we perceive no legitimate "expectation of privacy" in their contents. The checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act, the expressed purpose of which is to require records to be maintained because they "have a high degree of usefulness in criminal tax, and regulatory investigations and proceedings." 12 U.S.C. § 1829b(a)(1). Cf. *Couch v. United States,* supra, at 335, 93 S.Ct., at 619, 34 L.Ed.2d, at 558.
>
> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. *United States v. White,* 401 U.S. 745, 751-752, 91 S.Ct. 1122, 1125-1126, 28 L.Ed.2d 453, 458-459 (1971). This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed. *Id.,* at 752, 91 S.Ct., at 1126, 28 L.Ed.2d, at 459; *Hoffa v. United States,* 385 U.S. at 302, 87 S.Ct., at 413, 17 L.Ed.2d, at 382; *Lopez v. United States,* 373 U.S. 427, 83 S.Ct. 1381, 10 L.Ed.2d 462 (1963). [FN4]
>
> FN4. We do not address here the question of evidentiary privileges, such as that protecting communications between an attorney and his client. Cf. *Fisher v. United States,* 425 U.S., at 403-405, 96 S.Ct., at 1577, 48 L.Ed.2d, at 51-53.

Miller v. U.S., 425 U.S. 435, 442-443 (1976).
In *Miller,* Justices Brennan and Marshall both wrote dissenting opinions.

after *Miller*

In response to *Miller,* the U.S. Congress passed the Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq. (enacted 1978), which lets a customer of a bank challenge an administrative subpoena to the bank for information on a customer's account.[5] However, the basic holding in *Miller* — that disclosure destroys privacy or confidentiality of information — remains valid law in the USA, as shown by the following two cases, *U.S. v. Jacobsen* and *S.E.C. v. O'Brien,* from the year 1984:

---

[5] See legislative history at H.R.Rep. Nr. 1383, 95th Cong.2d Sess. 34, reprinted in 1978 U.S.CODE CONG. & ADMIN.NEWS 9273, 9306.

U.S. v. Jacobsen

The U.S. Supreme Court wrote:

> This standard follows from the analysis applicable when private parties reveal other kinds of private information to the authorities. It is well-settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information: "This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in a third party will not be betrayed." *United States v. Miller,* 425 U.S. 435, 443, 96 S.Ct. 1619, 1624, 48 L.Ed.2d 71 (1976).[FN13] The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated. In such a case the authorities have not relied on what is in effect a private search, and therefore presumptively violate the Fourth Amendment if they act without a warrant. [FN14]
>
> FN13. See *Smith v. Maryland,* 442 U.S. 735, 743-744, 99 S.Ct. 2577, 2581-2582, 61 L.Ed.2d 220 (1979); *United States v. White,* 401 U.S. 745, 749-753, 91 S.Ct. 1122, 1124-1126, 28 L.Ed.2d 453 (1971) (plurality opinion); *Osborn v. United States,* 385 U.S. 323, 326-331, 87 S.Ct. 429, 431-433, 17 L.Ed.2d 394 (1966); *Hoffa v. United States,* 385 U.S. 293, 300-303, 87 S.Ct. 408, 412-414, 17 L.Ed.2d 374 (1966); *Lewis v. United States,* 385 U.S. 206, 87 S.Ct. 424, 17 L.Ed.2d 312 (1966); *Lopez v. United States,* 373 U.S. 427, 437-439, 83 S.Ct. 1381, 1387-1388, 10 L.Ed.2d 462 (1963); *On Lee v. United States,* 343 U.S. 747, 753-754, 72 S.Ct. 967, 971-972, 96 L.Ed. 1270 (1952). See also *United States v. Henry,* 447 U.S. 264, 272, 100 S.Ct. 2183, 2187, 65 L.Ed.2d 115 (1980); *United States v. Caceres,* 440 U.S. 741, 744, 750-751, 99 S.Ct. 1465, 1467, 1470-1471, 59 L.Ed.2d 733 (1979).
>
> FN14. See *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967); *Berger v. New York,* 388 U.S. 41, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967); *Silverman v. United States,* 365 U.S. 505, 81 S.Ct. 679, 5 L.Ed.2d 734 (1961).

U.S. v. Jacobsen, 466 U.S. 109, 117-118 (1984).

S.E.C. v. O'Brien, Inc.

In another case in 1984, the U.S. Supreme Court wrote:

> Finally, respondents cannot invoke the Fourth Amendment in support of the Court of Appeals' decision. It is established that, when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities. *United States v. Miller,* 425 U.S. 435, 443, 96 S.Ct. 1619, 1624, 48 L.Ed.2d 71 (1976). Relying on that principle, the Court has held that a customer of a bank cannot challenge on Fourth Amendment grounds the admission into evidence in a criminal prosecution of financial

> records obtained by the Government from his bank pursuant to allegedly defective subpoenas, despite the fact that he was given no notice of the subpoenas. *Id.,* at 443, and n. 5, 96 S.Ct., at 1624, and n. 5. [footnote omitted] See also *Donaldson v. United States,* 400 U.S. 517, 522, 91 S.Ct. 534, 538, 27 L.Ed.2d 580 (1971) (Internal Revenue summons directed to third party does not trench upon any interests protected by the Fourth Amendment). [footnote omitted] These rulings disable respondents from arguing that notice of subpoenas issued to third parties is necessary to allow a target to prevent an unconstitutional search or seizure of his papers.

S.E.C. v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984).

Smith v. Maryland

Smith robbed a woman. After the robbery, Smith began making "threatening and obscene" telephone calls to the victim. Eleven days after the robbery, police observed a car in the victim's neighborhood that matched the description of the robber's car given by the victim. A check of the license plates on that car revealed the owner to be Smith. The police — without obtaining a warrant — asked the telephone company to install a pen register[6] on Smith's home telephone. The pen register showed that Smith was calling his robbery victim. Smith was convicted and sentenced to six years in prison. At his trial, his appeal in state court,[7] and his subsequent appeal to the U.S. Supreme Court, Smith's lawyer sought to have the evidence from the pen register suppressed, because the police did not have a warrant for its installation on Smith's home telephone.

The rule in *Miller* was extended by the U.S. Supreme Court to telephone company business records in *Smith v. Maryland.* In this case, the Court, in a 5 to 3 decision, said:

> Given a pen register's limited capabilities, therefore, petitioner's argument that its installation and use constituted a "search" necessarily rests upon a claim that he had a "legitimate expectation of privacy" regarding the numbers he dialed on his phone.
>
> This claim must be rejected. First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies "for the purposes of checking billing operations, detecting fraud and preventing violations of law." *United States v. New York Tel. Co.,* 434 U.S., at 174-175, 98 S.Ct., at 373. Electronic equipment is used not only to keep billing records of toll calls, but also "to keep a record of all calls dialed from a telephone which is subject to a special rate structure." *Hodge v. Mountain States Tel. & Tel. Co.,* 555 F.2d 254, 266 (CA9 1977) (concurring opinion). Pen registers are regularly employed "to determine whether a home phone is being used to conduct a business, to check

---

[6] A pen register is a device that records on paper tape the telephone numbers that are called from the telephone. A pen register does *not* record the contents of a telephone call.

[7] *Smith v. Maryland,* 389 A.2d 858 (Md. 1978).

for a defective dial, or to check for overbilling." Note, The Legal Constraints upon the Use of the Pen Register as a Law Enforcement Tool, 60 CORNELL L.REV. 1028, 1029 (1975) (footnotes omitted). Although most people may be oblivious to a pen register's esoteric functions, they presumably have some awareness of one common use: to aid in the identification of persons making annoying or obscene calls. See, e. g., *Von Lusch v. C & P Telephone Co.,* 457 F.Supp. 814, 816 (Md. 1978); Note, 60 CORNELL L.REV., at 1029-1030, n. 11; Claerhout, The Pen Register, 20 DRAKE L.REV. 108, 110-111 (1970). Most phone books tell subscribers, on a page entitled "Consumer Information," that the company "can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls." E. g., Baltimore Telephone Directory 21 (1978); District of Columbia Telephone Directory 13 (1978). 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.

Petitioner argues, however, that, whatever the expectations of telephone users in general, he demonstrated an expectation of privacy by his own conduct here, since he "us[ed] the telephone in his house to the exclusion of all others." Brief for Petitioner 6 (emphasis added). But the site of the call is immaterial for purposes of analysis in this case. Although petitioner's conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think that it would.

Second, even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not "one that society is prepared to recognize as 'reasonable.' " *Katz v. United States,* 389 U.S., at 361, 88 S.Ct., at 516. This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. E. g., *United States v. Miller,* 425 U.S., at 442-444, 96 S.Ct., at 1623-1624; *Couch v. United States,* 409 U.S., at 335-336, 93 S.Ct., at 619-620; *United States v. White,* 401 U.S., at 752, 91 S.Ct., at 1126 (plurality opinion); *Hoffa v. United States,* 385 U.S. 293, 302, 87 S.Ct. 408, 413, 17 L.Ed.2d 374 (1966); *Lopez v. United States,* 373 U.S. 427, 83 S.Ct. 1381, 10 L.Ed.2d 462 (1963). In *Miller,* for example, the Court held that a bank depositor has no "legitimate 'expectation of privacy' " in financial information "voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business." 425 U.S., at 442, 96 S.Ct., at 1624. The Court explained:

> "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."

Id., at 443, 96 S.Ct., at 1624.

Because the depositor "assumed the risk" of disclosure, the Court held that it would be unreasonable for him to expect his financial records to remain private.

This analysis dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of

business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. Tr. of Oral Arg. 3-5, 11-12, 32. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.

Petitioner argues, however, that automatic switching equipment differs from a live operator in one pertinent respect. An operator, in theory at least, is capable of remembering every number that is conveyed to him by callers. Electronic equipment, by contrast can "remember" only those numbers it is programmed to record, and telephone companies, in view of their present billing practices, usually do not record local calls. Since petitioner, in calling McDonough, was making a local call, his expectation of privacy as to her number, on this theory, would be "legitimate."

This argument does not withstand scrutiny. The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record. In these circumstances, petitioner assumed the risk that the information would be divulged to police. Under petitioner's theory, Fourth Amendment protection would exist, or not, depending on how the telephone company chose to define local-dialing zones, and depending on how it chose to bill its customers for local calls. Calls placed across town, or dialed directly, would be protected; calls placed across the river, or dialed with operator assistance, might not be. We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation.

We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not "legitimate." The installation and use of a pen register, consequently, was not a "search," and no warrant was required. The judgment of the Maryland Court of Appeals is affirmed.

Smith v. Maryland, 442 U.S. 735, 742-746 (1979).

In *Smith,* Justices Stewart and Marshall both wrote dissenting opinions, joined by Justice Brennan.

privacy of garbage

The U.S. Supreme Court has ruled that there is no privacy right for material in opaque garbage bags that are placed on the curb outside a house for collection. *California v. Greenwood,* 486 U.S. 35 (1988). Similarly, the Court has ruled that there is no privacy right for material discarded in a trash bin in a public place. *California v. Rooney,* 483 U.S. 307 (1987). As part of its justification in these two cases, the Court quoted *Smith v. Maryland:* "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Greenwood,* at 41; *Rooney* at 323.

If garbage were not handed to a third party for collection, then there would apparently be a privacy interest in the contents of opaque trash bags. In 1982, the U.S. Supreme Court wrote:

> One point on which the Court was in virtually unanimous agreement in *Robbins* was that a constitutional distinction between "worthy" and "unworthy" containers would be improper. [*Robbins,* 453 U.S. 420, 426-427 (1981)] Even though such a distinction perhaps could evolve in a series of cases in which paper bags, locked trunks, lunch buckets, and orange crates were placed on one side of the line or the other, the central purpose of the Fourth Amendment forecloses such a distinction. For just as the most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion, so also may a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case. [three footnotes omitted]

United States v. Ross, 456 U.S. 798, 822 (1982).

Therefore, an opaque plastic garbage bag is as good as a briefcase in keeping the contents private.

One of the first essays that I wrote on law criticized the U.S. Supreme Court's holding in *Greenwood.*[8]

Historical Origin of the Rule

Before I criticize *U.S. v. Miller* and *Smith v. Maryland,* let's look at the historical origin of the rule that disclosing information destroys the privacy of the information. The rule comes from a series of cases, in the years 1952 to 1971, involving a criminal's confession or admission to a person, who — unknown to the criminal — was either a government informant or a government agent.

---

[8] Ronald B. Standler, *Privacy Law in the USA,* http://www.rbs2.com/privacy.htm (July 1997).

On Lee

In *On Lee,* the defendant was convicted of selling opium on the basis of defendant's conversations with Chin Poy[9] — who unknown to defendant — was a government informer and wearing a microphone and radio transmitter. During the conversations, a government agent, Lee, stood outside the building and listened via radio.

> [Defendant] was talking confidentially and indiscreetly with one he trusted, and he was overheard. This was due to aid from a transmitter and receiver, to be sure, but with the same effect on his privacy as if agent Lee had been eavesdropping outside an open window. The use of bifocals, field glasses or the telescope to magnify the object of a witness' vision is not a forbidden search or seizure, even if they focus without his knowledge or consent upon what one supposes to be private indiscretions. It would be a dubious service to the genuine liberties protected by the Fourth Amendment to make them bedfellows with spurious liberties improvised by farfetched analogies which would liken eavesdropping on a conversation, with the connivance of one of the parties, to an unreasonable search or seizure. We find no violation of the Fourth Amendment here.

On Lee v. U.S., 343 U.S. 747, 753-754 (1952).

> Society can ill afford to throw away the evidence produced by the falling out, jealousies, and quarrels of those who live by outwitting the law. Certainly no one would foreclose the turning of state's evidence by denizens of the underworld. No good reason of public policy occurs to us why the Government should be deprived of the benefit of On Lee's admissions because he made them to a confidante of shady character.

On Lee, 343 U.S. at 756.

The majority opinion concluded:

> The use of informers, accessories, accomplices, false friends, or any of the other betrayals which are 'dirty business' may raise serious questions of credibility. To the extent that they do, a defendant is entitled to broad latitude to probe credibility by cross-examination and to have the issues submitted to the jury with careful instructions. But to the extent that the argument for exclusion departs from such orthodox evidentiary canons as relevancy and credibility, it rests solely on the proposition that the Government shall be arbitrarily penalized for the low morals of its informers. However unwilling we as individuals may be to approve conduct such as that of Chin Poy, such disapproval must not be thought to justify a social policy of the magnitude necessary to arbitrarily exclude otherwise relevant evidence. We think the administration of justice is better served if stratagems such as we have here are

---

[9] Chin Poy, "an old acquaintance and former employee [of defendant], sauntered in [to defendant's place of business] and, while customers came and went, engaged the accused in conversation in the course of which [defendant] made incriminating statements." *On Lee,* 343 U.S. at 749.

"We can only speculate on the reasons why Chin Poy was not called [to testify at trial]. It seems a not unlikely assumption that the very defects of character and blemishes of record which made On Lee trust him with confidences would make a jury distrust his testimony. Chin Poy was close enough to the underworld to serve as bait, near enough the criminal design so that petitioner would embrace him as a confidante, but too close to it for the Government to vouch for him as a witness. Instead, the Government called agent Lee. We should think a jury probably would find the testimony of agent Lee to have more probative value than the word of Chin Poy." *Ibid.* at 756.

> regarded as raising, not questions of law, but issues of credibility. We cannot say that testimony such as this shall, as a matter of law, be refused all hearing.

On Lee, 343 U.S. at 757-758.

Lopez, Lewis, and *Hoffa*

Lopez invited a known Internal Revenue Agent into Lopez's office. Lopez offered the Agent a $420 bribe. Lopez later claimed the payment was to compensate the Agent for preparing tax returns for Lopez's business. In later meetings, the Agent wore a microphone and radio transmitter and pretended to "pretend to play along with the scheme". Lopez was convicted of attempted bribery. *Lopez v. U.S.,* 373 U.S. 427 (1963).

In *Lewis,* a federal agent misrepresented his identity and arranged to purchase marihuana. After the agent entered the defendant's home and purchased the marihuana, the defendant was found guilty of selling marihuana. *Lewis v. U.S.,* 385 U.S. 206 (1966).

A labor leader, Partin, visited Jimmy Hoffa in Hoffa's hotel room during Hoffa's trial and heard Hoffa admit to bribing jurors. Unknown to Hoffa, Partin was a government informant who reported the conversations to a federal agent. Hoffa was then convicted of jury tampering.

> Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it. Indeed, the Court unanimously rejected that very contention less than four years ago in *Lopez v. United States,* 373 US. 427, 83 S.Ct. 1381, 10 L.Ed.2d 462. In that case the petitioner had been convicted of attempted bribery of an internal revenue agent named Davis. The Court was divided with regard to the admissibility in evidence of a surreptitious electronic recording of an incriminating conversation Lopez had had in his private office with Davis. But there was no dissent from the view that testimony about the conversation by Davis himself was clearly admissible.

Hoffa v. U.S., 385 U.S. 293, 302-303 (1966).

White

In *White,* defendant was convicted of narcotics offenses on the basis of his conversations with a Harvey Jackson,[10] who — unknown to defendant — was a government informant who was wearing a microphone and radio transmitter. Four justices of the U.S. Supreme Court agreed with the plurality opinion:

> Our problem is not what the privacy expectations of particular defendants in particular situations may be or the extent to which they may in fact have relied on the discretion of their companions. Very probably, individual defendants neither know nor suspect that their colleagues have gone or will go to the police or are carrying recorders or transmitters.

---

[10] Jackson was apparently a disreputable person, since the Supreme Court tersely notes "The prosecution was unable to locate and produce Jackson at the trial and the trial court overruled objections to the testimony of the agents who conducted the electronic surveillance."
White, 401 U.S. at 747.

> Otherwise, conversation would cease and our problem with these encounters would be nonexistent or far different from those now before us. Our problem, in terms of the principles announced in *Katz,* is what expectations of privacy are constitutionally 'justifiable' — what expectations the Fourth Amendment will protect in the absence of a warrant. So far, the law permits the frustration of actual expectations of privacy by permitting authorities to use the testimony of those associates who for one reason or another have determined to turn to the police, as well as by authorizing the use of informants in the manner exemplified by *Hoffa* and *Lewis.* If the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations which are later offered in evidence to prove the State's case. See *Lopez v. United States,* 373 U.S. 427, 83 S.Ct. 1381, 10 L.Ed.2d 462 (1963).
>
> Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his. In terms of what his course will be, what he will or will not do or say, we are unpersuaded that he would distinguish between probably informers on the one hand and probable informers with transmitters on the other. Given the possibility or probability that one of his colleagues is cooperating with the police, it is only speculation to assert that the defendant's utterances would be substantially different or his sense of security any less if he also thought it possible that the suspected colleague is wired for sound. At least there is no persuasive evidence that the difference in this respect between the electronically equipped and the unequipped agent is substantial enough to require discrete constitutional recognition, particularly under the Fourth Amendment which is ruled by fluid concepts of 'reasonableness.'
>
> Nor should we be too ready to erect constitutional barriers to relevant and probative evidence which is also accurate and reliable. An electronic recording will many times produce a more reliable rendition of what a defendant has said than will the unaided memory of a police agent. **....**

U.S. v. White, 401 U.S. 745, 751-753 (1971) (plurality opinion).

Justice Black concurred with the judgment, Justice Brennan concurred with the result, and three justices dissented.

Why the Rule in *Miller* and *Smith* Is Wrong

facts distinguishable

In *On Lee, Lopez, Lewis, Hoffa,* and *White,* the so-called "confidential information" was a confession or admission to a crime, and the third party who received the information was a government informant (or government agent in *Lopez* and *Lewis*). These facts are very different from the *Miller* and *Smith* cases, and also different from the National Security Letter cases.

In *Miller,* the confidential information was given to a bank, a trustworthy business. In *Smith,* the confidential information was "given" to automatic equipment at the telephone company, a highly regulated monopoly and trustworthy business. In the National Security Letter cases, the confidential information was given to an Internet Service Provider (i.e., trustworthy business) and librarians (i.e., professionals). Furthermore, in the National Security Letter cases, the information demanded by the government *may not* be a response to alleged criminal activity, but only suspicion of communicating with terrorists. Instead of treating banks and telephone companies as

trustworthy businesses who use confidential information only as intended by their customers, the U.S. Supreme Court in *Miller* and *Smith* treated banks and telephone companies the same as government informants who collect information on crimes by concealment, fraud, misrepresentation, disloyalty, etc.

Furthermore, the pen register in *Smith v. Maryland* is also distinguishable from the other cases in that records of a pen register are *not* routine business information kept by the telephone company — instead a pen register is a special service that was installed on one specific telephone line, only after the police requested the information. In other words, the pen register information was *created* at the request of the police, and is *not* information that the telephone company normally saves.

private vs. public

The words *private* and *public* are antonyms. The U.S. Supreme Court has held that conduct exposed to the public is *not* protected by privacy:

> What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. [citations omitted]

Katz v. U.S., 389 U.S. 347, 351 (1967).

In a case involving warrantless surveillance by police in an airplane of marijuana plants growing inside the curtilage of a house, the U.S. Supreme Court concluded:

> That the area is within the curtilage does not itself bar all police observation. The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible. E.g., *United States v. Knotts,* 460 U.S. 276, 282, 103 S.Ct. 1081, 1085-1086, 75 L.Ed.2d 55 (1983). "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz,* supra, 389 U.S., at 351, 88 S.Ct., at 511.
>
> **....** Any member of the public flying in this airspace who glanced down could have seen everything that these officers observed. On this record, we readily conclude that respondent's expectation that his garden was protected from such observation is unreasonable and is not an expectation that society is prepared to honor. [footnote omitted]

California v. Ciraolo, 476 U.S. 207, 213-214 (1986).

The holdings in *Katz* and *Ciraolo* are obviously correct — when a fact is easily observed by *any* member of the public, the privacy rights in that fact are lost. But, in *Miller* and *Smith v. Maryland,* the Court erred in drawing the line between private and public at disclosure to *one* person. As discussed below, privacy rights are not lost when disclosure is to an attorney, physician, licensed psychologist, or any other professional person with a fiduciary duty.

Furthermore, the existence of the tort of "publicity given to private life"[11] shows that society is prepared to award damages for widespread disclosure of private facts. The Restatement says:

> Every individual has some phases of his life and his activities and some facts about himself that he does not expose to the public eye, but keeps entirely to himself or at most reveals only to his family or to close personal friends. Sexual relations, for example, are normally entirely private matters, as are family quarrels, many unpleasant or disgraceful or humiliating illnesses, most intimate personal letters, most details of a man's life in his home, and some of his past history that he would rather forget. When these intimate details of his life are spread before the public gaze in a manner highly offensive to the ordinary reasonable man, there is an actionable invasion of his privacy, unless the matter is one of legitimate public interest.

RESTATEMENT SECOND OF TORTS § 652D, comment *b*, p. 386 (1977).

obvious exceptions to rule

The concept that information loses its confidential nature just because it is disclosed to someone is ridiculous. The common law recognizes several confidential relationships (e.g., attorney-client, psychotherapist-patient, clergy-parishioner, physician-patient) in which information from the client, patient, or parishioner must remain confidential.[12] The existence of these four well known exceptions to the rule tells us that the rule can not possibly be absolute.

People and businesses disclose trade secrets, under the contractual protection of a nondisclosure agreement, with the legitimate expectation that the information will *not* be transferred to other parties. And there are many common situations in which a person discloses confidential information as part of a routine transaction (e.g., credit card numbers when making a purchase, titles of books searched or checked-out of a library, diagnosis or names of drugs transmitted to a health insurance company with a request for payment, etc.) with a reasonable expectation that the information will *only* be used for the intended purpose.

why some information should be private

I find it remarkable that few of the dissenting opinions in U.S. Supreme Court cases mentioned *why* bank records and a list of telephone numbers dialled *should* be confidential information. I agree with Justice Douglas about bank records:

---

[11] RESTATEMENT SECOND OF TORTS § 652D (1977).

[12] Federal Rule of Evidence 501 (1974). Attorney-client privilege is discussed below, at page 19.

> It is, I submit, sheer nonsense to agree with the Secretary that all bank records of every citizen "have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings."[13] That is unadulterated nonsense unless we are to assume that every citizen is a crook, an assumption I cannot make.
>
> Since the banking transactions of an individual give a fairly accurate account of his religion, ideology, opinions, and interests, a regulation impounding them and making them automatically available to all federal investigative agencies is a sledge-hammer approach to a problem that only a delicate scalpel can manage. Where fundamental personal rights are involved — as is true when as here the Government gets large access to one's beliefs, ideas, politics, religion, cultural concerns, and the like — the Act should be 'narrowly drawn' (*Cantwell v. Connecticut,* 310 U.S. 296, 307, 60 S.Ct. 900, 905, 84 L.Ed. 1213) to meet the precise evil. [footnote omitted] Bank accounts at times harbor criminal plans. But we only rush with the crowd when we vent on our banks and their customers the devastating and leveling requirements of the present Act. 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 Ass'n v. Shultz, 416 U.S. 21, 85-86 (1974) (Douglas, J., dissenting).

And I agree with the terse paragraph written by Justice Stewart about telephone numbers:

> The numbers dialed from a private telephone — although certainly more prosaic than the conversation itself — are not without "content." Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life.

Smith v. Maryland, 442 U.S. at 748 (Stewart, J., dissenting).

bank/telephone are necessities

Bank and telephone accounts are "necessities" of modern life, *not* some optional activity that a person makes at his own risk. In an early case about privacy of bank statements, the California Supreme Court wrote:

> For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography.

Burrows v. Superior Court, 529 P.2d 590, 596 (Cal. 1974).

Quoted by Justice Brennan in his dissenting opinion in *Miller v. U.S.,* 425 U.S. 435, 451 (1976).

---

[13] Quoting majority opinion, 416 U.S. at 26, which quotes 12 U.S.C. § 1951 (enacted 1970).

Justice Marshall wrote in his dissent in *Smith* that a telephone account is "a personal or professional necessity". Justice Marshall then explained that people had no realistic choice about having a telephone account:

> Implicit in the concept of assumption of risk is some notion of choice. At least in the third-party consensual surveillance cases, which first incorporated risk analysis into Fourth Amendment doctrine, the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications. See, e. g., *Lopez v. United States,* 373 U.S. 427, 439, 83 S.Ct. 1381, 1388, 10 L.Ed.2d 462 (1963); *Hoffa v. United States,* 385 U.S. 293, 302-303, 87 S.Ct. 408, 413-414, 17 L.Ed.2d 374 (1966); *United States v. White,* supra, 401 U.S., at 751-752, 91 S.Ct., at 1125-1126 (plurality opinion). By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. Cf. *Lopez v. United States,* supra, 373 U.S., at 465-466, 83 S.Ct., at 1401-1402 (BRENNAN, J., dissenting). It is idle to speak of "assuming" risks in contexts where, as a practical matter, individuals have no realistic alternative.

Smith v. Maryland, 442 U.S. 735, 749-750 (Marshall, J., dissenting).

Brennan's dissents

Justice Brennan — my favorite Justice on the U.S. Supreme Court — wrote some strange dissents in the cases about disclosure to someone destroying the privacy of the information.
In *Lopez v. U.S.,* 373 U.S. at 446-471, Justice Brennan wrote a long opinion that mentioned the social cost of remaining silent in order to protect confidential information.
In *U.S. v. Miller,* 425 U.S. at 447-456, Justice Brennan mostly quoted a decision of the California Supreme Court in a different case.

I think the rule in *On Lee, Hoffa,* and *White* is correct: disclosure of crimes to a *non*professional person should destroy the privacy of the information. However, I am troubled by the misrepresentations of government agents in *Lopez* and *Lewis* — I do *not* like the legal rule that government agents can misinform people with the intent of gathering evidence of a crime or obtaining a confession to a crime. We should expect better behavior from government employees.

In my view, the problem with tape recording a face-to-face conversation (or a telephone conversation) is that the recording can be played to an audience of people to whom the speaker would *not* consent to speak. However, someone who was a party to a face-to-face conversation (or a telephone conversation) can testify in court from memory about the conversation.
A recording will be more accurate — more reliable, more trustworthy — than a person's memory. For that reason, I am not bothered by informants who wear a microphone and radio transmitter, although the practice offended Justice Brennan.

Attorney-Client Privilege

The subject of attorney-client privilege is relevant to this essay, not only because it is an obvious exception to the Supreme Court's rule that disclosure defeats confidentiality or privacy, but also because there are many reported cases that discuss how the presence of a third party in an attorney-client meeting may (or may not) defeat confidentiality. The attorney-client privilege is both a common law rule of evidence[14] and a professional obligation of every attorney.[15] The U.S. Supreme Court has explained the purpose of the attorney-client privilege:

> The attorney-client privilege is the oldest of the privileges for confidential communications known to the common law. 8 J. Wigmore, EVIDENCE § 2290 (McNaughton rev. 1961). Its purpose is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice. The privilege recognizes that sound legal advice or advocacy serves public ends and that such advice or advocacy depends upon the lawyer's being fully informed by the client.

Upjohn Co. v. U.S., 449 U.S. 383, 389 (1981).

Disclosure of confidential information to a nonattorney third party in a law office does *not* destroy the confidentiality of the information, when the third party is either:

1. assisting the attorney (e.g., secretary, paralegal, nontestifying consultant, or other agent(s) of the attorney),
2. assisting the client (e.g., agent(s) of the client),

or

3. facilitating the communication (e.g., translator, parent(s) of a child-client), regardless of whether hired by the attorney or by the client.[16]

Note that the third party must serve some "useful purpose"and the interests of the third party must not be adverse to the client, in order to preserve the attorney-client privilege.[17]

From this rule about attorney-client privilege, we see that confidential disclosure to the attorney, agents of the attorney, agents of the client, and those who facilitate the attorney-client communication are all protected by attorney-client privilege. It is the same with physician-patient privilege, where disclosures to a nurse can be protected by the physician-patient privilege. These

---

[14] Federal Rule of Evidence 501 (1974). The rule prohibits the introduction of evidence (e.g., testimony or documents) in trials, unless the client consents to the disclosure of the confidential information.

[15] American Bar Association Model Rule 1.6 (enacted 1983); RESTATEMENT OF THE LAW THIRD THE LAW GOVERNING LAWYERS, §§ 59-93 (2000).

[16] RESTATEMENT OF THE LAW THIRD THE LAW GOVERNING LAWYERS, §§ 60, 70 (2000); *Proposed Fed. Rule Evidence § 503(b),* 56 F.R.D. 183, 236 (1972).

[17] RESTATEMENT OF THE LAW THIRD THE LAW GOVERNING LAWYERS, § 70, comment *f* (2000).

well-accepted rules of law show that the rule in *Miller* about disclosure to one person destroying privacy can not be correct.

While many judicial opinions make the attorney-client relationship appear special, the attorney-client relationship is one example of fiduciary relationships, in which the fiduciary has the duty to use the client's information *only* for the benefit of the client.[18]

Anonymous Speech is Protected

Some of the cases involving government requests for information about subscribers are used to defeat anonymity.[19] The U.S. Supreme Court has repeatedly held that authors have the First Amendment right to anonymous or pseudonymous speech:

- *Talley v. California*, 362 U.S. 60, 64 (1960) ("Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all.");

- *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 357 (1995) ("Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority." At 342: "... the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.");

- *Victoria Buckley v. American Constitutional Law Foundation, Inc.,* 525 U.S. 182, 199 (1999) (The Court invalidated a Colorado state statute that required people circulating petitions to wear identification badges with their name: "The injury to speech is heightened for the petition circulator because the badge requirement compels personal name identification at the precise moment when the circulator's interest in anonymity is greatest. See [*American Constitutional Law Foundation, Inc. v. Meyer,*] 120 F.3d at 1102.");

- *Watchtower Bible and Tract Society of New York, Inc. v. Village of Stratton,* 536 U.S. 150, 166 (2002) ("We may, therefore, consider the impact of this ordinance on the free speech rights of individuals who are deterred from speaking because the registration provision would require them to forgo their right to speak anonymously.").

---

[18] RESTATEMENT OF THE LAW THIRD THE LAW GOVERNING LAWYERS, § 60(2) (2000). All agents have a duty to use the principal's information only for the benefit of the principal. RESTATEMENT SECOND OF AGENCY, §§ 387, 395.

[19] See the discussion of anonymous screen names on the Internet, below, beginning at page 28.

There is a long history of anonymous or pseudonymous speech in the USA, which the U.S. Supreme Court traced back to the pseudonym, Publius, in the FEDERALIST PAPERS. *McIntyre v. Ohio Elections Commission*, 514 U.S. at 342, n. 6; *Talley v. California*, 362 U.S. at 65.

legal right to access Internet anonymously

The right to anonymously access websites on the Internet has been repeatedly upheld by courts. First, consider the cases affirmed by a U.S. Court of Appeals or the U.S. Supreme Court:

- *American Civil Liberties Union v. Reno,* 929 F.Supp. 824, 849 (E.D.Pa. 1996) (Finding of Fact Nr. 121: "Anonymity is important to Internet users who seek to access sensitive information, such as users of the Critical Path AIDS Project's Web site, the users, particularly gay youth, of Queer Resources Directory, and users of Stop Prisoner Rape (SPR). Many members of SPR's mailing list have asked to remain anonymous due to the stigma of prisoner rape."), *aff'd,* 521 U.S. 844 (1997);

- *American Booksellers Foundation v. Dean,* 202 F.Supp.2d 300, 310 (D.Vt. 2002) (Finding of Fact Nr. 30: "Credit card verification technology likely would significantly decrease the number and frequency of visitors to sexualhealth.com because disclosure of credit card information removes visitors' anonymity, and most visitors would not use the site unless they can do so anonymously." At 318: "... there is evidence that imposing these age-verification requirements on Web publishers such as Sexual Health Network-for which the anonymity of the Internet is uniquely suited-would turn most users away. Thus, [the challenged statute] effectively drives protected and valuable speech for adults out of the 'marketplace of ideas.' "), *aff'd in part,* 342 F.3d 96, 99 (2dCir. 2003) ("Although technology exists that allows publishers to restrict website access by requiring credit card verification or registration with a commercial age-verification service, a significant number of adult web-users are unwilling or unable to use such verification systems. Such systems are not only an additional hassle, they also require that website visitors forgo the anonymity otherwise available on the internet.");

- *PSINET, Inc. v. Chapman,* 167 F.Supp.2d 878, 889 (W.D.Va. 2001) ("The stigma often associated with these Web sites may deter some individuals from accessing the sites if admission is conditioned on the receipt of personal information. That is, many adults do not want to create a record of their visits to sexually explicit Web sites."), *aff'd,* 362 F.3d 227, 236 (4thCir. 2004) ("The District Court explained that the stigma associated with the content of these Internet sites may deter adults from visiting them if they cannot do so without the assurance of anonymity.").

There are also several reported cases from U.S. District Courts that were not appealed.

- *American Civil Liberties Union of Georgia v. Miller,* 977 F.Supp. 1228 (N.D.Ga. 23 June 1997) (At 1233: "On its face, the act prohibits such protected speech as the use of false identification to avoid social ostracism, to prevent discrimination and harassment, and to protect privacy, as well as the use of trade names or logos in non-commercial educational speech, news, and commentary — a prohibition with well-recognized first amendment problems. [footnote omitted] Therefore, even if the statute could constitutionally be used to

prosecute persons who intentionally 'falsely identify' themselves in order to deceive or defraud the public, or to persons whose commercial use of trade names and logos creates a substantial likelihood of confusion or the dilution of a famous mark, the statute is nevertheless overbroad because it operates unconstitutionally for a substantial category of the speakers it covers. [citation omitted]" At 1234: "... the act's vagueness is particularly harmful because it chills protected expression. Plaintiffs' affidavits indicate that they have already altered what they believe to be innocent and legitimate behavior because of their inability to discern what exactly the act proscribes. Without court intervention, this self-censorship will continue until the act is amended, revoked, or definitively interpreted by the state supreme court.");

- *Columbia Ins. Co. v. seescandy.com,* 185 F.R.D. 573, 578 (N.D.Cal. 8 Mar 1999) (Cybersquatters registered Internet domain names that infringed on trademarks of See's Candy Shops, Inc. Trademark owner requested identities of the cybersquatters. "... this need must be balanced against the legitimate and valuable right to participate in online forums anonymously or pseudonymously. People are permitted to interact pseudonymously and anonymously with each other so long as those acts are not in violation of the law. This ability to speak one's mind without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate. Furthermore, it permits persons to obtain information relevant to a sensitive or intimate condition without fear of embarrassment. People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity.");

- *John Doe v. 2TheMart.com Inc.,* 140 F.Supp.2d 1088 (W.D.Wash. 26 April 2001) (Court quashed subpoena to Internet Service Provider for identity of 23 persons who posted anonymously on Internet bulletin boards operated by the ISP. At 1093: "The free exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously. If Internet users could be stripped of that anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment rights. Therefore, discovery requests seeking to identify anonymous Internet users must be subjected to careful scrutiny by the courts.").

Freedom of Association

Obtaining bank records of an political organization would allow the government to learn who was contributing money to that organization. In other contexts, the U.S. Supreme Court has held that the government may *not* force an organization to produce a list of its members (unless the government has a compelling need for the list), essentially because members have the right to be anonymous.

> It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as the forms of governmental action in the cases above were thought likely to produce upon the particular constitutional rights there involved. This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. When referring to the varied forms of governmental action which might interfere with freedom of assembly, it said in *American Communications Ass'n v. Douds,* supra, 339 U.S. at page 402, 70 S.Ct. at page 686: "A requirement that adherents of particular religious faiths or political parties wear

> identifying arm-bands, for example, is obviously of this nature." Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs. Cf. *United States v. Rumely,* supra, 345 U.S. at pages 56-58, 73 S.Ct. at pages 550-551 ([Douglas, J.,] concurring opinion).
>
> We think that the production order, in the respects here drawn in question, must be regarded as entailing the likelihood of a substantial restraint upon the exercise by petitioner's members of their right to freedom of association. Petitioner [NAACP] has made an uncontroverted showing that on past occasions revelation of the identity of its rank-and-file members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility. Under these circumstances, we think it apparent that compelled disclosure of petitioner's Alabama membership is likely to affect adversely the ability of petitioner and its members to pursue their collective effort to foster beliefs which they admittedly have the right to advocate, in that it may induce members to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure.

National Association for Advancement of Colored People v. State of Ala. ex rel. Patterson, 357 U.S. 449, 462-463 (1958).

Two years later, the Court said:

> We have recently had occasion to hold in two cases that there are times and circumstances when States may not compel members of groups engaged in the dissemination of ideas to be publicly identified. *Bates v. City of Little Rock,* 361 U.S. 516, 80 S.Ct. 412; *N.A.A.C.P. v. State of Alabama,* 357 U.S. 449, 462, 78 S.Ct. 1163, 1171, 2 L.Ed.2d 1488. The reason for those holdings was that identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance.

Talley v. California, 362 U.S. 60, 65 (1960)

Chief Justice Warren, concurring in the result in *Lopez,* said:

> The right to privacy is the obverse of freedom of speech in another sense. This Court has lately recognized that the First Amendment freedoms may include the right, under certain circumstances, to anonymity. See *N.A.A.C.P. v. Alabama ex rel. Patterson,* 357 U.S. 449, 78 S.Ct. 1163, 2 L.Ed.2d 1488; *Bates v. Little Rock,* 361 U.S. 516, 80 S.Ct. 412, 4 L.Ed.2d 480; *Talley v. California,* 362 U.S. 60, 80 S.Ct. 536, 4 L.Ed.2d 559; *Louisiana ex rel. Gremillion v. N.A.A.C.P.,* 366 U.S. 293, 81 S.Ct. 1333, 6 L.Ed.2d 301; *Gibson v. Florida Legislative Investigation Comm.,* 372 U.S. 539, 83 S.Ct. 889. The passive and the quiet, equally with the active and the aggressive, are entitled to protection when engaged in the precious activity of expressing ideas or beliefs. Electronic surveillance destroys all anonymity and all privacy; it makes government privy to everything that goes on.

Lopez v. U.S., 373 U.S. 427, 470-471 (1963) (Warren, C.J., concurring in result).

Justice Marshall dissented in *California Bankers Association,* a case that laid the foundation for the Court's decision in *U.S. v. Miller*:

> Nor can I accept the majority's analysis of the First Amendment associational claims raised by the American Civil Liberties Union on behalf of its members who seek to preserve the anonymity of their financial support of the organization. The First Amendment gives organizations such as the ACLU the right to maintain in confidence the names of those who belong or contribute to the organization, absent a compelling governmental interest requiring disclosure. See *NAACP v. Alabama,* 357 U.S. 449, 78 S.Ct. 1163, 2 L.Ed.2d 1488 (1958). See also *Lamont v. Postmaster General,* 381 U.S. 301, 85 S.Ct. 1493, 14 L.Ed.2d 398 (1965); *Gibson v. Florida Legislative Investigation Comm'n,* 372 U.S. 539, 83 S.Ct. 889, 9 L.Ed.2d 929 (1963); *Louisiana ex rel. Gremillion v. NAACP,* 366 U.S. 293, 81 S.Ct. 1333, 6 L.Ed.2d 301 (1961); *Shelton v. Tucker,* 364 U.S. 479, 81 S.Ct. 247, 5 L.Ed.2d 231 (1960); *Bates v. City of Little Rock,* 361 U.S. 516, 80 S.Ct. 412, 4 L.Ed.2d 480 (1960); *United States v. Rumely,* 345 U.S. 41, 73 S.Ct. 543, 97 L.Ed. 770 (1953). It is certainly inconsistent with this long line of cases for the Government, absent any showing of need whatsoever, to require the bank with which the ACLU maintains an account to make and keep a microfilm record of all checks received by the ACLU and deposited to its account. The net result of this requirement, obviously, is an easily accessible list of all of the ACLU's contributors. And, given the widespread informal access to bank records by Government agencies, see supra, at 1534-1535, the existence of such a list surely will chill the exercise of First Amendment rights of association on the part of those who wish to have their contributions remain anonymous. The technique of examining bank accounts to investigate political organizations is, unfortunately, not rare. See, e.g., *Pollard v. Roberts,* 283 F.Supp. 248 (E.D.Ark.), *aff'd per curiam,* 393 U.S. 14, 89 S.Ct. 47, 21 L.Ed.2d 14 (1968); *United States Servicemen's Fund v. Eastland,* 159 U.S.App.D.C. 352, 488 F.2d 1252 (1973).
>
> First Amendment freedoms are 'delicate and vulnerable'. They need breathing space to survive. *NAACP v. Button,* 371 U.S. 415, 433, 83 S.Ct. 328, 338, 9 L.Ed.2d 405 (1963). The threat of disclosure entailed in the existence of an easily accessible list of contributors may deter the exercise of First Amendment rights as potently as disclosure itself. Cf. *ibid.* See also *United States Servicemen's Fund v. Eastland,* supra, 159 U.S.App.D.C., at 365-368, 488 F.2d, at 1265-1268. More importantly, however slight may be the inhibition of First Amendment rights caused by the bank's maintenance of the list of contributors, the crucial factor is that the Government has shown no need, compelling or otherwise, for the maintenance of such records. Surely the fact that some may use negotiable instruments for illegal purposes cannot justify the Government's running roughshod over the First Amendment rights of the hundreds of lawful yet controversial organizations like the ACLU. Congress may well have been correct in concluding that law enforcement would be facilitated by the dragnet requirements of this Act. Those who wrote our Constitution, however, recognized more important values.
>
> I respectfully dissent.

California Bankers Ass'n v. Shultz, 416 U.S. 21, 97-99 (1974) (Marshall, J., dissenting).

The U.S. Senate Subcommittee on Internal Security issued a subpoena to a bank for records of the account of the U.S. Serviceman's Fund, a private organization. The U.S. Court of Appeals was willing to quash the subpoena, because the subpoena violated the First Amendment right of

association.[20] Because the subpoena was related to a legitimate legislative function, the U.S. Supreme Court reversed the Court of Appeals and refused to quash the subpoena.[21] The decisions of the Court of Appeals and Supreme Court in this case were issued *before* the Supreme Court's decision in *U.S. v. Miller.* A straightforward reading of the later decision in *Miller* would preclude First Amendment privacy rights in bank records.

In 1980, the U.S. Court of Appeals in Minnesota tersely noted:

> In *United States v. Citizens State Bank,* 612 F.2d 1091 (8th Cir. 1980), this court considered a conflict between the IRS subpoena power and freedom of association under the first amendment. In that case, the IRS ordered a bank to produce its records of a tax protester organization. The records would have revealed the names of members of the organization. The organization submitted declarations of three of its members that revelation of the names would discourage people from joining or contributing to the organization. The district court deemed this information irrelevant, but this court disagreed, stating that the organization had met its "initial burden by making a prima facie case of arguable First Amendment infringement; the burden then shifted to the government to make the appropriate showing of need for the material." *Id.* at 1094. On remand, the district court was to apply the following standard: "(D)isclosure of the identities of members of the group can be compelled only by showing that there is a rational connection between such disclosure and a legitimate government end, and that the governmental interest in disclosure is cogent and compelling," *id.,* quoting *Pollard v. Roberts,* 283 F.Supp. 248, 256-57 (E.D.Ark.), *aff'd,* 393 U.S. 14, 89 S.Ct. 47, 21 L.Ed.2d 14 (1968) (per curiam).

U.S. v. Life Science Church of America, Chapter No. 10075, 636 F.2d 221, 224 (8thCir. 1980). Neither *Citizens State Bank* nor *Life Science Church* mentioned *U.S. v. Miller. Pollard v. Roberts* was decided before *Miller.*

In 1982, the U.S. Supreme Court held the Ohio Campaign Expense Reporting Law *un*constitutional, because it required political parties to report to the state government the names and addresses of donors to the party. Near the beginning of the majority opinion, the U.S. Supreme Court again summarized the case law on compelling disclosure of membership lists.

> The Constitution protects against the compelled disclosure of political associations and beliefs. Such disclosures "can seriously infringe on privacy of association and belief guaranteed by the First Amendment." *Buckley v. Valeo,* supra, 424 U.S., at 64, 96 S.Ct., at 656, citing *Gibson v. Florida Legislative Comm.,* 372 U.S. 539, 83 S.Ct. 889, 9 L.Ed.2d 929 (1963); *NAACP v. Button,* 371 U.S. 415, 83 S.Ct. 328, 9 L.Ed.2d 405 (1963); *Shelton v. Tucker,* 364 U.S. 479, 81 S.Ct. 247, 5 L.Ed.2d 231 (1960); *Bates v. Little Rock,* 361 U.S. 516, 80 S.Ct. 412, 4 L.Ed.2d 480 (1960); *NAACP v. Alabama,* 357 U.S. 449, 78 S.Ct. 1163, 2 L.Ed.2d 1488 (1958). "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." *NAACP v. Alabama,* supra, 357 U.S., at 462, 78 S.Ct., at 1172. The right to privacy in one's political associations and beliefs will yield only to a "subordinating interest of the State [that is] compelling," *NAACP v. Alabama,* supra,

---

[20] *U. S. Servicemen's Fund v. Eastland,* 488 F.2d 1252, 1264-1268 (C.A.D.C. 1973).

[21] *Eastland v. U. S. Servicemen's Fund,* 421 U.S. 491 (1975).

> 357 U.S., at 463, 78 S.Ct., at 1172 (quoting *Sweezy v. New Hampshire,* 354 U.S. 234, 265, 77 S.Ct. 1203, 1219, 1 L.Ed.2d 1311 (1957) (concurring opinion)), and then only if there is a "substantial relation between the information sought and [an] overriding and compelling state interest." *Gibson v. Florida Legislative Comm.,* supra, 372 U.S., at 546, 83 S.Ct., at 893.

Brown v. Socialist Workers '74 Campaign Committee, 459 U.S. 87, 91-92 (1982).

This opinion of the U.S. Supreme Court does *not* mention the *Miller* opinion.

The U.S. Court of Appeals in Colorado heard an appeal involving anti-income-tax organizations efforts to quash a subpoena for the bank records of the organizations.

> On appeal, petitioners argue that the compelled disclosure of membership identities, which would be the inevitable result of unsealing the records and transferring them to the grand jury, would chill the rights of [National Commodity & Barter Association] NCBA and [National Unconstitutional Tax Strike Committee] NUTS members to freedom of association guaranteed by the First Amendment. Affidavits submitted to the district court describe harassment and intimidation of petitioners' known members, and the resulting reluctance of people sympathetic to the goals of NCBA to associate with the group for fear of reprisals. Petitioners assert that they have standing to raise these claims and that they have made out a prima facie case of infringement of associational rights sufficient to entitle them to an evidentiary hearing on the issue. We agree. [footnote omitted]
>
> "It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment ...." *NAACP v. Alabama,* 357 U.S. 449, 460, 78 S.Ct. 1163, 1170, 2 L.Ed.2d 1488 (1958). The Supreme Court declared this right to be protected against both intentional and incidental infringement. "In the domain of these indispensable liberties, whether of speech, press, or association, the decisions of this Court recognize that abridgement of such rights, even though unintended, may inevitably follow from varied forms of governmental action." *Id.* at 461, 78 S.Ct. at 1171. To overcome the deterrent effect on associational rights resulting from compelled disclosure of membership lists, the government must demonstrate a compelling interest, *id.* at 463, 78 S.Ct. at 1172, and a substantial relationship between the material sought and legitimate governmental goals, id. at 464, 78 S.Ct. at 1172. In *Buckley v. Valeo,* 424 U.S. 1, 96 S.Ct. 612, 46 L.Ed.2d 659 (1976), the Court said:
>
> > We long have recognized that significant encroachments on First Amendment rights of the sort that compelled disclosure imposes cannot be justified by a mere showing of some legitimate governmental interest. Since *NAACP v. Alabama,* we have required that the subordinating interests of the State must survive exacting scrutiny. We also have insisted that there be a 'relevant correlation' or 'substantial relation' between the governmental interest and the information required to be disclosed. [See *Pollard v. Roberts,* 283 F.Supp. 248, 257 (ED Ark.) (three-judge court), *aff'd,* 393 U.S. 14, 89 S.Ct. 47, 21 L.Ed.2d 14 (1968) (per curiam).]
>
> *Id.* at 64, 96 S.Ct. at 656 (footnotes omitted).

In re First National Bank, Englewood, Colo., 701 F.2d 115, 116-117 (10thCir. 1983).

This opinion by the Tenth Circuit cites *U.S. v. Miller* for the propositions that (1) "a depositor has no protected Fourth Amendment interests in bank records" and (2) "First Amendment claims may be implicated". On the second issue, the U.S. Supreme Court in *Miller* wrote:

> Respondent does not contend that the subpoenas infringed upon his First Amendment rights. There was no blanket reporting requirement of the sort we addressed in *Buckley v. Valeo,* 424 U.S. 1, at 60-84, 96 S.Ct. 612, at 654, 46 L.Ed.2d 659, at 711 (1976), nor any

> allegation of an improper inquiry into protected associational activities of the sort presented in *Eastland v. United States Servicemen's Fund,* 421 U.S. 491, 95 S.Ct. 1813, 44 L.Ed.2d 324 (1975).
>
> We are not confronted with a situation in which the Government, through "unreviewed executive discretion," has made a wide-ranging inquiry that unnecessarily "touch(es) upon intimate areas of an individual's personal affairs." *California Bankers Assn. v. Shultz,* 416 U.S., at 78-79, 94 S.Ct., at 1526, 39 L.Ed.2d, at 850 (Powell, J., concurring). Here the Government has exercised its powers through narrowly directed subpoenas Duces tecum subject to the legal restraints attendant to such process. **....**

Miller v. U.S., 425 U.S. 435, 444, n. 6 (1976).

It appears that the U.S. Supreme Court in *Miller* gave little attention to First Amendment issues of freedom of association, perhaps because the attorney for Miller did not raise the issue, based on the facts of that case.

The *Seattle Times* newspaper published a series of articles that were critical of the Aquarian Foundation, a religious group led by Keith Rhinehart. Rhinehart sued the newspaper for defamation and alleged that the articles had diminished donations to his Foundation. The newspaper asked for discovery of the identity of the Foundation's donors and amount of their donation during the five previous years. The Washington state courts granted the discovery order, with a protective order preventing the newspaper from either publishing or publicly disseminating this information. The U.S. Supreme Court affirmed the discovery order.[22] In my opinion, the result makes good sense, because the plaintiff had made the amount of donations an issue in litigation, so the defendant was entitled to conduct discovery in order to defend the case on the merits. The protective order prevented any unnecessary exploitation of the information on identities of donors.

Remarkably, there does not seem to be any published opinion by a U.S. Court of Appeals or the U.S. Supreme Court that reconciles (1) the lack of privacy in bank records as a result of *U.S. v. Miller* with (2) the clearly established First Amendment right of association, which should prevent the government from obtaining identities of donors to a political organization through bank records of the organization, unless the government has a compelling need for the identities (e.g., to arrest criminals).

---

[22] *Seattle Times Co. v. Rhinehart,* 467 U.S. 20 (1984).

Lack of Privacy on Internet

The U.S. Supreme Court's rule in *Miller* and *Smith v. Maryland* have resulted in reduction of anonymity and privacy on the Internet.

"anonymous" screen name

There is currently *no* Fourth Amendment legal protection for confidentiality of the name and address associated with an anonymous screen name on the Internet. A federal statute, the Electronic Communications Privacy Act, requires that government agents have a warrant or subpoena to obtain this information from an Internet Service Provider.

Hambrick

In 1998, a detective in New Hampshire obtained a subpoena from a New Hampshire Justice of the Peace[23] that ordered Mindspring, an ISP in Georgia, to provide the "name, address, credit card number, e-mail address, home and work telephone numbers, fax number" of the person associated with a certain screen name and IP address. A U.S. District Court held that there was *no* privacy interest in this subscriber information:

> To have any interest in privacy, there must be some exclusion of others. To have a reasonable expectation of privacy under the Supreme Court's risk-analysis approach to the Fourth Amendment, two conditions must be met: (1) the data must not be knowingly exposed to others, and (2) the Internet service provider's ability to access the data must not constitute a disclosure. In *Katz,* the Supreme Court expressly held that "what a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection." 389 U.S. at 351, 88 S.Ct. 507. Further, the Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland,* 442 U.S. 735, 743-44, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979); see, e.g., *United States v. Miller,* 425 U.S. 435, 442-43, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976); *Couch v. United States,* 409 U.S. 322, 335-36, 93 S.Ct. 611, 34 L.Ed.2d 548 (1973).
>
> The Supreme Court's risk-analysis approach makes the work of the courts difficult when analyzing previously unadjudicated situations in the world of cyberspace. This court's research, assisted by the parties' thorough briefs, has failed to find any factually and legally analogous case law. The defendant cites *United States v. Maxwell,* 45 M.J. 406 (1996), as the only published federal decision that deals with the question of the expectation of privacy in information obtained from an ISP. Although some of the facts of Maxwell appear to be similar to the facts in the present case, Maxwell has little or no precedential value because the United States Court of Appeals for the Armed Forces decided the case. That court reviews

---

[23] The Justice of the Peace who signed the subpoena was employed as a detective in the same police department where the investigating detective who requested the subpoena worked. The U.S. government conceded that the subpoena was defective. However, the government argued that there was no privacy interest in the subpoenaed information, so suppression at trial of the fruits of the invalid subpoena was not necessary. 55 F.Supp. 2d at 506.

the convictions of a court-martial and is entirely separate from the United States Courts of Appeals. Also, despite the fact that the Electronic Communications Privacy Act is evidence that some degree of privacy should be accorded the information at issue in this matter, the ECPA ultimately falls short of serving as a source of extra-constitutional protection for the information and cannot undo the Supreme Court's restrictive risk-analysis approach.

The court finds the defendant's implicit argument that certain information in cyberspace should be private requires careful consideration. Legal scholars and Congress have noted the ubiquity of cyberspace in the lives of all Americans. See generally, e.g., S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555; Michael Adler, Note, Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search, 195 YALE L.J. 1093 (1996); Randolph S. Sergent, Note, A Fourth Amendment Model for Computer Networks and Data Privacy, 81 VA. L. REV. 1181 (1995). The members of our society increasingly live important parts of their lives through the Internet. Cyberspace is a nonphysical "place" and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis. So long as the risk-analysis approach of *Katz* remains valid, however, this court is compelled to apply traditional legal principles to this new and continually evolving technology. In so doing, the court must deny Mr. Hambrick's [defendant's] motion to suppress.

When Scott Hambrick [defendant] surfed the Internet using the screen name "Blowuinva," he was not a completely anonymous actor. It is true that an average member of the public could not easily determine the true identity of "Blowuinva." Nevertheless, when Mr. Hambrick entered into an agreement to obtain Internet access from MindSpring, he knowingly revealed his name, address, credit card number, and telephone number to MindSpring and its employees. Mr. Hambrick also selected the screen name "Blowuinva." When the defendant selected his screen name it became tied to his true identity in all MindSpring records. MindSpring employees had ready access to these records in the normal course of MindSpring's business, for example, in the keeping of its records for billing purposes, and nothing prevented MindSpring from revealing this information to nongovernmental actors.[FN3] Also, there is nothing in the record to suggest that there was a restrictive agreement between the defendant and MindSpring that would limit the right of MindSpring to reveal the defendant's personal information to nongovernmental entities. Where such dissemination of information to nongovernment entities is not prohibited, there can be no reasonable expectation of privacy in that information.

> FN3. It is apparently common for ISPs to provide certain information that Mr. Hambrick alleges to be private to marketing firms and other organizations interested in soliciting business from Internet users.

Although not dispositive to the outcome of this motion, it is important to note that the court's decision does not leave members of cybersociety without privacy protection. Under the ECPA, Internet Service Providers are civilly liable when they reveal subscriber information or the contents of stored communications to the government without first requiring a warrant, court order, or subpoena. See 18 U.S.C. §§ 2703, 2707, 2708 (1994 & Supp. 1996). Here, nothing suggests that MindSpring had any knowledge that the facially valid subpoena submitted to it was in fact an invalid subpoena. Had MindSpring revealed the information at issue in this case to the government without first requiring a subpoena, apparently valid on its face, Mr. Hambrick could have sued MindSpring. This is a powerful deterrent protecting privacy in the online world and should not be taken lightly.

> The defendant's motion to suppress also embraces evidence found in his home pursuant to a residence search warrant. The defendant contends that because the residence search warrant was supported by an affidavit reciting evidence allegedly protected as to the defendant by his right to privacy, the court likewise must suppress the materials seized from his home. As this court has found that the MindSpring materials are not so protected, the predicate for this motion to suppress the materials seized from the defendant's home fails, and therefore the court does not suppress such materials.

U.S. v. Hambrick, 55 F.Supp.2d 504, 507-509 (W.D.Va. 7 July 1999).

Hambrick was convicted and he appealed to the U.S. Court of Appeals, which — in an unpublished decision — affirmed the District Court:

> "What a person knowingly exposes to the public ... is not a subject of Fourth Amendment protection." Id. at 351. Accordingly, the Supreme Court has held that a "person has no legitimate expectation of privacy in information ... voluntarily turn[ed] over to third parties." *Smith v. Maryland,* 442 U.S. 735, 743-44 (1979) (holding that under *Katz,* the defendant likely did not entertain an actual expectation of privacy in the phone numbers he dialed that were revealed through a pen registry, and if he did, that expectation was not one society would consider legitimate). The Supreme Court further stated in *Smith* that when an individual voluntarily conveys information to a third party, the individual "assume[s] the risk" of subsequent disclosure. See *id.* at 744.
>
> In *United States v. Miller,* 425 U.S. 435 (1976), the Supreme Court cited *Hoffa v. United States,* 385 U.S. 293 (1966), for the proposition that " 'no interest legitimately protected by the Fourth Amendment' is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy, into 'the security a man relies upon when he places himself or his property within a constitutionally protected area.' " *Miller,* 425 U.S. at 440 (citing *Hoffa,* 385 U.S. at 301-02). The Supreme Court in *Miller* emphasized that an individual has no Fourth Amendment privacy interest in information released to a third party and later conveyed by that third party to a governmental entity, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." [FN3] *Id.* at 443. The Supreme Court concluded that the bank records subpoenaed in *Miller* were not "private papers" and that the defendant could assert neither ownership nor possession over these papers. See *id* . at 441-42. Instead, the Supreme Court concluded that they were merely business records of the bank. See *id.* at 442.
>
> FN3. The district court, however, noted that there is no evidence in this case to suggest that there was a restrictive agreement between Hambrick and MindSpring that would limit the right of MindSpring to release Hambrick's personal information to nongovernmental entities. The district court further observed that it is common practice for ISPs, such as Mindspring, to reveal the type of information at issue in this case to marketing firms and other organizations interested in soliciting business from Internet users.
>
> **....** When Hambrick entered into a service agreement with MindSpring, he knowingly revealed this information to MindSpring and its employees. The records that the government obtained from MindSpring had been available to MindSpring employees in the normal course of business. Once the government received this information, it was not later utilized to read Hambrick's e-mails or to attain any other content information.

> While under certain circumstances, a person may have an expectation of privacy in content information, a person does not have an interest in the account information given to the ISP in order to establish the e-mail account, which is non-content information. See *Smith,* 442 U.S. at 741 (noting critical distinction between content and non-content information); *Katz,* 389 U.S. at 352 (holding that the user of a public telephone is entitled to "assume that the words he utters into the mouthpiece will not be broadcast to the world"). Disclosure of this non-content information to a third party destroys the privacy expectation that might have existed previously. In this case, the government never utilized the non-content information retrieved from MindSpring to attain additional content information, such as the substance of Hambrick's e-mails. In this case, as in *Miller,* there is no legitimate expectation of privacy in information "voluntarily conveyed to [a third party] and exposed to their employees in the ordinary course of business." *Miller,* 425 U.S. at 442. The information subject to the motion to suppress is merely third-party business records, and therefore, Hambrick's Fourth Amendment claim cannot succeed. [footnote omitted]

U.S. v. Hambrick, 2000 WL 1062039 at *3-*4 (4thCir. 3 Aug 2000) (per curiam).

Kennedy

In July 1999, an anonymous telephone call to RoadRunner, an ISP associated with cable television service, informed RoadRunner of child pornography images on a computer at a specific IP address serviced by RoadRunner. RoadRunner informed the FBI, but RoadRunner insisted on receiving a court order before supplying subscriber information for that computer. The FBI then obtained a court order directing RoadRunner to disclose subscriber information for that one IP address. When the defendant in the criminal prosecution moved for suppression of the evidence supplied by RoadRunner, the U.S. District Court agreed with the defendant that while "the ECPA [18 U.S.C. §§ 2701 et seq.] was violated, suppression of the evidence is not a remedy for such a violation."[24] A U.S. District Court tersely held that Defendant had *no* privacy interest in the subscriber information:

> Defendant's constitutional rights were not violated when Road Runner divulged his subscriber information to the government. Defendant has not demonstrated an objectively reasonable legitimate expectation of privacy in his subscriber information. On the contrary, the evidence is that defendant's computer had its sharing mechanism turned on. The only reasonable inference is that defendant had done so. See *California v. Greenwood,* 486 U.S. 35, 39, 108 S.Ct. 1625, 1628, 100 L.Ed.2d 30 (1988). "[W]hat a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection." *Katz v. United States,* 389 U.S. 347, 351, 88 S.Ct. 507, 511, 19 L.Ed.2d 576 (1967). "[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland,* 442 U.S. 735, 743-44, 99 S.Ct. 2577, 2582, 61 L.Ed.2d 220 (1979). When defendant entered into an agreement with Road Runner for Internet service, he knowing revealed all information connected to the IP address 24.94.200.54. He cannot now claim to have a Fourth Amendment privacy interest in his subscriber information.

U.S. v. Kennedy, 81 F.Supp.2d 1103, 1100 (D.Kan. 3 Jan 2000).

---

[24] *U.S. v. Kennedy,* 81 F.Supp.2d 1103, 1109.

Guest v. Leis

In 1995, a sheriff in Ohio seized two computer bulletin board systems during an investigation of obscenity. Users of the bulletin board system sued the sheriff in class action litigation. In July 2001, a U.S. Court of Appeals tersely noted:

> Plaintiffs argue that defendants violated the Fourth Amendment by accessing bulletin board subscriber information. These records include information such as subscribers' names, addresses, birthdates, and passwords. As we have noted above, a person must have a reasonable expectation of privacy in the matter searched in order to challenge a search under the Fourth Amendment. Individuals generally lose a reasonable expectation of privacy in their information once they reveal it to third parties. See *United States v. Miller,* 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976), limited by statute. A bank customer, for instance, does not have a legitimate expectation of privacy in the information that he or she has conveyed to the bank; by placing the information under control of a third party, the customer assumes the risk that the bank will convey the information to the government. *Id.* Courts have applied this principle to computer searches and seizures to conclude that computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person-the system operator. See *Maxwell,* 45 M.J. at 418; *United States v. Kennedy,* 81 F.Supp.2d 1103, 1110 (D.Kan. 2000) (rejecting a privacy interest in subscriber information communicated to an internet service provider); *United States v. Hambrick,* No. 99-4793, 2000 WL 1062039, at *4 (4th Cir. Aug.3, 2000) (unpublished) (holding that defendant destroyed any privacy interest in his subscriber information when he conveyed it to an internet service provider) (citing *Miller,* 425 U.S. at 442, 96 S.Ct. 1619). We conclude that plaintiffs in these cases lack a Fourth Amendment privacy interest in their subscriber information because they communicated it to the systems operators. In addition, in the O'Brien case,[25] subscriber information would be that of the users, who do not have Fourth Amendment standing.

Guest v. Leis, 255 F.3d 325, 335-336 (6thCir. 2 July 2001).

Warshak

A suspect in a criminal investigation sued the federal government to enjoin the government from seizing contents of e-mails without providing notice and opportunity to be heard to the subscriber of the e-mail account. The District Court granted the preliminary injunction, the government appealed, and the Court of Appeals affirmed nearly all of the injunction.

> *Phibbs* [999 F.2d 1053 (6thCir. 1993)] makes explicit, however, a necessary Fourth Amendment caveat to the rule regarding third-party subpoenas: the party challenging the subpoena has "standing to dispute [its] issuance on Fourth Amendment grounds" if he can "demonstrate that he had a legitimate expectation of privacy attaching to the records obtained." *Id.;* see also *United States v. Miller,* 425 U.S. 435, 444, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976) ("Since no Fourth Amendment interests of the depositor are implicated here, this case is governed by the general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant." (emphasis added)). This language reflects the rule that where the party challenging the disclosure has voluntarily

---

[25] O'Brien is one of the defendants in *Guest v. Leis,* 255 F.3d 325.

> disclosed his records to a third party, he maintains no expectation of privacy in the disclosure vis-a-vis that individual, and assumes the risk of that person disclosing (or being compelled to disclose) the shared information to the authorities. See, e.g., *United States v. Jacobsen,* 466 U.S. 109, 117, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984) ("[W]hen an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information.").
>
> Combining this disclosure to a third party with the government's ability to subpoena the third party alleviates any need for the third-party subpoena to meet the probable cause requirement, if the challenger has not maintained an expectation of privacy with respect to the individual being compelled to make the disclosure. For example, in *Phibbs,* the documents in question were credit card and phone records that were "readily accessible to employees during the normal course of business." 999 F.2d at 1078. A similar rationale was employed by the Supreme Court in *Miller.* 425 U.S. at 442, 96 S.Ct. 1619 ("The checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."). See also *SEC v. Jerry T. O'Brien, Inc.,* 467 U.S. 735, 743, 104 S.Ct. 2720, 81 L.Ed.2d 615 (1984) ("When a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities."). The government's compelled disclosure argument, while relevant, therefore begs the critical question of whether an e-mail user maintains a reasonable expectation of privacy in his e-mails vis-a-vis the party who is subject to compelled disclosure-in this instance, the ISPs. If he does not, as in *Phibbs* or *Miller,* then the government must meet only the reasonableness standard applicable to compelled disclosures to obtain the material. If, on the other hand, the e-mail user does maintain a reasonable expectation of privacy in the content of the e-mails with respect to the ISP, then the Fourth Amendment's probable cause standard controls the e-mail seizure.

Warshak v. U.S., 490 F.3d 455, 469 (6thCir. 18 June 2007).

Later in this same opinion, the Court of Appeals said:

> This focus on the specific information shared with the subject of compelled disclosure applies with equal force in the e-mail context. Compelled disclosure of subscriber information and related records through the ISP might not undermine the e-mail subscriber's Fourth Amendment interest under *Smith,* because like the information obtained through the pen register in *Smith* and like the bank records in *Miller,* subscriber information and related records are records of the service provider as well, and may likely be accessed by ISP employees in the normal course of their employment. Consequently, the user does not maintain the same expectation of privacy in them vis-a-vis the service provider, and a third party subpoena to the service provider to access information that is shared with it likely creates no Fourth Amendment problems. [FN3] The combined precedents of *Katz* and *Smith,* however, recognize a heightened protection for the content of the communications. Like telephone conversations, simply because the phone company or the ISP could access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course. [footnote omitted]

> FN3. Indeed, the SCA itself largely tracks this distinction by making it easier for the government to obtain records and subscriber information than to obtain the content of e-mails. Compare 18 U.S.C. § 2703(c)(2) (requiring disclosure by ISP to government of account holder's basic identifying information as a matter of course and without notice to account holder) with 18 U.S.C. § 2703(b) (requiring warrant, subpoena, or court order to obtain "contents of any wire or electronic communication").

> Similarly, under both *Miller* and *Katz,* if the government in this case had received the content of Warshak's e-mails by subpoenaing the person with whom Warshak was e-mailing, a Fourth Amendment challenge brought by Warshak would fail, because he would not have maintained a reasonable expectation of privacy vis-a-vis his e-mailing partners. See *Phibbs,* 999 F.2d at 1077. But this rationale is inapplicable where the party subpoenaed is not expected to access the content of the documents, much like the phone company in *Katz.* Thus, as Warshak argues, the government could not get around the privacy interest attached to a private letter by simply subpoenaing the postal service with no showing of probable cause, because unlike in *Phibbs,* postal workers would not be expected to read the letter in the normal course of business. See *Ex Parte Jackson,* 96 U.S. 727, 733, 24 L.Ed. 877 (1878) ("No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution."). Similarly, a bank customer maintains an expectation of privacy in a safe deposit box to which the bank lacks access [FN5] (as opposed to bank records, like checks or account statements) and the government could not compel disclosure of the contents of the safe deposit box only by subpoenaing the bank.

> FN5. See United States v. Thomas, No. 88-6341, 1989 WL 72926, at *2, 1989 U.S.App. LEXIS 9628, at *6 (6th Cir. July 5, 1989) ("Citizens have legitimate expectations of privacy in the contents of their safe deposit boxes.").

Warshak v. U.S., 490 F.3d 455, 471-472 (6thCir. 18 June 2007).

Later in *Warshak* there are a few terse sentences that may indicate a much more serious intrusion on privacy than obtaining a subpoena to learn the identity of anonymous screen names. The government informed the *Warshak* court that "ISPs regularly screen users' e-mails for viruses, spam, and child pornography."[26] I am aware that some ISPs screen e-mail for viruses or spam, but only with the permission of the user — the user can disable these services. Screening all e-mail for child pornography and reporting such e-mail to law enforcement is a potential invasion of privacy by the ISP. The court in *Warshak* tersely dismissed this concern:

> The government's statement that this process involves "technology," rather than manual, human review, suggests that it involves a computer searching for particular terms, types of images, or similar indicia of wrongdoing that would not disclose the content of the e-mail to any person at the ISP or elsewhere, aside from the recipient. But the reasonable expectation of privacy of an e-mail user goes to the content of the e-mail message. The fact that a computer scans millions of e-mails for signs of pornography or a virus does not invade an individual's content-based privacy interest in the e-mails and has little bearing on his expectation of privacy in the content. In fact, these screening processes are analogous to the post office screening

---

[26] *Warshak v. U.S.,* 490 F.3d at 474.

> packages for evidence of drugs or explosives, which does not expose the content of written documents enclosed in the packages. The fact that such screening occurs as a general matter does not diminish the well-established reasonable expectation of privacy that users of the mail maintain in the packages they send.

Warshak v. U.S., 490 F.3d 455, 474 (6thCir. 2007).

Note that the court cites no authority for its opinion. The analogy to the post office sniffing packages for explosives is flawed — explosives or anthrax in the mail is a life-threatening hazard to post office personnel. In contract, content of e-mail is never a hazard to employees of an ISP.

On 9 Oct 2007, the Sixth Circuit agreed to hear *Warshak* en banc, and they vacated the opinion of the three-judge panel that is reported at 490 F.3d 455.

search topics on Internet

Using the reasoning in *Smith v. Maryland,* the government could demand a search engine provide IP addresses of users who type certain words[27] as a query to the search engine. Under the law discussed above, the government could then obtain a warrant or subpoena to the Internet Service Provider (ISP) to provide the subscriber's name and address for each IP address.

Apparently the first case about privacy of search engine queries is *Gonzales v. Google, Inc.,* 234 F.R.D. 674 (N.D.Cal. 17 Mar 2006). This case arose out of a long series[28] of challenges by the ACLU to the constitutionality of the Child Online Protection Act, 47 U.S.C. § 231 (enacted 1998). During this litigation, the government decided it wanted data from search engines to test blocking and filtering software as possible least restrictive alternatives to the challenged statute. AOL, Yahoo!, and Microsoft gave the requested data from their search engines to the government without a fuss. However, Google challenged the government's subpoena. Google argued that it would be lose business goodwill — i.e., the trust of its users — if it gave 5000 search engine queries to the government.[29] Judge Ware agreed: the "burden of loss of trust by Google's users base on Google's disclosure of its users' search queries to the Government outweighs the ... benefit to the Government's study."[30] Judge Ware denied the Government's request for 5000

---

[27] The words might be associated with pedophiles, terrorists, and other criminal activity. For example, the query "how to make a bomb" might lead law enforcement to suspects before the bomb is detonated.

[28] *American Civil Liberties Union v. Reno,* 31 F.Supp.2d 473 (E.D.Pa. 1999) (granted preliminary injunction), *aff'd,* 217 F.3d 162 (3dCir. 2000), *vacated,* 535 U.S. 564 (2002), *on remand,* 322 F.3d 240 (3dCir. 2003), *aff'd and remanded,* 542 U.S. 656 (2004), *on remand,* 2006 WL 2927284 (E.D.Pa. Oct 11, 2006) (denied government's motion), 478 F.Supp.2d 775 (E.D.Pa. 22 Mar 2007) (issued permanent injunction).

[29] 234 F.R.D. at 683-684.

[30] 234 F.R.D. at 686.

search engine queries. Then, Judge Ware, on his own initiative, raised the question of privacy of Google's users:

> The Court raises, sua sponte, its concerns about the privacy of Google's users apart from Google's business goodwill argument. **....**
>
> The Government contends that there are no privacy issues raised by its request for the text of search queries because the mere text of the queries would not yield identifiable information. Although the Government has only requested the text strings entered (Subpoena at 4), basic identifiable information may be found in the text strings when users search for personal information such as their social security numbers or credit card numbers through Google in order to determine whether such information is available on the Internet. (Cutts Decl. ¶¶ 24-25.) The Court is also aware of so-called "vanity searches," where a user queries his or her own name perhaps with other information. Google's capacity to handle long complex search strings may prompt users to engage in such searches on Google. (Cutts Decl. ¶ 25.) Thus, while a user's search query reading "[user name] stanford glee club" may not raise serious privacy concerns, a user's search for "[user name] third trimester abortion san jose," may raise certain privacy issues as of yet unaddressed by the parties' papers. This concern, combined with the prevalence of Internet searches for sexually explicit material (Supp. Stark Decl. ¶ 4)[31] — generally not information that anyone wishes to reveal publicly — gives this Court pause as to whether the search queries themselves may constitute potentially sensitive information.
>
> The Court also recognizes that there may a difference between a private litigant receiving potentially sensitive information and having this information be produced to the Government pursuant to civil subpoena. The interpretation of the Federal Rules in this Circuit requires that "when the government is named as a party to an action, it is placed in the same position as a private litigant, and the rules of discovery in the Federal Rules of Civil Procedure apply." *Exxon Shipping,* 34 F.3d at 776 n. 4. However, in *Exxon Shipping,* the Ninth Circuit was faced with a situation where a litigant sought discovery from the Government; in this case, information is being produced to the Government. Even though counsel for the Government assured the Court that the information received will only be used for the present litigation, it is conceivable that the Government may have an obligation to pursue information received for unrelated litigation purposes under certain circumstances regardless of the restrictiveness of a protective order.[FN7] The Court expressed this concern at oral argument as to queries such as "bomb placement white house," but queries such as "communist berkeley parade route protest war" may also raise similar concerns. In the end, the Court need not express an opinion on this issue because the Government's motion is granted only as to the sample of URLs and not as to the log of search queries.
>
> FN7. "Says the DOJ's [spokesperson Charles] Miller, 'I'm assuming that if something raised alarms, we would hand it over to the proper [authorities].' " (Decl. of Ashok Ramani, Ex. B. "Technology: Searching for Searches," NEWSWEEK, Jan. 30, 2006.) (second alteration in original)

Gonzales v. Google, 234 F.R.D. at 687-688.

---

[31] "... over a quarter of all Internet searches are for pornography ... indicates that at least some of Google's users expect some sort of privacy in their searches." 234 F.R.D. at 684.

Note that Judge Ware cited neither *Miller* nor *Smith v. Maryland.* The conclusion depends on whether a judge holds that a query (1) is content, which is protected under *Katz*, or (2) shared information that is available to employees of Google, which is not protected under *Miller* and *Smith.* When a user enters a query to a search engine, the user is not *creating* original content, but only providing a list of a *few* words that the user expects to find in webpages of interest to the user — an argument that makes queries akin to telephone numbers dialled. As Judge Ware correctly mentions, a user does have a privacy interest in personal sexual conduct, health care (e.g., abortion), political opinions, etc. On the other hand, the same argument was made in a dissenting opinion about the privacy of dialled telephone numbers, but that privacy argument was *un*convincing to the majority of the U.S. Supreme Court.[32]

offsite storage

Some ISPs (and various other companies) allow subscribers to store a backup copy of the user's computer files on a computer owned and operated by the ISP (or storage company). I wonder if application of the rule in *Miller* and *Smith v. Maryland* leads to the conclusion that a user has *no* privacy in files that are stored on someone else's computer. This is a serious concern, because wordprocessing documents may contain confidential information, spreadsheets and accounting files probably contain confidential information, and there may be confidential information in other kinds of files.

The files could be analogized to contents of a telephone call, for which there is a legitimate expectation of privacy. However, because the files are communicated to the storage company's automatic equipment — by analogy with the transmission of dialled telephone numbers in *Smith v. Maryland* — courts may find that there is *no* legitimate expectation of privacy. Once the files are stored on company A's computer, it is a trivial task for an employee of company A to browse through the file names and display (or copy) the contents of the files. Since the storage computer is connected to the Internet, it is also possible that a hacker could enter the computer and browse, change, or delete files.

The written contact between the owner of the files and the owner of the storage computer is not likely to create a strong privacy right for the owner of the files, because the contract is written by the storage company and is therefore unlikely to create legal liability for the storage company.

---

[32] *Smith v. Maryland,* 442 U.S. at 748 (Stewart, J., dissenting). Quoted above, at page 17.

Records of Bookshops and Libraries

When one checks a book out of the library, one must disclose each book to a librarian. Does the rule in *Miller* and *Smith v. Maryland* mean that disclosure to a librarian destroys the confidentiality of which books a patron borrows? The American Library Association is adamant that there is confidentiality of library records.[33] Similarly, when one purchases a book at a bookshop, one must disclose the purchase to a sales clerk. However, there are surprisingly few reported cases on this topic.

Brown v. Johnston

An Iowa state investigator obtained a subpoena from a county attorney that directed the Des Moines Public Library to provide the names of all persons who had checked out any books on a list attached to the subpoena. "The State's application requested a long list of titles dealing mainly with witchcraft and related topics."[34] A state statute mandated confidentiality of library records:

> The following public records shall be kept confidential, unless otherwise ordered by a court, by the lawful custodian of the records, or by another person duly authorized to release information:
>
> ....
>
> 13. The records of a library which, by themselves or when examined with other records, would reveal the identity of the library patron checking out or requesting an item from the library.

Iowa Code § 68A7, quoted in *Brown v. Johnston,* 328 N.W.2d 510, 511 (Iowa 1983).

Despite this statute (which plainly specifies a court order, *not* a subpoena from a county attorney) and after tersely considering constitutional privacy arguments by the plaintiffs, the Iowa Supreme Court refused to quash the subpoena:

> The State's interest in well-founded criminal charges and the fair administration of criminal justice must be held to override the claim of privilege here. ....

Brown v. Johnston, 328 N.W.2d 510, 513 (Iowa 1983).

I think this is a horrible case. Maybe the proper conclusion is "Don't live in Iowa, if you want to check out books on witchcraft." <*laughing*>

---

[33] See the American Library Association policy, adopted in 1971 and amended in 1975 and 1986: http://www.ala.org/ala/oif/statementspols/otherpolicies/confidentialitylibraryrecords.pdf

[34] *Brown v. Johnston,* 328 N.W.2d 510, 511 (Iowa 1983).

Kramerbooks & Afterwords

In April 1998, Independent Counsel Kenneth Starr had a grand jury issue subpoenas to two bookstores to produce "all documents and things referring or relating to any purchase by Monica Lewinsky" from Nov 1995 to the present. Starr was seeking a list of books that Monica had given to President Bill Clinton. Each bookstore moved to quash the subpoena. In a preliminary ruling, Judge Norma Holloway Johnson ordered Starr to submit "a filing describing its need for the materials sought". *In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.,* 26 MEDIA LAW REPORTER 1599 (D.D.C. 6 April 1998). One of the bookshops, Barnes & Noble, made a disclosure to the judge. On 8 June 1998 the judge found "none of the material submitted by Barnes & Noble falls within the zone of compelling interest", and the judge quashed that subpoena.[35] Subsequently attorneys for Kramerbooks negotiated with Starr and Starr agreed not to request Lewinsky's purchase records. Because the later Colorado Supreme Court case of *Tattered Cover* cites more U.S. Supreme Court cases — and does a more comprehensive job of explaining why book purchases should be confidential — than the *Kramerbooks* opinion, I have chosen not to quote the *Kramerbooks* opinion.

Patriot Act

Section 215 of the Patriot Act in 2001,[36] 50 U.S.C. § 1861, gave the government the ability to obtain an order from the Foreign Intelligence Surveillance Court for production of business records, specifically including "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records".[37] The American Library Association[38] and American Civil Liberties Union — amongst others — have opposed this section of the Patriot Act. In practice, it appears that it was too much trouble for the FBI to request library records this way.[39] Instead FBI agents used a National Security Letter, as discussed in my essay at http://www.rbs2.com/NSL.pdf

---

[35] Phillip Taylor, "Kramerbooks declares victory in subpoena battle," http://www.freedomforum.org/templates/document.asp?documentID=9736 (22 June 1998).

[36] Public Law 107-56, 115 Statutes-At-Large 272, 287-288 (enacted 26 Oct 2001).

[37] 50 U.S.C. § 1861(a)(3), added by 120 Stat. 192, 196 (enacted 9 Mar 2006).

[38] http://www.ala.org/ala/oif/ifissues/usapatriotact.htm

[39] See, e.g., *American Civil Liberties Union v. U.S. Dept. of Dept. of Justice,* 321 F.Supp.2d 24, 27 (D.D.C. 2004) (§ 215 used zero times in first two years); *Doe v. Gonzales,* 386 F.Supp.2d 66 (D.Conn. 2005) (National Security Letter used at library).

Whether library records are obtained under 50 U.S.C. § 1861 or obtained by a National Security Letter, I am concerned that disclosure of books to a librarian when borrowing them may — according to the rule in *U.S. v. Miller* — destroy any privacy rights that the library patron had.

Tattered Cover

A police department in Colorado executed a search warrant on a bookshop for records of all books purchased by a specific individual, who was suspected of manufacturing illicit drugs, during a thirty-day period. The bookshop challenged the search warrant in court. A unanimous Colorado Supreme Court quashed the search warrant.

> With this case, we recognize that both the First Amendment to the United States Constitution and Article II, Section 10 of the Colorado Constitution protect an individual's fundamental right to purchase books anonymously, free from governmental interference. Law enforcement officials implicate this right when they seek judicial approval of a search warrant authorizing seizure of customer purchase records from an innocent, third-party bookseller. This case requires us to decide what test should be applied to balance the constitutional rights of individuals and bookstores against the duty of law enforcement officials to investigate crime.
>
> We hold that the Colorado Constitution requires that the innocent bookseller be afforded an opportunity for an adversarial hearing prior to execution of a search warrant seeking customer purchase records. At that hearing, the court must apply a balancing test to determine whether the law enforcement need for the search warrant outweighs the harm to constitutional interests caused by its execution. In order for law enforcement officials to prevail, they must demonstrate a compelling governmental need for the specific customer purchase records that they seek. **....**

Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1047 (Colo. 2002).

> At that hearing [in the trial court], the Tattered Cover presented unrefuted testimony that the execution of the search warrant in this case would have a substantial chilling effect on the willingness of its customers to purchase controversial books. Meskis stated that she had received an "enormous amount of feedback" from customers about this case, including over one hundred letters from customers in support of the Tattered Cover's position. Many customers told Meskis that they shopped at the Tattered Cover because of the Tattered Cover's policy of not disclosing customer book purchase records. Meskis further testified that if book purchase records were made available to investigative authorities, customers would not feel at ease perusing, buying, or reading a wide variety of books. Meskis pointed out that "people who read books are very concerned about First Amendment issues, and their privacy as it relates to First Amendment issues. This is not an uninformed society, they care."
>
> There was also other testimony at the hearing about the warrant's likely effect. An official from the American Library Association testified about the chilling effect that results from disclosure of library circulation records. A bookstore owner from the State of Washington also testified about the concerns expressed by his customers about their privacy rights while a case analogous to this one, *In re Grand Jury Subpoena to Kramerbooks & Afterwords Inc.,* 26 Med. L. Rptr. 1599 (D.D.C. 1998), discussed in detail below, was pending.

Tattered Cover, Inc., 44 P.3d at 1050.

The Colorado Supreme Court noted that "freedom of speech" in the federal and state constitutions also included the freedom to receive ideas, and specifically the freedom to read. This is the legal basis for protecting the anonymity of purchasers of books, and also protecting the anonymity of books borrowed from libraries.

> The First Amendment to the United States Constitution protects more than simply the right to speak freely. It is well established that it safeguards a wide spectrum of activities, including the right to distribute and sell expressive materials, the right to associate with others, and, most importantly to this case, the right to receive information and ideas. [FN11] These various rights, though not explicitly articulated in either the Federal or Colorado Constitution, are necessary to the successful and uninhibited exercise of the specifically enumerated right to "freedom of speech." [two footnotes omitted]
>
> FN11. See, e.g., *Stanley v. Georgia,* 394 U.S. 557, 564, 89 S.Ct. 1243, 22 L.Ed.2d 542 (1969) ("It is now well established that the Constitution protects the right to receive information and ideas."); *Griswold v. Connecticut,* 381 U.S. 479, 482, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965) ("The right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, the right to read ... and freedom of inquiry...."); *Bantam Books, Inc. v. Sullivan,* 372 U.S. 58, 64-65 n. 6, 83 S.Ct. 631, 9 L.Ed.2d 584 (1963) ("The constitutional guarantee of freedom of the press embraces the circulation of books as well as their publication."); *Smith v. California,* 361 U.S. 147, 150, 80 S.Ct. 215, 4 L.Ed.2d 205 (1959) (stating that "the free publication and dissemination of books and other forms of the printed word furnish very familiar applications" of the First Amendment); *Martin v. City of Struthers,* 319 U.S. 141, 143, 63 S.Ct. 862, 87 L.Ed. 1313 (1943) ("The right of freedom of speech and press has broad scope.... This freedom embraces the right to distribute literature ... and necessarily protects the right to receive it."); *Lovell v. City of Griffin,* 303 U.S. 444, 452, 58 S.Ct. 666, 82 L.Ed. 949 (1938) (circulation of expressive material is constitutionally protected).

> Without the right to receive information and ideas, the protection of speech under the United States and Colorado Constitutions would be meaningless. It makes no difference that one can voice whatever view one wishes to express if others are not free to listen to these thoughts. The converse also holds true. Everyone must be permitted to discover and consider the full range of expression and ideas available in our "marketplace of ideas." [FN13] As Justice Brandeis so eloquently stated, "[Our founders] believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth." *Whitney v. California,* 274 U.S. 357, 375, 47 S.Ct. 641, 71 L.Ed. 1095 (1927) (Brandeis, J., concurring). [footnote omitted]
>
> FN13. See, e.g., *Stanley,* 394 U.S. at 565, 89 S.Ct. 1243 ("[The petitioner] is asserting the right to be free from state inquiry into the contents of his library.... If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch."); *Lamont v. Postmaster Gen.,* 381 U.S. 301, 308, 85 S.Ct. 1493, 14 L.Ed.2d 398 (1965) (Brennan, J., concurring) ("The dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them. It would be a barren marketplace of ideas that had only sellers and no buyers.").

....

Anonymity is often essential to the successful and uninhibited exercise of First Amendment rights, precisely because of the chilling effects that can result from disclosure of identity. The Supreme Court has recognized this principle numerous times in various contexts.[FN16] For instance, in *McIntyre v. Ohio Elections Commission,* the Court stated, "Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation-and their ideas from suppression-at the hand of an intolerant society." 514 U.S. 334, 357, 115 S.Ct. 1511, 131 L.Ed.2d 426 (1995) (citation omitted). In another case, *Lamont v. Postmaster General,* 381 U.S. 301, 307, 85 S.Ct. 1493, 14 L.Ed.2d 398 (1965), the Court struck down a federal statute that required citizens who wished to receive "communist political propaganda" to affirmatively so notify the post office. The Court's holding rested on concerns that First Amendment speech rights would be chilled if people were required to reveal their identities before being able to receive these expressive materials. *Id.*

FN16. See, e.g., *Talley v. California,* 362 U.S. 60, 64-65, 80 S.Ct. 536, 4 L.Ed.2d 559 (1960) (invalidating a law that prohibited the distribution of handbills that did not include the names and addresses of those who prepared, distributed, or sponsored it); *Bates v. City of Little Rock,* 361 U.S. 516, 527, 80 S.Ct. 412, 4 L.Ed.2d 480 (1960) (reversing conviction based on violation of an ordinance requiring organizations to disclose their membership lists); *Bursey,* 466 F.2d at 1085 ("Protection of the anonymity of publishers, printers, and distributors of newspapers and pamphlets is an integral part of press freedom.").

The need to protect anonymity in the context of the First Amendment has particular applicability to book-buying activity. As was explained in *United States v. Rumely,* governmental inquiry and intrusion into the reading choices of bookstore customers will almost certainly chill their constitutionally protected rights:

> Once the government can demand of a publisher the names of the purchasers of his publications, the free press as we know it disappears. Then the spectre of a government agent will look over the shoulder of everyone who reads.... Fear of criticism goes with every person into the bookstall. The subtle, imponderable pressures of the orthodox lay hold. Some will fear to read what is unpopular, what the powers-that-be dislike. [When the light of publicity may reach any student, any teacher, inquiry will be discouraged. The books and pamphlets that are critical of the administration, that preach an unpopular policy in domestic or foreign affairs, that are in disrepute in the orthodox school of thought will be suspect and subject to investigation. The press and its readers will pay a heavy price in harassment. But that will be minor in comparison with the menace of the shadow which government will cast over literature that does not follow the dominant party line. If the lady from Toledo can be required to disclose what she read yesterday and what she will read tomorrow,][40] fear will take the place of freedom in the libraries, book stores, and homes of the land. Through the harassment of hearings, investigations, reports, and subpoenas government will hold a club over speech and over the press.

Rumely, 345 U.S. 41, 57-58, 73 S.Ct. 543, 97 L.Ed. 770 (1953) (Douglas, J., concurring). The right to engage in expressive activities anonymously, without government intrusion or observation, is critical to the protection of the First Amendment rights of book buyers and sellers, precisely because of the chilling effects of such disclosures. Search warrants directed to bookstores, demanding information about the reading history of customers, intrude upon

---

[40] Brackets enclose text of Justice Douglas' concurring opinion in *Rumely* that was omitted from the Colorado Supreme Court's opinion in *Tattered Cover.*

> the First Amendment rights of customers and bookstores because compelled disclosure of book-buying records threatens to destroy the anonymity upon which many customers depend.
>
> In sum, the First Amendment embraces the individual's right to purchase and read whatever books she wishes to, without fear that the government will take steps to discover which books she buys, reads, or intends to read. A governmental search warrant directed to a bookstore that authorizes seizure of records that reflect a customer's purchases necessarily intrudes into areas protected by this right. [footnote omitted]

Tattered Cover, Inc., 44 P.3d at 1051-1053.

The Colorado Supreme Court noted the "conflict" between the First and Fourth Amendments to the U.S. Constitution.

> Conflicts between First Amendment and Fourth Amendment rights are inevitable when law enforcement officials attempt to use search warrants to obtain expressive materials. This is because a seizure of documents, books, or films is conceptually distinct from a seizure of objects such as guns or drugs. See, e.g., *A Quantity of Books v. Kansas,* 378 U.S. 205, 211-12, 84 S.Ct. 1723, 12 L.Ed.2d 809 (1964). The former category of objects implicates First Amendment expressive rights, while the latter category of objects does not. *Id.*
>
> Outside the context of obscenity, few federal cases have discussed this collision between the Fourth Amendment and the First Amendment. However, the Supreme Court has made clear that, when expressive rights are implicated, a search warrant must comply with the particularity requirements of the Fourth Amendment with "scrupulous exactitude." *Zurcher v. Stanford Daily,* 436 U.S. 547, 564, 98 S.Ct. 1970, 56 L.Ed.2d 525 (1978); *Stanford v. Texas,* 379 U.S. 476, 485, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965).
>
> ....
>
> The Fourth Amendment provides significant and important privacy protections to Americans. Nonetheless, there are occasionally situations where the Fourth Amendment simply does not go far enough. This case presents one such situation.

Tattered Cover, Inc., 44 P.3d at 1055.

I disagree with the Colorado Supreme Court about both (1) "conflicts ... are inevitable" and (2) the alleged "collision" between Amendments. If a search is permissible under the Fourth Amendment, but not permissible under the First Amendment, then the final result is that the search is *not* permissible. This is *not* a conflict between Amendments, but rather a case where an infringed right exists under the First Amendment, but not under the Fourth Amendment.[41]

The Colorado Supreme Court gave residents of Colorado more protection than federal law in *Zurcher.* The U.S. Supreme Court in *Zurcher* only required that the search warrant specify with "scrupulous exactitude" the items to be seized. However, the Colorado Supreme Court held:

---

[41] For a situation involving a true conflict between amendments, consider (1) the First Amendment right of the news media to publish information that will prejudice a future jury in a criminal trial and (2) the Sixth Amendment right of a criminal defendant to an initially impartial jury. In this situation there are *two* different groups of people with conflicting rights. See, e.g., Ronald B. Standler, *Pretrial Publicity Prevents a Fair Trial in the USA,* http://www.rbs2.com/pretrial.pdf (Jan 2004).

> Thus, we find the protections afforded to fundamental expressive rights by federal law, under the above interpretation of *Zurcher,* to be inadequate. **....**
>
> Our basic rationale for this holding is that, before law enforcement officials are permitted to take actions that are likely to chill people's willingness to read a full panoply of books and be exposed to diverse ideas, law enforcement officials must make a heightened showing of their need for the innocent bookstore's customer purchase records. We emphasize that a bookstore's customer purchase records are not absolutely protected from discovery and that this question must be decided on the particular facts of each case.

Tattered Cover, Inc., 44 P.3d at 1056.

For more about this case, see the essay by the owner of Tattered Cover, Joyce Meskis, published in 79 DENVER UNIV. LAW REVIEW 522 (2002).

Personal Letters

People often write intimate thoughts or private facts in personal letters or e-mail to a friend or relative. While there is confidentiality for the communication in transit, once the letter or e-mail is opened by the recipient, there is no longer any confidentiality, following the rule in *Miller* about disclosure destroying privacy.

Hubbard

In 1979, federal agents executed search warrants on three properties owned by the Church of Scientology. The Church filed a motion with a U.S. District Court for the return of various documents. The court denied the request, holding:

> The defendants' second ground is completely unconvincing. According to the defendants, merely because they purportedly authored or were to receive certain letters, they have a legitimate expectation of privacy with respect to the contents of such letters. First, the defendants cannot rely on the government's "purported" allegations or the indictment, but have the burden of asserting a property or possessory interest in the seized property. *Rakas v. Illinois,* 99 S.Ct. 421, 423 n.1 (1978).[footnote omitted] Having failed to do so, they have failed to meet their burden. Second, even assuming the defendants had established that they received the letters would not decide the issue. The legitimate expectations of privacy of a party who has received letters is obviously affected by what happens to the letters after their arrival. If the letters are kept in the office of the addressee, the addressee would have standing under the rule of the *Mancusi* case [392 U.S. 364]. However, if the letters are forwarded to a central filing system, and access to such system is available to numerous third parties, the expectations of privacy would be seriously undermined. Finally, the Court is unable to understand how sending letters to a third party would form a basis for a legitimate expectation of privacy after their delivery. [footnote omitted] The reasonableness of one's privacy expectations would certainly be undermined by the act of relinquishing control. See *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976).

U.S. v. Hubbard, 493 F.Supp. 209, 214-215 (D.C.D.C. 1979).

Ray

In 1980, James Earl Ray — the assassin of Martin Luther King — alleged that an investigator for a U.S.House of Representatives Committee had directed a third party to steal, from Ray's brother's hotel room, letters that Ray had written to his brother. The U.S. District Court dismissed Ray's claims and the U.S. Court of Appeals affirmed:

> The district court, relying on *Rakas v. Illinois,* 439 U.S. 128, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978), held that Ray lacked standing to raise a Fourth Amendment claim for damages because the search and seizure involved the property and premises of another, Jerry Ray. *Ray v. United States Department of Justice,* supra, 508 F.Supp. at 726. The district court apparently concluded that James' letters to Jerry Ray became Jerry's property upon receipt and that James accordingly lost any expectations of privacy that he had in the letters. *Id.*
>
> Although not cited by the district court, *United States v. Hubbard,* 493 F.Supp. 209 (D.D.C. 1979), supports its conclusion. **....** Therefore, the appellant [i.e., James Earl Ray] did not retain a legitimate expectation of privacy in those papers. We agree with the district court's dismissal of this claim because James Earl Ray lacks standing to contest the alleged search of Jerry Ray's hotel room.

Ray v. U.S. Dept. of Justice, 658 F.2d 608, 610-611 (8thCir. 1981) (per curiam).

King

In January 1992, a Mrs. King asked her former husband, Peter Trainor, to remove some papers from her home and burn them. Instead, Trainor gave some of the papers — including 51 letters from Mrs. King's current husband — to the FBI. The letters "contained detailed instructions from defendant to his wife concerning ways in which to commit bank fraud."[42] The letters were used as evidence in Mr. King's trial, where he was convicted and sentenced to 33 months in prison. The U.S. Court of Appeals affirmed:

> We agree with the government's contention that King has no standing to challenge the government's seizure and use of the letters he mailed to his wife. We also agree with the government that, even if King had standing to allege a Fourth Amendment violation, the letters should not be suppressed because they were acquired through the acts of a private individual.
>
> **....**
>
> It is well established that letters are "in the general class of effects" protected by the Fourth Amendment. *United States v. Jacobsen,* 466 U.S. 109, 114, 104 S.Ct. 1652, 1656, 80 L.Ed.2d 85 (1984). However, if a letter is sent to another, the sender's expectation of privacy ordinarily terminates upon delivery. 4 Wayne R. LaFave, SEARCH AND SEIZURE, § 11.3(f)(1987); *United States v. Knoll,* 16 F.3d 1313, 1321 (2nd Cir.), *cert. denied sub nom., Gleave v. United States,* 513 U.S. 1015, 115 S.Ct. 574, 130 L.Ed.2d 490 (1994). This is true even though the sender may have instructed the recipient to keep the letters private.

---

[42] *U.S. v. King,* 55 F.3d 1193, 1195.

United States v. Williams, 951 F.2d 853, 856 (7th Cir. 1992) (test for standing is whether sender of note expected it to be returned).

In this case, King voluntarily mailed the letters at issue to his wife. Although he may have instructed her to preserve the confidentiality of the letters, there is no evidence that he expected her to return the letters to him. Under those circumstances, his expectation of privacy in the letters terminated upon delivery of the letters to his wife. Therefore, King lacks standing to allege a Fourth Amendment violation in the seizure of those letters.

In addition, even if King had standing, the letters should not be suppressed because the government acquired them through the actions of a private individual. The Fourth Amendment does not apply to searches or seizures by private persons. *Jacobsen,* 466 U.S. at 114, 104 S.Ct. at 1656. Rather, it "proscribes only governmental action and does not apply to a search or seizure, even an unreasonable one, conducted by a private individual not acting as an agent of the government or with the participation or knowledge of any governmental official." *United States v. Lambert,* 771 F.2d 83, 89 (6th Cir.), *cert. denied,* 474 U.S. 1034, 106 S.Ct. 598, 88 L.Ed.2d 577 (1985).

Once a private search is conducted, the government's subsequent use of the information obtained in the private search does not implicate the Fourth Amendment as long as the government's use does not exceed the scope of the private search. *Jacobsen,* 466 U.S. at 116-117, 104 S.Ct. at 1658. This is true even if the private party betrayed a confidence in providing the information to the government:

It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information:

> "This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in a third party will not be betrayed."

Id. at 117, 104 S.Ct. at 1658 (quoting *United States v. Miller,* 425 U.S. 435, 443, 96 S.Ct. 1619, 1624, 48 L.Ed.2d 71 (1976)).

U.S. v. King, 55 F.3d 1193, 1195-1196 (6thCir. 1995).

Gordon

Gordon sent letters containing photographs of "large sums of currency" to a prison inmate. Mail to prisoners that is neither "legal, official, [n]or privileged" is routinely searched by prison authorities. The prison authorities suspected that Gordon, the author of the letters, was engaged in illegal "drug or gang activity". Because Gordon was on parole, the prison authorities sent a copy of the letter and photographs to Gordon's parole officer. Gordon was subsequently arrested and charged with various crimes. His attorney moved to suppress the letters and photographs. The U.S. District Court denied the motion and the U.S. Court of Appeals affirmed:

The district court refused to suppress the letters intercepted by Lieutenant Barnes at the El Dorado Correctional Facility. Defendant argues this was error. We disagree. In order to challenge the seizure of the letters, Defendant must have a reasonable expectation of privacy in the items seized. See *Rakas,* 439 U.S. at 143-44, 99 S.Ct. 421. Although letters "are in the general class of effects in which the public at large has a legitimate expectation of privacy,"

> *United States v. Jacobsen,* 466 U.S. 109, 115, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984), the Fourth Amendment does not protect items "knowingly exposed to the public." *United States v. Miller,* 425 U.S. 435, 442, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976) (internal quotations omitted). Thus, once a letter is sent to someone, "the sender's expectation of privacy ordinarily terminates upon delivery." *United States v. King,* 55 F.3d 1193, 1196 (6thCir. 1995). In the case of unprivileged incoming and outgoing prison mail, regulation by prison officials is "essentially an administrative matter in which the courts will not intervene." *Wilkerson v. Warden of U.S. Reformatory, El Reno,* 465 F.2d 956 (10th Cir. 1972).
>
> In this case, Defendant sent the letters and photographs to an inmate in a correctional facility. As a former inmate of that facility, Defendant was aware that under prison regulations all mail that was not "legal, official or privileged mail may be inspected at any time." Kansas Admin. Regulations 44-12-601(I)(1). Defendant does not claim that these letters were "legal, official or privileged." **....** Because Defendant sent the letters to an inmate at a correctional facility, fully aware that prison officials could lawfully and, would likely, inspect the letters, he had no reasonable expectation of privacy in them.

U.S. v. Gordon, 168 F.3d 1222, (10thCir. 1999).

While the Defendant, Gordon, was a parolee who sent a letter to a prison inmate, the holding of the U.S. Court of Appeals is general enough to apply to *any* letter sent to anyone. According to *Gordon* — citing *Miller* — sending a letter to *one* person is equivalent to a public disclosure. This rule of law seems wrong to me.

Guest v. Leis

The case of *Guest v. Leis* was discussed above in the context of revealing identities of people who used anonymous screen names. Another part of the opinion in *Guest v. Leis* declares that there is no privacy for e-mail after delivery to the recipient.

> The Guest user-plaintiffs' standing would turn on the materials they had on the CCC BBS. Users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting. See *United States v. Maxwell,* 45 M.J. 406, 417-19 (C.A.A.F. 1996). They would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose "expectation of privacy ordinarily terminates upon delivery" of the letter. *United States v. King,* 55 F.3d 1193, 1196 (6th Cir. 1995) (citations omitted); see also *Maxwell,* 45 M.J. at 418. Whether the users had more private material on the system that entitled them to standing is not a question we must reach since we conclude below that there was no Fourth Amendment violation in this case.

Guest v. Leis, 255 F.3d 325, 333 (6thCir. 2 July 2001).

This holding is cited with approval in *U.S. v. Lifshitz,* 369 F.3d 173, 190 (2dCir. 2004).

Dunning

The First Circuit considered a case involving privacy of letters after delivery to the recipient. The relevant facts are reported in a judicial opinion:

> On March 1, 2000, Dunning learned that Dawn Touchette was pregnant. After learning that he was the father, Dunning surrendered himself on outstanding state criminal warrants and went into custody at the Merrimack County House of Corrections. Dunning kept a correspondence with Dawn while he was incarcerated.

U.S. v. Dunning, 312 F.3d 528, 530 (1stCir. 2002).

During a search of the Touchette home, federal agents noticed several letters from Dunning to Dawn Touchette in plain view and they seized the letters. The letters were to be used as evidence against Dunning in a trial, but Dunning pled guilty. On appeal, Dunning again argued that the letters should have been suppressed as a violation of his Fourth Amendment rights. The U.S. Court of Appeals rejected Dunning's assertion:

> While it is well settled that "[l]etters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy," *United States v. Jacobsen,* 466 U.S. 109, 114, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984), the Fourth Amendment does not protect items that a defendant "knowingly exposes to the public." *United States v. Miller,* 425 U.S. 435, 442, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). Consequently, if a letter is sent to another, the sender's expectation of privacy ordinarily terminates upon delivery. *United States v. Gordon,* 168 F.3d 1222, 1228 (10th Cir. 1999); *United States v. King,* 55 F.3d 1193 (6th Cir. 1995).
>
> In this case, Dunning sent the letter to his girlfriend, Dawn Touchette, and encouraged her to share its contents with her parents. Dunning does not assert a relationship of legal confidentiality with Touchette; his assertion that he has a privacy interest in the letter derives entirely from Dunning's expectation that the two would keep their letters until after Dunning's release from prison, perhaps even to include them in a scrapbook. However, even if the sentimental letter in question — sent to tip off the Touchettes that they were the subject of an imminent raid by federal agents — was indeed a cherished memento to be preserved for the future, this does not change the fact that Dunning relinquished any expectation of privacy he may have otherwise had in the letter when it was delivered to Dawn Touchette. *Id.* at 1196.

U.S. v. Dunning, 312 F.3d 528, 531 (1stCir. 2002).

conclusion to privacy of letters/e-mail

These cases show how the rule in *Miller* degrades privacy of personal letters, by considering them as a public disclosure after the one recipient has read the contents of the letter. The rule in *Miller* is consistent with the rule stated in *On Lee, Hoffa,* and *White* that disclosure of crimes to anyone destroys privacy of that information. However, the rule in *Miller* — and repeated in the above cases — is broader than disclosure of crimes. Once the recipient has read the contents of *any* letter, those contents are considered public, and no longer private, regardless of the content.

Not only has the author lost privacy rights in the contents of his/her letter, but also the author has no standing to assert a Fourth Amendment violation when the letter is seized from the recipient's location or some other location not controlled by the author.

Note that the above cases all involve the privacy of letters or e-mail in the context of evidence in a *criminal* trial. Civil law does recognize privacy of letters or e-mail. A recipient of a letter who publishes private facts in the letter could be liable for the tort of publicity given to private life.[43] If a recipient of a letter were to publish the letter, the recipient could be liable for copyright infringement.[44]

Conclusion

As explained above, the U.S. Supreme Court has declared that disclosure of confidential information to any person destroys the confidentiality (or destroys the reasonable expectation of privacy) of that information. I believe this rule is a mistake, which the Court derived from a faulty analogy to confessions or admissions to third parties in criminal cases. After reviewing the cases cited above, I conclude:

1. The rule in *On Lee, Hoffa,* and *White* is correct: disclosure of crimes to a *non*professional person should destroy the privacy of the information.

2. We should expect better behavior from government employees (e.g., in *Lopez* and *Lewis*) than misleading suspects in order to obtain a confession to a crime.

3. The rule in *U.S. v. Miller* and *Smith v. Maryland* is wrong. There should be *at least* three exceptions to this rule in these two cases:
   A. Disclosure of confidential information to an attorney, psychotherapist, clergy, physician, or agent of those should preserve the confidentiality of the information.

   B. Disclosure of confidential information to anyone who has either a fiduciary duty of confidentiality or a duty of confidentiality recognized in statute should prevent voluntary disclosure of that information, but not prevent disclosure pursuant to a judicial order.

   C. Disclosure of confidential information to a trustworthy business should prevent voluntary disclosure of that information, but not prevent disclosure pursuant to a judicial order. A trustworthy business either
      - is regulated by a state or federal statute that mandates confidentiality of information,
      - has a First Amendment right of confidentiality,

---

[43] RESTATEMENT SECOND OF TORTS § 652D (1977).

[44] 17 U.S.C. § 106.

or

- is under a contractual obligation to maintain confidentiality of information.

There are at least five types of trustworthy businesses:

(1) Monopolies (electric utility, water, heating gas, landline telephone, garbage collection, cable television, etc.).

(2) Other necessities (e.g., bank,[45] health care providers, Internet service providers, insurance companies, credit reporting agencies,[46] etc.).

(3) Businesses dealing in materials protected by the First Amendment (e.g., library, bookseller, videocassette sale/rentals,[47] etc.).

(4) Custodial storage of records[48] (e.g., bank safe deposit box, warehouse with boxes of old paper, online backup of computer, escrow of source code, etc.)

(5) Educational institutions.[49]

The problem is that not only does the U.S. Supreme Court have a very narrow view of privacy, but also the Supreme Court is openly hostile to finding new areas of privacy.[50] Both the U.S. Congress and state legislatures have adopted a piecemeal, ad hoc approach to creating privacy rights in statutes, instead of having one statute with a comprehensive, systematic view of privacy rights of people.

I conclude that the government *should* be required to obtain a warrant from a judge — *not* a subpoena, *not* a National Security Letter — before demanding that some third party disclose confidential or private information about a person. A copy of the warrant should be given to the person whose confidential information is sought, so that person's attorney can appear in court and move to quash the warrant. Given that this change in law is unlikely to come from the U.S. Supreme Court, Congress needs to enact a statute.

I emphasize that the words in this conclusion are my personal opinion of what the law should be. This conclusion is *not* a statement of the current law in the USA.

---

[45] 12 U.S.C. § 3401 et seq. (enacted 1978).

[46] 15 U.S.C. § 1681, et seq. (enacted 1970).

[47] 18 U.S.C. § 2710 (enacted 1988).

[48] *Couch v. U.S.,* 409 U.S. 322, 337 (1973) (Brennan, J., concurring) ("In my view, the [Fifth Amendment] privilege is available to one who turns records over to a third person for custodial safekeeping ...." [citations omitted]).

[49] 20 U.S.C.A. § 1232g (enacted 1974).

[50] See, e.g., Ronald B. Standler, *Fundamental Rights Under Privacy in the USA,* http://www.rbs2.com/priv2.pdf .

Bibliography

Stephen E. Henderson, "Learning From All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information From Unreasonable Search," 55 CATHOLIC UNIV. LAW REVIEW 373 (Winter 2006).

Stephen E. Henderson, "Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too," 34 PEPPERDINE LAW REVIEW 975 (2007).

Matthew D. Lawless, Note, "The Third Party Doctrine Redux: Internet Search Records and the Case for a 'Crazy Quilt' of Fourth Amendment Protections," 2007 UCLA JOURNAL OF LAW & TECHNOLOGY 1 (Spring 2007).

Christopher Slobogin, "Subpoenas and Privacy," 54 DEPAUL LAW REVIEW 805 (Spring 2005).

Daniel J. Solove, "The First Amendment as Criminal Procedure," 82 NEW YORK UNIVERSITY LAW REVIEW 112 (April 2007).

This document is at **www.rbs2.com/priv4.pdf**
My most recent search for court cases on this topic was in October 2007.
revised 31 Oct 2007

return to my homepage at http://www.rbs2.com/