

ELECTRONIC PRIVACY INFORMATION CENTER

November 1, 2004

Committee on Privacy and Court Records
Supreme Court of Florida
500 South Duval Street
Tallahassee, FL 32399-1900

To The Committee on Privacy and Court Records:

Introduction

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

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

Florida Residents Are At Heightened Privacy Risk

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 Texans.² 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.³ This graphic shows the information made available to federal law enforcement, apparently from public records, by ChoicePoint.⁴

Broward Cty FL Warrants	\$2.00
Broward Cty FL Traffic Citations	\$2.00
FL Accidents	\$2.00
FL Attorneys	\$2.00
FL Banking Licensees	\$2.00
FL Beverage Licensees	\$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 Licensees	\$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 Licensees	\$2.00
FL Insurance Agents	\$2.00
FL Lab Licensees	\$2.00
FL Marriages	\$2.00
FL Money Transmitters	\$2.00
FL Notary Licensees	\$2.00
FL Nursing Licensees	\$2.00
FL Real Estate Licensees	\$2.00
FL Salt Water Product Licensees	\$2.00
FL Securities Dealers	\$2.00
FL Sexual Predators	\$2.00
FL Sweepstakes	\$2.00
FL Tangible Property	\$2.00
FL Tobacco Licensees	\$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

² ChoicePoint, Pricing Schedule D (Apr. 11, 2002) (document obtained from the DEA), available at <http://epic.org/privacy/choicepoint/cpdea7.3.02.pdf> [hereinafter Pricing Schedule D].

³ *Id.*

⁴ *Id.*

Personal information from government records not only flows to law enforcement easily, it is also sold to direct marketers. Here are four driver's marketing databases available on Floridians that do not exist in any other state. Note that the source for this data is not self-reported, rather, it they come from government records. All four are reproduced from the February 2003 SRDS Direct Marketing List Source, a two-volume compilation of marketing lists for sale. This type of data marketing drives unwanted telemarketing and junk mail.

FLORIDA MOTORCYCLISTS
 Data Verified: Dec 26, 2002.
 Location ID: 10 DCLS 508 Mid 732214-000
 SmartTarget Marketing, 725 Broad Street, Augusta, GA 30901. Toll Free 800-329-5478, Fax 706-823-3471.
 E-mail: contact@smarttarget.com

1. PERSONNEL
 Gen Mgr—Tim Killebrew
 Natl Sales Mgr—Arthur bud Henderson
 Operations Manager—Debby Goolsby

2. SUMMARY DESCRIPTION
 Motorcycles registered to individuals in the state of Florida.

3. LIST SOURCE
 Compiled government records.

4. SELECTIONS WITH COUNTS
 Updated: Dec 16, 2002.

	Total Number	Price per/M
Total list	181,139	65.00
Minimum order	5,000	

4A. OTHER SELECTIONS
 SCF, Zip, MSA, country, 5.00/M extra; age, 10.00/M extra; ethnicity, 15.00/M extra; manufacturer, 25.00/M extra; marital status, gender of owner, income, key coding, 5.00/M extra.

5. COMMISSION, CREDIT POLICY
 Cancel charges: Cancellation fee: 25% of total after receipt of purchase order up to shipping date, full fee is due after shipping date. Prepayment required for new customers. Credit terms may be arranged for subsequent orders upon approval of finance department.

6. METHOD OF ADDRESSING
 Cheshire labels, 4-up; diskette, 5.00 fee; e-mail, 30.00 fee; FTP or bulletin board, 30.00 fee; zip disk or cd, 25.00 fee; mag tape, data cartridge, 55.00 fee; pressure sensitive labels, 10.00/M extra; clear labels, 25.00/M extra; galley listing, 25.00 fee; 8 1/2 x 11 sheets laser printed, 50.00/M extra.

8. RESTRICTIONS
 Two sample mailing pieces required. One time use only. Unless prior arrangement has been made.

New Listing

FLORIDA'S EXOTIC AUTOMOBILES
 Data Verified: Jan 17, 2003.
 Location ID: 10 DCLS 508 Mid 770430-000
 Member: D.M.A.
 SmartTarget Marketing, 725 Broad Street, Augusta, GA 30901. Toll Free 800-329-5478, Fax 706-823-3471.
 E-mail: contact@smarttarget.com

1. PERSONNEL
 Operations Manager—Debby Goolsby

2. SUMMARY DESCRIPTION
 Database of exotic automobiles registered in the State of Florida.

3. LIST SOURCE
 Compiled public records.

4. SELECTIONS WITH COUNTS
 Updated: Dec 1, 2002.

	Total Number	Price per/M
Total list	157,701	85.00
Minimum order	5,000	

4A. OTHER SELECTIONS
 Gender, state, SCF, Zip, MSA, county, marital status, run charge, 5.00/M extra; Vehicle selections: antique vehicles, lender-financier, vehicle-leased, vehicle-manufacturer, vehicle-model, vehicle-type, vehicle-year purchased, 5.00/M extra; carrier route/mailstream sort, 8.00/M extra; age, 10.00/M extra; ethnicity, 15.00/M extra; telephone number, 25.00/M extra.

5. COMMISSION, CREDIT POLICY
 Cancel charges: Cancellation fee: 25% of total after receipt of purchase order up to shipping date. Full fee is due after ship date. Prepayment required for new customers. Credit terms may be arranged for subsequent orders upon approval of our Financial Department.

6. METHOD OF ADDRESSING
 Cheshire labels, 4-up; pressure sensitive labels, 10.00/M extra; mag tape, 55.00 fee; diskette, 5.00 fee; e-mail, 30.00 fee; CD, 10.00 fee; data cartridge, 25.00/M extra; Zip disk, 25.00/M extra; galley listing, 25.00/M extra; FTP, 30.00 fee; bulletin board, 30.00 fee; electronic delivery, 30.00 fee; 8 1/2 x 11 laser printed sheets, 0.85 fee.

8. RESTRICTIONS
 Sample mailing piece required. One time use only.

AUTO INSURANCE INDIVIDUALS OF FLORIDA
FLORIDA
 Data Verified: Dec 26, 2002.
 Location ID: 10 DCLS 508 Mid 736676-000
 SmartTarget Marketing, 725 Broad Street, Augusta, GA 30901. Toll Free 800-329-5478. Fax 706-823-3471.
 E-mail: contact@smarttarget.com

- PERSONNEL**
 Gen Mgr—Tim Killebrew
 Natl Sales Mgr—Arthur bud Henderson
 Operations Manager—Debby Goolsby
- SUMMARY DESCRIPTION**
 Vehicles registered to individuals in the state of Florida.
- LIST SOURCE**
 Controlled circ government records.
- SELECTIONS WITH COUNTS**
 Updated: Dec 16, 2002.

	Total Number	Price per/M
Total file	8,659,982	55.00
Minimum order	5,000	

- OTHER SELECTIONS**
 Zip, SCF, gender, year purchased, income, insurance company by name, finance company, 5.00/M extra; ethnic (Jewish/Hispanic), 10.00/M extra; vehicle types: motorcycles, antique vehicles, suv, recreational vehicles, mobile homes, vehicle selects: brand, model, model year, year purchased, leased vehicles, carrier route sort, 5.00/M extra; key coding, 2.00/M extra.
- COMMISSION, CREDIT POLICY**
 Cancel charges: Cancellation fees: 25% of total after receipt of purchase order up to shipping date. Full fee is due after shipping date. Prepayment required for new customers. Credit terms may be arranged for subsequent orders upon approval of finance department.
- METHOD OF ADDRESSING**
 Cheshire labels, 4-up; diskette, 5.00 fee; modem, 45.00 fee; e-mail, 25.00 fee; FTP or bulletin board, 25.00 fee; zip disk or cd, 25.00 fee; mag tape, 25.00 fee; pressure sensitive labels, 10.00/M extra; clear labels, 25.00/M extra; galley listing, 25.00 fee; 8 1/2 x 11 sheets laser printed, 50.00/M extra.
- RESTRICTIONS**
 Two sample mailing pieces required. One time use only. Unless prior arrangement has been made.
- MAINTENANCE**
 December, 2000.

New Listing
SUV OWNERS OF FLORIDA
 Data Verified: Jan 17, 2003.
 Location ID: 10 DCLS 508 Mid 770431-000
 Member: D.M.A.
 SmartTarget Marketing, 725 Broad Street, Augusta, GA 30901. Toll Free 800-329-5478. Fax 706-823-3471.
 E-mail: contact@smarttarget.com

- PERSONNEL**
 Operations Manager—Debby Goolsby
- SUMMARY DESCRIPTION**
 Owners of SUVs registered in the State of Florida.
- LIST SOURCE**
 Compiled public records.
- SELECTIONS WITH COUNTS**
 Updated: Dec 1, 2002.

	Total Number	Price per/M
Total list	900,183	75.00
Minimum order	5,000	

- OTHER SELECTIONS**
 Gender, state, SCF, Zip, MSA, county, income, marital status, run charge, 5.00/M extra; Vehicle selections; lender-financier, vehicle-leased, vehicle-manufacturer, vehicle-model, vehicle-type, vehicle-model year, vehicle-year purchased, 5.00/M extra; carrier route/mailstream sort, 8.00/M extra; age, 10.00/M extra; ethnicity, 15.00/M extra; telephone number, 25.00/M extra.
- COMMISSION, CREDIT POLICY**
 Cancel charges: Cancellation fee: 25% of total after receipt of purchase order up to shipping date. Full fee is due after ship date. Prepayment required for new customers. Credit terms may be arranged for subsequent orders upon approval of our Financial Department.
- METHOD OF ADDRESSING**
 Cheshire labels, 4-up; pressure sensitive labels, 10.00/M extra; mag tape, 55.00 fee; diskette, 5.00 fee; e-mail, 30.00 fee; CD, 10.00 fee; data cartridge, 25.00/M extra; Zip disk, 25.00/M extra; galley listing, 25.00/M extra; FTP, 30.00 fee; bulletin board, 30.00 fee; electronic delivery, 30.00 fee; 8 1/2 x 11 laser printed sheets, 0.85 fee.
- RESTRICTIONS**
 Sample mailing piece required. One time use only.

Additional Resources

In addition to these comments, we submit two additional resources. The first, *Access and Aggregation*, explains that serious privacy threats are raised by government collection of personal information.⁵ It also clearly states the inherent problems and unfairness of current public records policy:

Imagine that the government had the power to compel individuals to reveal a vast amount of personal information about themselves - where they live, their phone numbers, their physical description, their photograph, their age, their medical problems, all of their legal transgressions throughout their lifetimes whether serious crimes or minor infractions...

⁵ Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 MINNESOTA LAW REVIEW 1137 (2002).

Then imagine that the government routinely poured this information into the public domain - by posting it on the Internet where it could be accessed from all over the world, by giving it away to any individual or company that asked for it, or even by providing entire databases of personal information upon request...

Imagine the ease with which this information could fall into the hands of crafty criminals, identity thieves, stalkers, and others who could use the information to threaten or intimidate individuals. Imagine also that this information would be available to those who make important decisions about an individual's life and career - such as whether the individual will get a loan or a job. Also imagine that in many cases, the individual might not be able to explain any concerns raised by this information or even know that such information was used in making these decisions.

Imagine as well that this information would be traded among hundreds of private-sector companies that would combine it with a host of other information such as one's hobbies, purchases, magazines, organizations, credit history, and so on. This expanded profile would then be sold back to the government in order to investigate and monitor individuals more efficiently.

Stop imagining. What I described is what is currently beginning to occur throughout the United States by the use of federal, state, and local public records, and the threat posed to privacy by public records is rapidly becoming worse.

The second is a paper by identity theft expert Beth Givens.⁶ She recommends that:

- Court systems only post indexes, registers, and calendars on the web rather than the full texts of court proceedings.
- Adopt information automation systems that support redaction features.
- Sensitive court files should not be posted in full.
- Fully consider the policy objectives served by adopting electronic dissemination. Sometimes the policy objective can be met by posting less information.
- Place regulations on the information brokerage industry.
- Fix loopholes in background check laws.
- Regulate the private investigator industry in states where they are not subject to licensure.
- Seek policies that encourage "social forgiveness," the principle that individuals should be forgiven by society for derogatory information in their dossiers.

⁶ Beth Givens, Public Records on the Internet: The Privacy Dilemma (n.d.).

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.⁷ 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 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."⁸

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 and copy public records and documents, including judicial records and documents."⁹ It is essential to recognize at the outset of this process that individuals possess this right in order to

⁷ EPIC maintains a comprehensive resource on privacy and public records online at <http://www.epic.org/privacy/publicrecords/>.

⁸ *Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission* (1977).
⁹ 435 U.S. 589, 597 (1978).

monitor public agencies and to inquire into the operation of government.¹⁰ 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.¹¹ These unauthorized biographies can be inaccurate, expose individuals to risks, and be used to justify adverse employment decisions.¹²

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.

The State Has Legal Authority to Protect Public Records

The US Supreme Court has recognized limits to the right of public access in order to address the risk to personal privacy that may occur from secondary, improper uses of personal

¹⁰ *Id.* at 598.

¹¹ See *supra* footnote 2.

¹² *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.

information. In *Nixon*, the Court qualified the general right in favor of access to judicial records, "It is uncontested, however, that the right to inspect and copy judicial records is not absolute. Every court has supervisory power over its own records and files, and access has been denied where court files might have become a vehicle for improper purposes. For example, the common-law right of inspection has bowed before the power of a court to insure that its records are not 'used to gratify private spite or promote public scandal' through the publication of 'the painful and sometimes disgusting details of a divorce case.'"¹³

In other decisions, the Court has recognized legitimate privacy interests that qualify a right to access public records and other records held by government. In *DOJ v. Reporters Committee for Freedom of the Press*, the Court denied access to criminal "rap" sheets, aggregate summaries of criminal histories compiled from multiple jurisdictions.¹⁴ The Court in that case found a privacy interest in information that was publicly accessible, but because it was stored in courthouses across the country, the information remained "practically obscure."¹⁵ In denying access to the rap sheets, the Court noted that, "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 computerized summary located in a single clearinghouse of information."¹⁶ The Court concluded, "Accordingly, we 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

¹³ *Nixon*, 435 U.S. at 598.

¹⁴ 489 U.S. 749 (1989).

¹⁵ *Id.*

¹⁶ *Id.* at 764.

seeks no 'official information' about a Government agency, but merely records that the Government happens to be storing, the invasion of privacy is 'unwarranted.'"¹⁷

In *Los Angeles Police Department v. United Reporting Publishing Corporation*, the Court denied a First Amendment challenge to a statute that limited commercial access to arrest records.¹⁸ The statute allowed the public access to the records for scholarly, journalistic, political, or governmental purposes.¹⁹ The company that challenged the law used arrest records to target advertising to recent arrestees, and argued that the statute unconstitutionally burdened commercial free speech rights. The Court held that the statute simply allowed the government to deny access to information that it possessed.²⁰

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.²¹

¹⁷ Id. at 780.

¹⁸ 528 U.S. 32 (1999).

¹⁹ Id. at 35.

²⁰ Id. at 40.

²¹ 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>.

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.

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 / Experian) back to the government for law enforcement purposes.²² 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."²³

²² 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).

²³ See *supra* footnote 5.

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.²⁴

One example of a system that alters the power relationship as a result of access to personal information is the MATRIX, the Multi-State Anti-Terrorism Information Exchange. MATRIX is a prototype database system run by the State of Florida and Seisint, a private company. Built by a consortium of state law enforcement agencies, MATRIX combines public records and private record data from multiple databases with data analysis tools. MATRIX is available to law enforcement agents in participating states, and provides a wealth of personal information in near-real time. The name of the MATRIX is deceptive, because it is not an anti-terrorism exchange. The database includes information on normal, law-abiding people, from public records. So little attention has been given to privacy risks that several of the original states participating in the program have withdrawn.

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

²⁴ See supra footnote 5.

information—was an impermissible burden on the right to vote.²⁵ 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.

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.

Specific Recommendations

Minimization is key to protecting privacy

First, we commend the Court for taking an approach that is first focused on reducing the amount of personal information collected by government. This practice, known as minimization, encourages entities to collect the minimum amount of information necessary to carry out a government function. Minimization is highly effective at reducing privacy risks.

Paper should be protected too

Second, we encourage the Committee to advise the Court to expand privacy protections beyond electronic records. Paper public records also present privacy problems. Paper records should receive the same protections that electronic records get. The relevant privacy issue here

²⁵ 782 F. Supp. 1106 (ED Va. 1992).

is access to records—not access to electronic records. If electronic records are treated in a more restrictive fashion, it only means that the average person will have reduced access to the information in those records. Sophisticated data aggregators and others have the resources to visit the actual courthouse and scan paper records, which then are effectively made "electronic."

Consider limitations on the use of personal information in public records

Third, the Committee should advise the Court 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*.²⁶ As noted above, in that case, the LAPD only released arrest information to the public for specific purposes, including law enforcement, research, and journalistic uses. Commercial resale of the information was restricted.

Reduce the appearance of unique identifiers

Last, we urge the Committee to pay particular attention to the minimization of unique identifiers. Unique identifiers make aggregation and secondary use of public records possible. Accordingly, wherever possible, the Committee should recommend against the collection or release of Social Security Numbers, addresses, phone numbers, and dates of birth.

Respectfully submitted,

/s

Chris Jay Hoofnagle
Associate Director
Electronic Privacy Information Center

²⁶ 528 U.S. 32 (1999).