The American Bar Association
Section of Individual Rights and Responsibilities,
Princeton University Center for Information Technology Policy and the
ABA Center for Continuing Legal Education
Present

Public Access to Court Records
The materials contained herein represent the opinions of the authors and editors and should not be construed to be the action of the American Bar Association Section of Individual Rights and Responsibilities, Princeton University Center for Information Technology Policy or the Center for Continuing Legal Education unless adopted pursuant to the bylaws of the Association.

Nothing contained in this book is to be considered as the rendering of legal advice for specific cases, and readers are responsible for obtaining such advice from their own legal counsel. This book and any forms and agreements herein are intended for educational and informational purposes only.

© 2011 American Bar Association. All rights reserved.

This publication accompanies the audio program entitled “Public Access to Court Records” broadcast on March 17, 2011 (Event code: CET1PAR).
Discuss This Course Online

Visit http://www.abanet.org/cle/discuss to access the discussion board for this program. Discussion boards are organized by the date of the original program, which you can locate on the preceding page of these materials.
INTRODUCTION

An important phenomenon of the digital age is the dissemination of sensitive personal information in "public" records. Courthouse records are open to the public because transparency and accountability are essential to our democratic system of government. Many of these records contain sensitive personal information, such as Social Security numbers, medical and financial data, and information about minor children. Data mining companies purchase court records in bulk, using them for credit checks, employee background checks, and other purposes unknown to the citizens who are affected by the disclosure of the information. This means there are significant privacy concerns associated with court records, especially when they are disclosed in digital form.

The presumption of public access to court records allows citizens to monitor the functioning of our courts, thereby insuring quality, honesty, and respect for our legal system. But it does not follow that every piece of personal information contained within a “public” record in the courthouse needs to be published worldwide on the Internet. Publication of court records should be tailored to serve the court’s proper civic purposes, not to broadcast personally identifiable information like Social Security numbers.

PUBLIC RECORDS: TRANSPARENCY AND ACCOUNTABILITY

Court records have long been presumed open to the public, and the tradition of public access to court case files is rooted in constitutional principles. Legal accessibility has traditionally meant that citizens may use contemporary technology to review current law and redistribute it at will. In ancient courts, this implied open public access to the proceeding itself. Indeed, the principle was literally built into the architecture of the courthouses. As American law matured, it incorporated a right to read and reproduce the text of decisions without paying a license fee. The Copyright Act specifically exempts all government works from monopoly protection because such works essentially “belong” to the people.

1. See Richmond Newspapers v. Virginia, 448 U.S. 555, 575-77 (finding that the First Amendment right of access to criminal trials is predicated on openness, fairness, perception, and confidence in governmental process).

2. See Nixon v. Warner Communication, Inc, 98 S. Ct. 1306, 1312 (1978) (“It is clear that courts of this country recognize a general right to inspect and copy public records and documents, including judicial records and documents.”); Soc’y of Prof’l Journalists v. Briggs, 675 F. Supp 1308, 1309 (D. Utah 1987) (acknowledging a constitutional right to access public documents based on Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 583-84 (1980), which stated that the First Amendment is based on access to information and Press-Enterprise Co. v. Superior Court, 464 U.S. 501, 518 (1984), which stated “a claim to access cannot succeed unless access makes a positive contribution to this process of self-governance”).
The reasons for keeping court records open to the public are several, reflecting the balance of powers among the branches of government and civic principles of government based upon the rights and duties of the individual. For example, in criminal cases, open trials prevent prosecutorial misconduct. A very important aspect of criminal law in this country is the principle of holding law enforcement to its burden of proof. The executive branch, in the person of the prosecutor, is obliged not merely to conduct zealous prosecutions, but to serve the broader interests of justice. Criminal courts are open, therefore, in part to ensure that prosecutorial zeal is checked by rigorous legal standards. “The right of access to criminal trials in particular is properly afforded protection by the First Amendment both because such trials have historically been open to the press and public and because such right of access plays a particularly significant role in the functioning of the judicial process and the government as a whole.” Globe Newspaper Co. v. Superior Ct., 457 U.S. 596

In civil cases, court proceedings are open to the public for a number of reasons. Before damages are awarded, injunctions enforced, or money transferred from one pocket to another, our system demands that the process of adjudication be exposed to scrutiny. Broader and more convenient access to court records allows greater public understanding and scrutiny of our legal system. As information technology makes broader availability economically feasible, public officials have an obligation to respond by using those technologies to expand public access.

Access to court records keeps courts honest. If court activities are secret, the public will have no way to verify that the court's procedures and decisions are fair and consistent with the law. Public access also promotes equality before the law by ensuring that those of limited means will not be disadvantaged by a lack of access to information.

PACER stands for “Public Access to Court Electronic Records.” It is the website the federal judiciary uses to make public records available to the general public. Although PACER is officially available to the general public, it is mostly used by practicing attorneys. The site is difficult for non-lawyers to navigate, and it has a “paywall” that requires users to pay significant fees for the documents they download from PACER.

You can use PACER to access legal documents relating to thousands of federal court cases. The fee-supported structure of PACER has been allowed by Congress, most recently in the 2002 E-Government Act. The courts use the fees they collect from PACER users to maintain and upgrade the PACER system, but also for other purposes. The E-Government Act also made clear that the courts should be moving toward free public access to court records.

RECAP is an extension (or “add on”) for the Firefox web browser that improves the PACER experience while helping PACER users build a free and open repository of public court records. RECAP users automatically donate the documents they purchase from PACER into a public

---


4. See Richmond Newspapers, 448 U.S. at 569 (stating that open trials assure that proceedings are conducted fairly and discourage perjury and misconduct).

5. See U.S. v. Gooding, 25 U.S. 460, 461 (1827) (“In criminal proceedings, the onus probandi rests upon the prosecutor, unless a different provision is expressly made by statute.”).

repository hosted by the Internet Archive. And RECAP saves users money by alerting them when a document they are searching for is already available from this repository. RECAP also makes other enhancements to the PACER experience, including more user-friendly file names.


Under the rules of the federal courts, each party to a case is responsible for redacting personally-identifiable information from its own documents, and courthouse personnel are responsible for redacting documents produced directly by the courts. So in theory, there shouldn’t be any sensitive personal information in PACER. Unfortunately, these rules are not always enforced, and inappropriate information sometimes leaks out into the public version of court documents.

Ideally, the courts would do a better job of enforcing these rules. But until that happens, RECAP is taking three steps to cope with the problem:

- At RECAP’s request, the Internet Archive has disallowed search engine indexing of the documents RECAP submits. (This may be changed in the future if RECAP develops better ways of addressing privacy concerns.)
- The RECAP servers automatically scan all submitted documents for Social Security numbers before they are uploaded to the Internet Archive. Any document in which RECAP detects such information is automatically suppressed.
- RECAP users are asked to report privacy problems.

RECAP directly increases public access to legal documents by creating a free repository that anyone can access. By donating bandwidth and CPU cycles to the cause of public access, RECAP is reducing the load on the PACER servers, making it feasible for the courts to make more documents freely available with the computing resources they already have. Finally, RECAP provides an opportunity to study the practical challenges involved in large-scale open access to public documents. This should help the judiciary improve its own systems. And hopefully it will inspire the Administrative Office of the Courts to accelerate its own movement toward an open access regime.

RECAP provides free access to documents that would otherwise cost money to obtain from PACER. Free access is consistent with the principle that citizens are assumed to know the law. To ensure broad public access, the courts have long held that court records are not subject to copyright. That means that once a user has obtained a court document, he is generally free to redistribute it without payment. But until the rise of the Internet, practical barriers limited the dissemination of legal records. Courts produce millions of pages of documents every year, and it would have been impractical to distribute paper copies of every document to public libraries. In principle, anyone could have physically driven down to a courthouse and asked to see copies of court records, but practically speaking only practicing lawyers and a handful of sophisticated journalists and academics knew how to navigate this system successfully.
Internet natives expect the government to be accessible online. The US Courts were remarkably prescient in this regard, implementing electronic access to case information as early as the 1980s. However, this access came at a price. In order to fund electronic access to court records, the judiciary decided to charge user fees for every minute of dial-up access. As the web matured, the courts transitioned to the new platform and perpetuated a fee-based model. The motivation was understandable: new services cost money. However, some people began to argue that the price for this model included not only transaction costs for users, but also decreased legitimacy, accountability, fairness, and democratic due process at the heart of the open access doctrine.

Another cost of the transition to digital formats has been the rise of data mining. This has significant implications for individual privacy.

**DATA MINING: SENSITIVE PERSONAL INFORMATION**

Court records often contain information that is exquisitely personal, such as:
- Social Security numbers;
- income and business tax returns;
- information provided or exchanged by the parties in child support enforcement actions;
- home addresses of litigants, witnesses and jurors;
- photographs depicting violence, death, or children subjected to abuse;
- name, address, or telephone number of victims, including sexual assault and domestic violence cases;
- names, addresses, and telephone numbers of witnesses in criminal cases;
- names, addresses, and telephone numbers of informants in criminal cases;
- names, addresses, or telephone numbers of potential or sworn jurors in criminal cases;
- juror questionnaires and transcripts of voir dire of prospective jurors;
- medical or mental health records, including examination, diagnosis, evaluation, or treatment records;
- psychological evaluations of parties, for example regarding competency to stand trial;
- child custody evaluations in family law or abuse and neglect actions;
- information related to the performance, conduct, or discipline of judicial officers;
- information related to alleged misconduct by entities or individuals licensed or regulated by the judiciary;
- trade secrets and other intellectual property.  

The personal information taken from government records is often not used for its intended purpose but instead purchased and sold for purposes totally unrelated to government mandates. Citizens are compelled to disclose information about themselves to the courts, but their information may be mined and sold for a profit. Nor is the information used for purposes that benefit the individual.

These court records can be used to create an underclass of people who have difficulty getting jobs, renting apartments, and obtaining credit. For example, data mining companies that perform

8. Id. at 1194-95.
9. See id. at 1145, 1149-50, 1152.
employee background checks keep permanent records of arrests and criminal sentences. \(^{10}\) Once recorded in commercial databases, these records cannot be corrected or expunged, even if the arrests never led to conviction or if the data become stale and irrelevant. \(^{11}\) This disproportionately affect minority groups in the United States. \(^{12}\)

Traditionally, documents that make it through the courthouse door become part of the public record and open to scrutiny. However, this tradition was not intended for the purpose of broadcasting details about the litigants. \(^{13}\) Government records are made available to the public so that citizens can make political decisions, to instill confidence in the system, to make the government accountable, and to facilitate business, personal and legal affairs. \(^{14}\)

The difficulty with publishing every data item that comes into the courthouse is that although it would preserve the principle that judicial proceedings should be conducted in public, there is a substantial risk that over-publication will have a chilling effect.

The courts and state and local government agencies must not disregard the consequences of publishing these records. State actors have no obligation to help data mining companies make a profit. However, state and local government agencies do have an obligation to protect the public interest in privacy. This can be done without compromising the spirit and purpose of open government records legislation, which is to shed light on government operations. The courts should make it a condition of doing business, that data aggregators adopt the principles of fair information practices.

**FAIR INFORMATION PRACTICES**

United States Privacy Protection Study Commission articulated a set of fair information practices to limit the government’s use of personally identifiable information. \(^{15}\) These principles provide guidelines to limit the collection, use, disclosure, retention, and disposal of personal information by the government, and they have become widely accepted. \(^{16}\) The following principles of fair information practices:

---


13. For this reason, discovery is not conducted in public domain, but in confidence. Indeed, the government has a substantial interest in controlling and preventing discovery abuse. See Rhinehart v. Seattle Times Co., 654 P.2d 673, 690 (Wash. 1982); see also Wilk v. Am. Med. Ass’n, 635 F.2d 1295, 1300-01 (7th Cir. 1981) (suggesting a party would not be entitled to a hearing if it brought suit solely to obtain discovery material); Hammock v. Hoffman LaRoche, Inc., 662 A.2d 546, 558 (N.J. 1995) (finding that the public interest in health and welfare may be invoked to prevent abuse of discovery for commercial gain or competitive advantage).


information practices have become the foundation for many privacy laws and codes of practice around the world:

Collection limitation. There should be limits to the collection of personal data. Any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject.

Data Quality. Personal data should be relevant to the purposes for which the data are gathered and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

Purpose Specification. The purposes for which personal data are collected should be specified no later than the time of data collection, and the subsequent use should be limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation. Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with the purpose specification principle except with the consent of the data subject or by the authority of law.

Security Safeguards. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

Openness. There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data custodian.

Individual Participation. An individual should have the right:

(a) to obtain from a data custodian confirmation of whether or not the data custodian has data relating to him;

(b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him;

(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

(d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

Accountability. A data custodian should be accountable for complying with measures that give effect to the principles stated above.17

The United States Privacy Protection Study Commission recognized that “[t]he real danger is the gradual erosion of individual liberties through the automation, integration and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.”18 The Internet has realized this prediction. Indeed, credit

card companies, financial institutions, and government agencies share or sell personal information unless the affected individuals take affirmative steps to demand that their records not be disclosed.  

**PRIVACY AND CONTEXTUAL INTEGRITY**

The reasons for keeping the system open to the public have to do with the health and well-being of our legal system, not for the benefit of consumer profiling or other commercial interests. The Constitution provides for jury trials not only to determine questions of fact, but also to make the community an integral part of the judicial system. Open court records similarly serve an important educational function: not to titillate the masses with news of their neighbors’ misfortunes, but to support a functioning democracy. Government records empower citizens to make good political decisions. Court records publish final judgments and liens, facilitating business, and personal and legal affairs.

The legal system is not about the litigants but about self-government. It is tempting to think that the American court system revolves around the litigants, i.e., the plaintiff and defendant. To the contrary, the jury trial right guaranteed by the Seventh Amendment (civil trials) forms an important part of the American system of self-government.

The core interest underlying the American judicial system is not the interest of the parties, but of the citizens - the jurors and the gallery - who monitor the judges, the witnesses, the prosecutors, the police and the lawyers. Open public trials give the public an opportunity to deter corruption in the system. As de Tocqueville observed,

> The institution of the jury ... places the real direction of society in the hands of the governed ..... and not in that of the government..... [It] invests the people, or that class of citizens, with the direction of society.

> ... The jury system as it is understood in America appears to me to be as direct and as extreme a consequence of the sovereignty of the people as

---


20. See Globe Newspaper Co. v. Superior Court of Norfolk, 457 U.S. 596, 606 (1982) (“[T]he right of access to criminal trials plays a particularly significant role in the functioning of the judicial process and the government as a whole. Public scrutiny of a criminal trial enhances the quality and safeguards the integrity of the factfinding process, with benefits to both the defendant and to society as a whole.”); Neb. Press Ass’n v. Stuart, 427 U.S. 539, 587 (1976) (“[F]ree and robust reporting, criticism, and debate can contribute to public understanding of the rule of law and to comprehension of the functioning of the entire criminal justice system, as well as improve the quality of that system by subjecting it to the cleansing effects of exposure and public accountability.”).


24. See Edith Guild Henderson, *The Background of the Seventh Amendment*, 80 HARV. L. REV. 289, 295 (1966) (stating that the Seventh Amendment concerning jury trials in civil cases was a principal Antifederalist demand); Charles W. Wolfram, *The Constitutional History of the Seventh Amendment*, 57 MINN. L. REV. 639, 667-669, 678 (1973) (explaining that the Seventh Amendment was a reaction to the powerful government established by the Constitution, and antifederalists sought to protect debtors and litigants from oppressive judges).
universal suffrage. They are two instruments of equal power, which contribute to
the supremacy of the majority.25

For this reason, African-Americans and women have struggled for the right to serve on juries,
not for the benefit of the parties, but for the sake of being part of the system.26 The infusion of
these groups’ knowledge into the system also serves the overarching social purpose of protecting
the innocent from erroneous verdicts of liability.27

If litigants, jurors, and witnesses lose control over confidential information about themselves,
they will similarly adopt privacy-protective behaviors, most likely by refusing to participate in
the justice system. This raises a significant risk to public confidence in the court system and to
our functioning democracy.

Courthouse data generates profits for data aggregators, while potentially harming individuals.
Civil cases are filed because litigants have failed to reach a private compromise. This fact does
not transform the litigants’ pleadings, or evidence submitted with motion practice, into a
commodity that should be public for any and all purposes. Inaccuracies spawn statistics and
perceptions that are incorrect.

The judiciary has been wary of discovery abuse for commercial gain (or competitive advantage),
and its concerns should extend to other aspects of administering justice.28 Unhindered access
to case files may result in a further increase in identity theft. Marketers may take advantage of
compiled records to target advertising at former litigants and witnesses. Personal information
that is disclosed for the purposes of litigation could unfairly stigmatize a litigant in his or her
future pursuit of employment or educational opportunities.29

Litigants do not give up their privacy rights simply because they have walked,
voluntarily or involuntarily, through the courthouse door. . . . The mere payment
of a filing fee entitles a plaintiff to compel production of intensely personal and
confidential information, such as medical records, marital information, religious
documents, financial records, and even trade secrets or intellectual property. The
defendant, of course, can respond in kind. The loss of privacy through litigation
is compounded when the information is disclosed to the media, competitors,
political adversaries, and even curious members of the public.30

25. ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA 293-94 (1945); see also Gannett, 443 U.S. at 428-29
(Blackmun, J., concurring and dissenting) (finding that the public should be educated about the manner in which
criminal justice is administered); Detroit Free Press v. Ashcroft, 303 F.3d 681, 683 (6th Cir. 2002) (“Democracies
die behind closed doors.”).


28. Security is also an important aspect of electronic access to court files, as electronic files can be hacked,
modified, stolen and misused. See Michael Whiteman, Appellate Court Briefs on the Web: Electronic Dynamos or
Legal Quagmire?, 97 L. LIBR. J. 467, 476-78 (2005) (discussing various privacy concerns related to electronic
filing).

29. See Illinois v. Rodriguez, 497 U.S. 177, 181-82 (1990) (showing that the fact that information has been
disclosed to one individual does not mean that it can be freely disclosed to another – a guest in somebody’s home
cannot open the door to the police to conduct a search).

Just because a piece of information is in a “public record” does not mean it can be published for any purpose. The U.S. Supreme Court explained this at length in *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*. \(^{31}\) “[There is a] privacy interest inherent in the nondisclosure of certain information even where the information may have been at one time public.”\(^{32}\) One need not maintain perfect secrecy in order to maintain a degree of confidentiality. “[T]he fact that an event is not wholly ‘private’ does not mean that an individual has no interest in limiting disclosure or dissemination of the information.”\(^{33}\)

Release of information on computer tape in many instances is far more revealing than release of hard copies, and offers the potential for far more intrusive inspections. Unlike paper records, computerized records can be rapidly retrieved, searched, and reassembled in novel and unique ways, not previously imagined. For example, doctors can search for medical-malpractice claims to avoid treating litigious patients; employers can search for workers-compensation claims to avoid hiring those who have previously filed such claims; and credit companies can search for outstanding judgments and other financial data. Thus, the form in which information is disseminated can be a factor in the use of and access to records.\(^{34}\)

The inherent difficulty of obtaining and distributing paper files used to effectively insulate individuals from the harm that could result from misuse of information in government records. The Court referred to the relative difficulty of gathering paper files as “practical obscurity,” and recognized that it influenced the privacy equation.\(^{35}\) “Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a [government-created] computerized summary located in a single clearinghouse of information.”\(^{36}\)

It is overly simplistic to say that “public records are public records.” As discussed above, court records are not public because of any inherent characteristics; they are public for reasons that have to do with our system of self-government. Moreover, electronic records have attributes that fundamentally change the premises for categorizing information as “public.” The judiciary should resist the temptation to rely on oversimplified arguments that once a document can be found in the public domain it can no longer be considered private.\(^{37}\) Instead, the courts should consider afresh the reasons for making court records public and draw a distinction among the kinds of documents that should be made available online.

It is incorrect to assume there is a category of information about people that is “up for grabs,” to be used by anyone for any person. Philosopher and privacy scholar Helen Nissenbaum calls this the problem of “privacy in public.”\(^{38}\) For example, a woman was raped and badly beaten in New

---


\(^{32}\) *Id.* at 767.

\(^{33}\) *Id.* at 770.


\(^{35}\) *Id.* at 762.

\(^{36}\) *Id.* at 764.

\(^{37}\) The government may not impose sanctions for publishing information the government itself has already placed in the public domain, but it has no affirmative obligation to publish personally identifiable information about citizens. *See supra* notes 104-09 and accompanying text.

York’s Central Park in 1989. The case became famous as a racially charged example of prosecutorial misconduct.\(^{39}\) Even though the rape occurred in a public place, and the trials of the accused rapists were public events, the victim maintained a measure of privacy as to her identity.\(^{40}\) Even in more mundane situations, moreover, there does exist a right to maintain a measure of confidentiality in public. As Nissenbaum points out, for example, it is within one’s rights to say “none of your business” to a stranger who asks your name, even in a public square or sidewalk.\(^{41}\)

**BALANCING PUBLIC ACCESS AND PRIVACY**

The courts must notify individuals that their personal information may be disclosed to the public. They should put the public on notice that their personal information in government records may be disclosed. Many people are unaware that their personal information may become public when they make disclosures for the purpose of doing business with state and local government agencies.\(^{42}\)

There is a public interest in privacy applies with respect to courthouse records. It is entirely possible to serve the interests of open government and, at the same time, safeguard the public interest in individual privacy with respect to courthouse records.

The courts should redact from online records all Social Security numbers and other personal information that could facilitate identity theft or financial fraud. This is consistent with the Supreme Court’s decision in *United States Dep’t of Justice v. Reporters Committee for Freedom of the Press*. “[W]e hold as a categorical matter that a third party’s request for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen’s privacy, and that when the request seeks no ‘official information’ about a Government agency, but merely records that the Government happens to be storing, the invasion of privacy is ‘unwarranted.’”\(^{43}\)

No benefit accrues to individuals who are forced to disclose information about themselves as a result of being haled into court. Litigants, jurors, and witnesses should be entitled to a measure of protection, instead of having their personal information mined for the commercial benefit of enterprises with which the individuals have no relationship.

The courts may constitutionally require that businesses be explicit about what they intend to do with the personal information they obtain from the judicial branch. In *Los Angeles Police Department v. United Reporting Publishing Corp.*, for example, the Supreme Court upheld a statute that limited commercial access to arrest records.\(^{44}\) The statute permitted public access for

---


scholarly, journalistic, political, or governmental purposes.\(^{45}\) The Court concluded that the government may selectively grant access to public record information.\(^{46}\) In *Seattle Times v. Rhinehart*, the Court stated that the government may condition the receipt of discovery information on nondisclosure.\(^{47}\) Criminal records that merit special protection include presentence reports, plea agreements, unexecuted warrants, and pre-indictment documents.

The judiciary must adopt state-of-the-art security measures to prevent hackers and information brokers (including the judiciary’s own outsourcing contractors) from culling sensitive information from its electronic files.

Rules of Court should be amended to account for privacy and security. The courts must put litigants, witnesses, and jurors on notice that personal information about them may be sold and/or published worldwide on the Internet. The rules should establish liability and consequences for releasing restricted information, as well as remedies for providing erroneous or incomplete information derived from court records.\(^{48}\)

Privacy protection should extend to persons, not corporations.\(^{49}\) To a limited extent, anonymity is already permitted: grand jury secrecy protects the interests of an innocent accused,\(^{50}\) and some litigants (such as rape victims and minors) are permitted to use their initials only.\(^{51}\) The principles that protect the privacy interests of individuals who must participate in the court system should extend to electronic court records.

Court records should not be sold to generate revenue for the judicial branch. In this country, personally identifiable information is treated as a commodity, and the data-mining industry generates substantial revenues.\(^{52}\) The judiciary could easily sell court records for profit to companies that collect information to do background checks and the like. This would be highly inappropriate. The courts are created to serve the entire population of the state. Their costs should not be borne exclusively by litigants, witnesses, and others who have involuntarily come into contact with the justice system.

**CONCLUSION**

Personal information about individuals is a valuable commodity in the United States, where large commercial data aggregation companies sell Social Security numbers\(^ {53}\) and create consumer

\(^{45}\) Id. at 35.

\(^{46}\) Id. at 41.

\(^{47}\) Id.

\(^{48}\) The rules should also provide remedies and consequences for improperly withholding public information.

\(^{49}\) Federal Communications Commission v. AT&T Inc., No. 09-1279 (U.S. Mar. 1, 2011)

\(^{50}\) See, e.g., Douglas Oil v. Petrol Stops Nw., 441 U.S. 211, 219 (1979).


profiles for profit. Companies like ChoicePoint, Acxiom and Reed Elsevier work very hard to extract personal information about people from court records.

Meanwhile, much information about the judicial system itself remains secret. For example, the courts operate with public money, but decisions as to the allocation of budget monies are made in secret. These decisions affect the public, but the public is not informed as to how or why they are made. State courts offer many programs affecting the operation of the judicial system, such as mediation, arbitration, child custody, and pretrial intervention. “All of these programs cost time and money, and affect court personnel, litigants, lawyers and the public.” They are adopted in a process that is not publicized. Thus, individuals are exposed to scrutiny, while much of the system itself remains secret.

This makes the courts and other state actors the guardians of a “public interest in privacy.” The government has a duty to protect its citizens from incursions upon their privacy interests. Instead, however, the distinction between governmental and commercial interests is fading. Government records are being used to build commercial databases, and governments are purchasing commercial databases, apparently for the purpose of building dossiers on citizens.

The greatest threat to privacy comes from government in secret. The best way to protect individual privacy is to make the government accountable to its citizens, by making court records opened the public, while protecting the confidential personal information of individuals.

55. See Electronic Privacy Information Center, ChoicePoint, http://www.epic.org/privacy/choicepoint/ (last visited Jan. 29, 2006) (listing ChoicePoint as a company that sells information and listing Reed Elsevier as a “private sector data seller” along with ChoicePoint, Experian, Polk, Seisint and Acxiom).
57. See, e.g., id. at 39 (discussing New Jersey).
58. Although Judge Haines argues that all of the programs are adopted in a process involving extensive unwritten reports, the author disagrees with this statement and believes instead that many, but not all programs are adopted in such a way. See id.
The presenters for this program are privacy advocates and experts on public access to government records:

**Grayson Barber**, the lead author of this article, is a privacy advocate with a law office in Princeton, New Jersey. She serves on the advisory board of the Electronic Privacy Information Center and works as a volunteer attorney for the American Civil Liberties Union. Grayson advises the Intellectual Freedom subcommittee of the New Jersey Library Association, and chairs the Individual Rights Section of the New Jersey State Bar Association. She served on the New Jersey Privacy Study Commission and the state Supreme Court Special Committee on Public Access to Court Records. A graduate of Rutgers Law School in Newark, Grayson clerked for the Honorable Robert E. Cowen, U.S. Court of Appeals for the Third Circuit.

**Lillie Coney** is the Associate Director of the Electronic Privacy Information Center (EPIC). EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. Ms. Coney identifies emerging privacy issues, manages EPIC’s Privacy Coalition and outreach to civil society organizations in the US and around the world. She is a member of the Election Assistance Commission's Board of Advisors. She is the 2011 Co-chair of the Computers Freedom and Privacy Conference to be held at the Georgetown Law Center in Washington DC on June 14-16.

**Helen Nissenbaum** is Professor of Media, Culture and Communication, and Computer Science and Senior Fellow of the Information Law Institute at New York University. She is the author of *Privacy in Context* (Stanford Law Books), and has written widely on the issue of privacy in public.

**Stephen Schultze** is Associate Director of the Center for Information Technology Policy at Princeton University. His work at CITP includes internet privacy, security, government transparency, telecommunications policy, and more. He is part of the team that built RECAP, a free tool for sharing court records. He holds degrees in Computer Science, Philosophy, and Media Studies from Calvin College and MIT. He has also been a Fellow at the Berkman Center for Internet & Society at Harvard, and helped start the Public Radio Exchange.