

# EXHIBIT B



## Public Works Projects for the Internet

**To:** The Honorable Lee H. Rosenthal, Chairman  
Judicial Conference Committee on Rules and Procedure

**Cc:** The Honorable Alex Kozinski, Chief Judge, Ninth Circuit  
The Honorable Edith H. Jones, Chief Judge, Fifth Circuit  
The Honorable Dennis Jacobs, Chief Judge, Second Circuit  
The Honorable J.L. Edmondson, Chief Judge, Eleventh Circuit  
The Honorable Karen J. Williams, Chief Judge, Fourth Circuit

**From:** Public.Resource.Org

**Date:** May 3, 2008

**Subj:** **Confidential - 1,718 Personal Identifiers Found in Appellate Opinions**

Examination of appellate decisions reveals 1,718 cases with Alien Numbers or Social Security Numbers published in the opinions. The issue applies across all circuits and many of the opinions in question are still available on court web sites. This memorandum explains the problem and suggests corrective actions to be taken.

### **Background: Personal Identifiers in Court Opinions**

The E-Government Act of 2002 and [Appellate Rule 25](#) “require that personal identification information be redacted from documents filed with the court.” While the focus of the Privacy Rules are on lawyers, requiring them to redact personal identification numbers from documents filed with the courts, there is also an obligation for the courts themselves to do their part, particularly when the appearance of personal identification materials in court opinions is the result of the opinion publication process or is inherent in the procedures established by the courts for submitting appeals.

In a recent [Memorandum Describing the Privacy Rules and Judicial Conference Privacy Policy](#) issued by the Rules Committee, special note was made of immigration and Social Security cases:

#### **Cases That Are Not Subject to the Redaction Requirement**

In addition, the new Civil Rules becoming effective on December 1, 2007, do not apply the redaction requirements to certain categories of cases that are exempted from remote public access. These categories are immigration cases and Social Security cases.

The parties have remote electronic access to filings in these cases, but the public has access to the filings only at the courthouse.

It is clear that Alien Numbers and Social Security Numbers are not meant to be made available for general public access as publication of these numbers poses a substantial and real threat of identity theft for the individuals involved.

### **Opinions Found Containing Personal Identifiers**

Public.Resource.Org is a 501(c)(3) nonprofit corporation dedicated to making public information more readily available on the Internet. As part of our mission, we recently obtained 50 years of Courts of Appeals decisions from a commercial vendor, reformatted this data to be compliant with modern Internet standards such as XML markup, SHA1-based document integrity checks, and explicit labels indicating the public domain status of the underlying data.

We then made this data available in bulk, and it is now being used by numerous for-profit and non-profit organizations providing access to the general public and legal professionals.

In April, we were notified by an individual that his Alien Number, the personal identifier used on the Green Card, had been published on the Internet. We investigated the issue and determined that the Immigration and Naturalization Service routinely used the Alien Number as the Docket Number for their cases, and this information is present in 1,499 published opinions, many of which are currently available on court web sites.

In addition, we scanned the corpus for Social Security Numbers and found those present in 219 published opinions. All told, 1,718 published opinions contain these personal identifiers. These opinions are distributed among all the circuits, as detailed in Table 1.

<b>Court</b>	<b>Number of Cases with Personal Identifiers in the Published Opinion</b>
Ninth Circuit	990
Fifth Circuit	171
Second Circuit	93
Eleventh Circuit	85
Fourth Circuit	81
Seventh Circuit	64
Eighth Circuit	54
Sixth Circuit	53
Third Circuit	42
Tenth Circuit	40
First Circuit	22
DC Circuit	16
Federal Circuit	6
Court of Claims	1

Table 1: Number of Cases by Circuit

**The Problem Is Ongoing**

Table 2 shows the number of opinions found over time. As can be seen from the continuing high volume of incidents, the problem is ongoing and not just historical.

Year	Number of Cases with Personal Identifiers in the Published Opinion
1949-1979	53
1980-1989	154
1990-1994	210
1995-1999	816
2000-2004	370
2005	60
2006	82
2007	26

Table 2: Number of Cases by Year

Appendix A contains a detailed listing of each case found. The table contains the citation in the National Reporter Series, any docket numbers found, the date (which in some cases is date submitted and in others is date filed), and indicators if the case contains an Alien Number or a Social Security Number and if the case appears to be accessible via the court's own web site.

We would be happy to make available additional information from our database of cases found, such as names of judges (or *en banc* status), URLs to access the pages, and the specific patterns and resulting matches.

It is important to note that these identification numbers are present in the opinions delivered by the courts, not just in briefs submitted by the appellants. In many cases, the summary information is embedded in the prefatory information generated by the courts. For example, take the case of [REDACTED]

[REDACTED] in the Court of Appeals for the Tenth Circuit:

[REDACTED]

As can be seen, dire [REDACTED] etitioner and Respondent, the docket number is followed by A73-[REDACTED] Alien Number:

[REDACTED]

## **Corrective Steps**

A series of specific actions have been mandated for all Executive Branch agencies in OMB Memorandum M-07-16, "[Safeguarding Against the Breach of Personally Identifiable Information](#)," where breach is defined as "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic." That policy goes on to state:

"Safeguarding personally identifiable information in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. ... this memorandum requires agencies to develop and implement a breach notification policy **within 120 days.**" [emphasis in original.]

Upon discovery of a breach of personal identifiers, a series of steps are considered Best Current Practices, both in industry and in government:

1. Mitigate the immediate damage by fixing the breach.
2. Notify upstream sources and downstream users of the data.
3. Investigate the cause and implement corrective steps to prevent reoccurrence.

Upon discovery of breach, Public.Resource.Org took the following steps:

1. We algorithmically scanned all court cases to find Alien Numbers and Social Security Numbers, then individually checked all numbers flagged. We then scrambled the identifiers, substituting random alphabetic characters for the numbers.
2. Bulk users of our data ("downstream users") were notified of the specific cases found. Per this memorandum, we are notifying the courts ("upstream sources").
3. We have implemented a policy of scanning all databases we post for personal identifiers, even if those databases are public records produced by the government. We have also implemented a policy which allows users to notify us if they discover information.

We believe the courts should take a similar set of steps:

1. Active steps should be taken to redact the personal identifiers, particularly the ones found on your web sites, as well as scanning for additional materials such as briefs containing this information.
2. Best Current Practices require the notification of affected parties of the breach. We believe it is incumbent on you to notify all of the individuals who were exposed. In addition you should notify your downstream users, particularly the major legal services such as West, Lexis, and AltLaw.
3. The presence of personal identifiers, particularly in immigration cases, is well known and documented as evidenced by Judicial Conference reports. An investigation as to why that did not translate into concrete actions by the courts and how to prevent further breaches is thus recommended.

We realize that mitigating this breach will require time and money, but this is essential to "ensure the government retains the trust of the American Public," a principle that applies equally to all three branches of our government.

Pages 5-38 of this document, which consisted of an Appendix listing redacted personal identifying information, have been removed from the Exhibit.