ELECTRONIC PRIVACY INFORMATION CENTER

[BY EMAIL publicaccesscomments@pacourts.us]

November 17, 2005

David S. Price
Chair, Public Access Ad Hoc Committee
Administrative Office of Pennsylvania Courts
5035 Ritter Road, Suite 700
Mechanicsburg, PA 17055

Re: Comments on Privacy and Access to Court Records

Dear Mr. Price:

Thank you for soliciting public comment on privacy and court records. The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

EPIC occupies a unique space in this debate because the organization both advocates for the right of privacy and pursues access to government records under the Freedom of Information Act. EPIC is one of two judicially-recognized entities with "news media" status under the Freedom of Information Act.[1] EPIC is a strong supporter of access to government information. At the same time, the presence of personal information within public records raises serious privacy issues.

We wish to emphasize that the very purpose of public records—the ability of the individual to learn about the government—is turned on its head when the records include excessive personal information. Instead of being citizens' window into government activities, public records are giving the government, law enforcement, and data brokers a window into our

[1] *Elec. Privacy Info. Ctr. v. DOD*, 241 F. Supp. 2d 5 (D.D.C. 2003).

daily lives. Without privacy protections, court and other public records will be commodified for commercial purposes unrelated to government oversight.

General Comments

Public Records Present Both Benefits and Risks.

Reconciling the public access and privacy interests associated with access to case records involves complex and important issues.[2] Public access to court records brings both benefits and risks to the public. Greater public access into the workings of the court system will provide citizens with tools to evaluate the court system. This increased accessibility will foster greater confidence in government and the courts. Promotion of public access to court records will provide more opportunities for scholars, journalists, and researchers to provide insight into the nature of government. Courts will also benefit from the improved efficiency that electronic access to court records offers.

Our nation's approach to access to public records evolved at a time when there were no computers or information brokers. Further, as the Congressionally-created 1977 Privacy Protection Study Commission recognized, public records were not rich with information when our country formulated policies to address access: "The records of a hundred years ago tell little about the average American, except when he died, perhaps when and where he was born, and if he owned land, how he got his title to it."[3]

As a strong advocate of open government, EPIC supports the right of public access to judicial records found in common law. In *Nixon v. Warner Communications, Inc.*, the Supreme Court noted that, "It is clear that the courts of this country recognize a general right to inspect

[2] EPIC maintains a comprehensive resource on privacy and public records online at http://www.epic.org/privacy/publicrecords/.
[3] *Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission* (1977).

and copy public records and documents, including judicial records and documents."[4] It is essential to recognize at the outset of this process that individuals possess this right in order to monitor public agencies and to inquire into the operation of government.[5] This is a right that empowers individuals against a government that might attempt to obfuscate its operations through secrecy.

This right of access should not be confused with arguments by data aggregators and profilers who use public records to build dossiers on individuals. The building of dossiers based on court and other public records amounts to the creation of an "unauthorized biography" on all Americans that can be used by government and the private sector alike for the classification of individuals' behaviors. These unauthorized biographies can be inaccurate, expose individuals to risks, and be used to justify adverse employment decisions.[6]

Similarly, the Committee should not be persuaded by data brokers' arguments that information should be released in order to maintain an accurate credit reporting system. It is not the role of government to collect information from citizens, who are often under legal compulsion to provide their data, and then release the personal information to the private sector for the purpose of compiling dossiers. It is not the duty of government to facilitate credit reporting. Under the federal Fair Credit Reporting Act, credit reporting agencies are the parties responsible for maintaining practices that guarantee "maximum possible accuracy." The courts are under no duty to perform any function on behalf of credit reporting agencies and data brokers.

---

[4] 435 U.S. 589, 597 (1978).
[5] *Id*. at 598.
[6] *Firms Dig Deep Into Workers' Pasts Amid Post-Sept. 11 Security Anxiety*, Wall Street Journal, Mar. 12, 2002, at 1; *FBI's Reliance on the Private Sector Has Raised Some Privacy Concerns; Big Brother isn't gone. He's just been outsourced*, Wall Street Journal, Apr. 13, 2001 at 1.

Summary of Privacy Risks Raised by Public Records

Identity Theft and Stalking.

Personal data is the lifeblood of two growing crimes—identity theft and stalking. It is possible to obtain credit using another's identity through information that is available in public records. Bankruptcy records, for instance, provide all the keys that an identity thief needs to take advantage of persons who have already experienced financial difficulty. Often, victims are unaware that the crime occurred until many months after an impostor steals their identity. Victims typically expend considerable time and expense to regain their credit rating and to clear any criminal record that the impostor may have accumulated while posing as the victim.[7]

Social Forgiveness.

Data that finds its way into private sector information brokers may never be erased, even if the data subject has a record expunged. As Vance Packard points out in the *Naked Society* (1964), the contravenes our society's "right to hope for tolerant forgiveness or overlooking of past foolishnesses, errors, humiliations, or minor sins--in short, the Christian notion of the possibility of redemption."

Predatory Exploitation of Personal Information.

Some businesses (credit repair, and even "privacy protection" businesses) deliberately target individuals appearing in court filings in order to take advantage of them. For instance, one company operated a type of 21st Century extortion where individuals could opt-out of the sale of their personal information from public records for a $15 fee.

[7] Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solution, Prepared Testimony before the Senate Subcommittee on Technology, Terrorism, and Government Information, 106th Cong. (2000) (statement of Beth Givens, Director, Privacy Rights Clearinghouse), at http://www.privacyrights.org/ar/id_theft.htm; excellent resources on identity theft for policymakers and victims are posted on the Privacy Rights Clearinghouse Web Site at: http://www.privacyrights.org/identity.htm.

Ubiquitous Data Marketing.

Data aggregators and marketers may take advantage of compiled records to target advertising at former litigants and witnesses. In many cases, this targeted advertising may serve as a reminder of incidents best forgotten.

Government Use of Personal Information.

Increasingly, information from public records is being sold by private companies (ChoicePoint / LexisNexis) back to the government for law enforcement purposes.[8] This alters the balance of power among individuals, the government, and the private sector. The 1977 Privacy Protection Study Commission warned President Carter that information policy should change to avoid unfair power relationships. It recognized that the records of the day "mediate relationships between individuals and organizations and thus affect an individual more easily, more broadly, and often more unfairly than was possible in the past."[9] It recognized that information empowers the organization over the individual, and that as a society, we need to address that balance of power:

> In a larger context, Americans must also be concerned about the long-term effect record-keeping practices can have not only on relationships between individuals and organizations, but also on the balance of power between government and the rest of society. Accumulations of information about individuals tend to enhance authority by making it easier for authority to reach individuals directly. Thus, growth in society's record-keeping capability poses the risk that existing power balances will be upset.[10]

States that allow broad access to public records are supplying troves of data to law enforcement. For instance, ChoicePoint, a company that sells personal information to law enforcement, includes thirty-six extra databases on Florida residents and seven extra on

[8] See, e.g., *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement*, 29 UNIVERSITY OF NORTH CAROLINA JOURNAL OF INTERNATIONAL LAW & COMMERCIAL REGULATION 595 (Summer 2004).
[9] See supra footnote 3.
[10] See supra footnote 3.

Texans.[11] Access to information on Florida residents is particularly broad. It includes marriage records, beverage licensees, concealed weapons permits, day care licensees, handicapped parking permits, "sweepstakes," worker compensation, medical malpractice, and salt water product licensees.[12] This graphic shows the information made available to federal law enforcement, apparently from public records, by ChoicePoint.[13]

Broward Cty FL Warrants	$2.00
Broward Cty FL Traffic Citations	$2.00
FL Accidents	$2.00
FL Attorneys	$2.00
FL Banking Licenses	$2.00
FL Beverage Licenses	$2.00
FL Boat Registrations	$2.00
FL Boating Citations	$2.00
FL Closed Claims	$2.00
FL Concealed Weapons	$2.00
FL Condos and Co-ops	$2.00
FL Convicted Felony Offenders	$2.00
FL Day Care Licenses	$2.00
FL Department of Education	$2.00
FL Divorces	$2.00
FL Driver Licenses	$2.00
FL Handicapped Parking Permits	$2.00
FL Hotel and Restaurant Licenses	$2.00
FL Insurance Agents	$2.00
FL Lab Licenses	$2.00
FL Marriages	$2.00
FL Money Transmitters	$2.00
FL Notary Licenses	$2.00
FL Nursing Licenses	$2.00
FL Real Estate Licenses	$2.00
FL Salt Water Product Licenses	$2.00
FL Securities Dealers	$2.00
FL Sexual Predators	$2.00
FL Sweepstakes	$2.00
FL Tangible Property	$2.00
FL Tobacco Licenses	$2.00
FL Unclaimed Property	$2.00
FL Vehicle Registrations	$2.00
FL Worker Compensation	$2.00
FL Real Property	$2.00
FL Medical Malpractice	$2.00
Miami-Dade Cty FL Warrants	$2.00
FL Statutes	$0.00
Telephone Listings	$2.00

h

[11] ChoicePoint, Pricing Schedule D (Apr. 11, 2002) (document obtained from the DEA), available at http://epic.org/privacy/choicepoint/cpdea7.3.02.pdf.
[12] *Id.*
[13] *Id.*

An additional concern is that companies hungry for personal information are creating state, federal, and international law that treats any information in a public record as exempt from all privacy law. This is a dangerous development, considering the amount of personal information that finds its way into court files. Soon, a defense to practices that are privacy invasive will be, "well, we didn't invade anyone's privacy because sometime in history, somewhere in the world, the information appeared in a public record."

Third-Party Interests.

Not all individuals involved in a lawsuit there on their own accord. Witnesses, children, jurors, and others can be drawn into a lawsuit and required to provide personal information into the public record.

Less Use of Courts/Voluntary Cooperation.

In *Greidinger v. Davis*, the 4th Circuit held that public disclosure of the SSN for voting registration—even with use restrictions on the information—was an impermissible burden on the right to vote.[14] Just as individuals may not want to register to vote in order to avoid revealing personal information, use of the courts may be chilled by individuals who do not want personal information in the public record.

Errors Have A Greater Effect.

Some public records contain errors, or may be construed incorrectly. For instance, in *Paul v. Davis*, police circulated flyers with an individual's picture and erroneous conviction for theft. Broader access to these files could increase the effect of errors.

[14] 782 F. Supp. 1106 (ED Va. 1992).

Sophistication of Litigants.

Some approaches rely upon clients' attorneys to redact or otherwise protect privacy. In a large number of cases, however, litigants appear *pro se* and may not understand the risks or approaches to protecting privacy.

Efficiency.

There is a risk that we develop a scheme that is too unwieldy for efficient operation of the courts. Whatever approach is taken, we have to ensure that clerks are treated fairly by the system, and that their duties are reasonable.

General Recommendations

Minimization Should be the Key Rule.

Minimization, that is, the a policy that discourages collection of personal information, should be a guiding principle. In following minimization principles, an entity collects the last amount of personal information necessary in order to perform a certain function. Minimization is highly effective at reducing privacy risks.

In the court record context, the first inquiry to make is whether the court actually needs the information that it collects. Sometimes, system changes make it unnecessary to collect certain identifiers, and they continue to be collected simply because they always have been. We encourage the Committee to perform an audit to determine whether sensitive identifiers must be collected.

Access and Use Limitations Should be Considered

The Committee should consider that use limitations may be appropriate to protect privacy. Under such a scheme, acceptable uses could be defined for public records that are consistent with the policy reasons for providing them to the public. One system worth visiting

was reviewed by the Supreme Court in *LAPD v. United Reporting*.[15] The statute reviewed in that case allowed the public access to the records for scholarly, journalistic, political, or governmental purposes.[16] Commercial resale of the information was restricted.

Specific Recommendations

Section 2.00 STATEMENT OF GENERAL POLICY

Subsection A specifies that the proposed policy covers all electronic case records. We urge you to expand protections to paper files as well.

The relevant privacy issue here is access to records—not access to electronic records. If electronic records are treated in a more restrictive fashion, it means that the average person will have reduced access to the information in those records. Practical obscurity does not provide enough protection anymore, because sophisticated data aggregators and others have the resources to visit the actual courthouse and scan paper records, which then are effectively made "electronic." Therefore, in order to protect the privacy of individuals before the court, there must be some means to protect paper records as well.

We acknowledge that it creates burdens upon court administrators to limit disclose of discrete personal information from within case files. However, those burdens can be shared in order to reach the goal of protecting personal information without unduly causing costs to the state. As noted above, adopting a policy of minimization operates as a first step in limiting the invasiveness of court records. As noted in the commentary on the proposed rule, courts can adopt a public/private file system, where certain identification information is collected by the court on a separate form that is not released to the general public (but is accessible by parties,

[15] 528 U.S. 32 (1999).
[16] Id. at 35.

law enforcement, another others with a legitimate, specific need to access it). We are encouraged that the Committee has recommended the creation of a sensitive data form.

The court could also place the burden on litigants to manually redact Social Security numbers and other sensitive information that appear on copies of records accessible to the public.

The Committee could recommend to combine these different approaches, and implement them over time. Even adopting a policy to address prospective records is better than taking no action at all to address paper records.

Finally, we urge the Committee to set a deadline to revisit the paper records issue. If unaddressed, paper records will make irrelevant the attempts to shield electronic records from misuse.

Subsection C prohibits courts or offices from adopting more restrictive access policies. We urge you not to preempt or supercede attempts to create more restrictive policies. Local courts may need to react quickly to a new problem caused by access to records. We have seen that generally, local institutions react first to privacy problems, and can address invasive practices before the problem arises to the attention of a larger political jurisdiction.

Section 3.00 ELECTRONIC CASE RECORD INFORMATION EXCLUDED FROM PUBLIC ACCESS

We applaud the Committee for limiting access to Social Security numbers, full dates of birth, specific home address information, and operator license numbers. These identifiers are used by the credit industry to identify and "authenticate" individuals who are applying for credit accounts. Their presence in public records raises the risk that this information fall into the hands of frausters.

In order to comprehensively cover account numbers, subsection (A)(10) should be broadened to cover account numbers generally, and PINs or passwords used to secure accounts.

It has become clear that individuals attempting to invade others' privacy not only obtain financial account numbers, but also may make a target of utilities accounts or telephone accounts. These accounts should be shielded from disclosure or partially redacted as well.

Section 3.10 REQUESTS FOR BULK DISTRIBUTION OF ELECTRONIC CASE RECORDS AND COMPILED INFORMATION FROM ELECTRONIC CASE RECORDS

Subsection A is permissive in allowing bulk access to personal information from case records for any purpose. Even a requestor intending to use the information to send fraudulent solicitations would be permitted access under the rules. Indeed, there is increasing evidence that lists of personal information obtained from companies or public records are being used to target individuals for scams. For instance, the Iowa Attorney General has initiated a probe of database seller "Walter Karl" for providing lists to scam artists.[17] The company sells databases that claim to include "impulsive buyers…primarily mature" and "highly impulsive consumers…sure to respond to all of your low-end offers."[18] More recently, the Wall Street Journal covered the story of an identity thief who located victims by acquiring lists of prison inmates.[19]

We suggest that a use limitation be in place for bulk records requests, limiting access to non-commercial purposes. We furthermore urge the Committee to apply some of the safeguards articulated in subsection B to all bulk records requests.

---

[17] Attorney General of Iowa, A.G. asks Court to Order List Broker to Respond to Telemarketing Fraud Probe State asks court to order list-broker "Walter Karl, Inc." to cooperate with consumer protection investigation of direct mail and telemarketing schemes, Mar. 3, 2005, available at http://www.state.ia.us/government/ag/latest_news/releases/mar_2005/Walter_Karl.html.

[18] Affidavit of Barbara Blake, Investigator, Office of the Attorney General of Iowa, Mar. 1, 2005, available at http://www.state.ia.us/government/ag/latest_news/releases/mar_2005/Walter%20Karl%20BBlake%20Affidavit%203-1-05.pdf.

[19] Andrea Coombes, *Identity Thieves Head Off to College*, Oct. 25, 2005, available at http://online.wsj.com/article/SB113019456857878139.html. See also David Lazarus, *Annuities Used as Come On*, San Francisco Chron., Oct. 26, 2005, available at http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2005/10/26/BUG3CFDSU11.DTL (marketers buy lists to target customers for grey-market schemes); Adam Smith, Ruining My Credit Was Easy, Thief Says, St. Petersburg Times, Oct. 23, 2005, available at http://www.sptimes.com/2005/10/23/Worldandnation/Ruining_my_credit_was.shtml (identity thieves use list of consumers with good credit to target victims).

Subsection B allows bulk access to a broader set of personal information, as long as safeguards are in place to prevent certain misuse of the data. We propose the addition of the following language:

> 3.(d) the data will not be combined with other information sources or processes that serve to identify the individuals in the database.

This provision is necessary to prevent the practice of "reidentification." In reidentification, sophisticated techniques are used to discover the identities of individuals in a previously anonymous data set.

Carnegie Mellon Professor Latanya Sweeney has demonstrated that anonymous data sets can often be readily reidentified. In one experiment, Sweeney, using 1990 Census data, demonstrated that individuals often have demographic values that occur infrequently. Since these values occur infrequently, they allow the re-identification of individuals in putatively anonymous datasets. Sweeney found in her report *Uniqueness of Simple Demographics in the U.S. Population*:

> ...87% (216 million of 248 million) of the population in the United States had reported characteristics that likely made them unique based only on {5-digit ZIP, gender, date of birth}. About half of the U.S. population (132 million of 248 million or 53%) are likely to be uniquely identified by only {place, gender, date of birth}, where place is basically the city, town, or municipality in which the person resides. And even at the county level, {county, gender, date of birth} are likely to uniquely identify 18% of the U.S. population. In general, few characteristics are needed to uniquely identify a person.

SECTION 6.00 CORRECTING DATA ERRORS

While the proposed policy devotes a specific process for access to bulk records, no such process is specified for individuals facing the challenge of correcting erroneous public records. Identity theft expert Beth Givens has identified "wrongful criminal records" as a growing

problem for identity theft victims.[20] This occurs where an identity thief is arrested and supplies identity documents of another person to the police.

There should be processes specified for individuals can clear their records of erroneous information. The process should be simple enough that individuals can clear their records without the expense of hiring an attorney. We recommend that the Court make available a guide for individuals that articulates the steps to clear errors in their records.

Respectfully submitted,

/s

Chris Jay Hoofnagle
Senior Counsel
Electronic Privacy Information Center West Coast Office
944 Market St. #709
San Francisco, CA 94102
415-981-6400

[20] Beth Givens, Identity Theft: The Growing Problem of Wrongful Criminal Records, Jun. 1, 2000, available at http://www.privacyrights.org/ar/wcr.htm.