05-AP- 005

05-BK- 012

05-CV- 030

05-CR- 016

ELECTRONIC PRIVACY INFORMATION CENTER

[Submitted Electronically at http://www.uscourts.gov/rules/]

February 15, 2006

Secretary of the Committee on Rules of Practice and Procedure
Administrative Office of the United States Courts
Washington, DC 20544

Re: Comments of EPIC concerning Proposed Rule 5.2 of the Federal Rules of Civil Procedure; Proposed Rule 49.1 of the Federal Rules of Criminal Procedure; Proposed Rule 9037 of the Federal Rules of Bankruptcy Procedure and Proposed Rule 25(a)(5) of the Federal Rules of Appellate Procedure.

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**

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

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

Court records are becoming the fodder for dossiers on Americans. Currently in Congress, lobbyists from data companies are attempting to place an exemption into privacy legislation that would free data companies from consumer protections, so long as the information they sell is present in a public record. This would mean that companies that traffic in sensitive personal information--including Social Security Numbers--would not have to abide by security safeguards or inform consumers if this information was stolen! The data brokers are banking on the courts to pour personal information into the public record so that it can be sold without privacy safeguards.

We wish to highlight five points to guide the Committee in its revisions of rules to protect personal information in public records:

Minimization is key to protecting privacy

First, we recommend that court systems generally approach privacy issues by first determining whether they need the personal information collected. Institutions should not collect personal information unless it is necessary for some legitimate purpose. 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 and Courthouse Access should be protected too

Second, the relevant issue here is not access to electronic records, but rather access to public 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." Commercial data brokers employ hundreds of stringers who hand-copy sensitive personal information out of paper public records.

We therefore encourage the Committee to revise rule 5.2(c). This section limits online reproduction of certain sensitive case files, but allows complete access from within the courthouse. This loophole will allow sophisticated data aggregators to collect sensitive health information and personal identifiers.

Consider limitations on the use of personal information in public records

Third, we urge the Committee to consider use limitations 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*.[2] 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

Fourth, 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. The Committee has recommended the partial redaction of Social Security Numbers, dates of birth, and account numbers. Because redaction policies are not consistent (some institutions redact the first five digits of the SSN, while others redact the last four), we recommend complete removal of the SSN from the file. Partial redaction allows sophisticated data companies to "reidentify," or reconstruct, full SSNs.

We furthermore recommend that home addresses, telephone numbers and mother's maiden names be redacted. These identifiers are being used by the credit industry to

[2] 528 U.S. 32 (1999).

"authenticate" individuals for new accounts, and therefore, their availability exposes individuals to identity theft.

Limit Bulk Downloads

Finally, we recommend that the Committee consider limitations on bulk downloads of documents from the PACER system. There is increasing evidence that lists of personal information obtained from companies and public records in bulk 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.[3] The company has used database technology to locate individuals who are "impulsive buyers...primarily mature" and "highly impulsive consumers...sure to respond to all of your low-end offers."[4] More recently, the Wall Street Journal covered the story of an identity thief who located victims by acquiring lists of prison inmates.[5] Bulk access should be allowed for legitimate journalistic, research, and academic purposes, but not for commercial solicitations or profiling.

Respectfully submitted,

/s

Chris Jay Hoofnagle
Electronic Privacy Information Center

---

[3] 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.

[4] 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.

[5] 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).