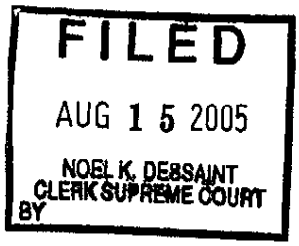
STAFF ATTORNEYS
COPY



Jennifer A. Greene, Policy Analyst
Court Services Division, AOC
Arizona Supreme Court
1501 W. Washington, Suite 410
Phoenix, AZ 85007-3231
(602) 542-9555

IN THE SUPREME COURT OF THE STATE OF ARIZONA

In the Matter of:	)	R-05-0018
AMENDMENT TO SUPREME	)	
COURT RULE 123, R.CIV.P. 5(f),	)	Supreme Court
and R.CRIM.P. 1.8	)	R. No. 2005-_____

Pursuant to Rule 28 of the Rules of the Supreme Court, Jennifer A. Greene, on behalf of the Rule 123 Workgroup, petitions the Supreme Court to approve an amendment to Supreme Court Rule 123, that will reduce the risk that court records may be used to commit identify theft while permitting law enforcement agencies to continue to provide the courts with defendants' social security numbers.

Emergency adoption of the amendment is requested to synchronize the proposed amendment with other changes to the rule that are scheduled to take effect December 1, 2005.

GROUNDS FOR APPROVAL OF PETITION
(emergency consideration requested)

On June 1, 2005, this Court approved changes requested by rule change petition number R-03-0012. The petition sought to reconcile the public's interests in

privacy and online access to court records. Before the petition was approved, a workgroup convened by the Supreme Court Staff Attorney's Office drafted modifications to resolve concerns expressed in comments received by the clerk's office. Among other things, the new rule requires that when parties need to submit sensitive data, such as Social Security Numbers and financial account numbers, to the court, they must do so on a separate "sensitive data form," and ensure that such data not appear on any other documents they file. The new rule also prohibits Internet publication of specified non-confidential case information such as parties' home addresses, and non-confidential case documents, such as pre-sentence reports, and party-filed records in domestic relations, juvenile, and probate matters.

One frequently-filed court record that was overlooked in the effort to make appropriate policy changes is the Arizona Traffic Ticket and Complaint form (ATTC), available as Appendix A to the Rules of Procedure in Traffic Cases and Boating Cases. Under the terms of A.R.S. §13-3903, this form must be used by law enforcement personnel for citing a defendant with a traffic, misdemeanor, or petty offense when the officer does not take the defendant into custody. Hundreds of different police and regulatory entities throughout the state of Arizona file thousands of these forms in lower jurisdiction courts every day.

A completed ATTC form displays, inter alia, the defendant's name, gender, home and business address, phone number, driver's license number, date of

birth, and social security number. This combination of personal data is essential to courts if identification and location of the defendant and enforcement of court imposed financial sanctions is later necessary, but the data also potentially offers enormous advantages for identity thieves if it is not properly protected.

Courts refer to the social security number appearing on the ATTC in drafting failure-to-appear warrants. The social security number on the ATTC is also used by courts for collection of delinquent court fines and penalties. For example, the statewide collection program that intercepts tax refunds and lottery winnings authorized by A.R.S. §42-1122, requires that courts provide the Department of Revenue with the defendant's name and social security number. The Traffic Ticket Enforcement and Assistance Program, authorized by A.R.S. §28-1631, requires that courts provide the Motor Vehicle Division with a defendant's name, date of birth, driver's license, and social security number. These important tools used to enforce court orders would no longer be available to local courts if citing agencies ceased to provide defendants' social security numbers on the ATTC form.

Under the new scheme for protecting sensitive data that becomes effective December 1st, police agencies will be required to file a separate sensitive data form with each citation, or not provide the social security number at all. Apart from the enormous training issues this new protocol will engender for police agencies, is the

unwelcome prospect of lower jurisdiction courts handling colossal amounts of extra paperwork for data entry to automated case management systems.

The attached proposal offers a practical approach to the problem. Under the proposed amendment, parties filing the ATTC form are exempted from the sensitive data form requirement (Civil Rule 5(f)(1)(A) & Criminal Rule 1.8(1)(A)), and the ATTC form is added to the list of records that are not to be posted to a court's Internet website (Rule 123(g)(5)(G)). An informal survey of some of the more technologically-advanced municipal and justice courts in Arizona -- Chandler, Phoenix, Scottsdale, Tempe, and Tucson City Courts and the Maricopa Justice Courts -- revealed that although most of them have the capacity to post these forms to a website, none are planning to do so in the near future. In the near term, these courts are working towards making the digital image of the ATTC form available to court staff and the public on computers *at the courthouse,* but not on the Internet. The proposal would not interfere with this plan.

Emergency consideration of this petition is requested because the Administrative Office of the Courts working with local courts needs to launch a large-scale public information effort to educate practitioners, court staff, and the general public about the new sensitive data form requirement before the December 1st effective date. Adoption of amendments to the sensitive data form requirement after

December 1st may engender confusion and require additional training and public outreach thereafter to clarify the ATTC-related modifications to the new requirements.

Respectfully submitted this 15th day of August, 2005.

Jennifer A. Greene, Policy Analyst
Court Services Division, AOC
Arizona Supreme Court
1501 W. Washington, Suite 410
Phoenix, AZ 85007-3231
(602) 542-9555

Proposed Amendment
(new language underlined, deletions ~~stricken through~~)

Rule 123. Public Access to the Judicial Records of the State of Arizona

(a) – (f) No changes

(g) Access to Audiotape, Videotape, Microfilm, Computer or Electronic Based Records.

(1) – (4) No changes.

(5) *Remote Electronic Access to Records and Cost; Limitations on Remote Access.*

(A)-(F) No changes.

(G) The following records and data elements are not open to public inspection by remote electronic means:

(i) presentence reports;

(ii) criminal case exhibits, unless attached to a motion or other filing;

(iii) petitions for an order of protection or injunction against harassment;

(iv) a juvenile victim's name, and a victim's address and telephone number or other locating information; and

(v) documents, docket and calendar information on unserved orders of protection or injunctions against harassment.

(vi) The Arizona Traffic Ticket and Complaint Form. Non-sensitive data extracted from this form may be displayed.

The court may offer this information by remote electronic means to parties and attorneys of record in their own cases. In addition, parties" residential addresses should not be displayed on Web sites offering basic individual case information extracted from case records. However, parties' residential addresses need not be redacted from case records before they are made accessible online.

(H) In cases filed before January 1, 2007, case documents filed by parties shall not be posted to a court's publicly-accessible Web site~~, except that this provision shall not apply to the electronic posting of the Arizona Traffic Ticket and Complaint form in traffic and boating cases~~. In cases filed on or after January 1, 2007, non-confidential case documents filed in criminal, civil or tax cases may be displayed on Web sites in accordance with the provisions of this rule. In domestic relations, juvenile, and probate cases, only court-generated records such as appellate opinions, judgments, orders, notices, calendars, dockets, or minute entries may be posted to a court's publicly-accessible Web site; provided, however, that the court shall not place sensitive data in such court-generated records except upon a finding of good cause. The Clerk of the Court shall be immune from suit for any conduct relating to the electronic posting of case documents containing sensitive data that a party or parties have failed to redact.

(I)-(J) No changes.

(6) No changes.

(h) Inspection and Photocopying. No changes

New Rules of Criminal (1.8) and Civil (5(f)) Procedure

Rule ___. Sensitive Data

(1) *Filing Sensitive Data.*

(A) *Filings of Parties.* Before filing any paper containing sensitive data with the court, the filing party shall omit or otherwise redact the sensitive data unless it is specifically requested by the court or is required by statute. If the sensitive data is specifically required by the court or by statute, the filer shall record the requested information on a separate sensitive data form which shall be maintained by the clerk as a confidential record. Unless the court orders otherwise, any further written reference to a sensitive data element shall thereafter be made by referring to its corresponding item number on the sensitive data form or other means, rather than by inserting the actual data into the document being filed with the court. Parties filing an Arizona Traffic Ticket and Complaint form are exempt from the requirements of this subsection.

(B) *Court Records.* The court shall not place sensitive data in court-generated records such as judgments, orders, notices, calendars, dockets, or minute entries, except upon a finding of good cause.

(C) *Supplementation of Sensitive Data Form.* Whenever new information is needed to supplement the record in a case, the parties shall file an updated sensitive data form, reflecting all previously disclosed sensitive data plus any additional sensitive data required to be filed in the case.

(2) *Sensitive Data Defined.* For purposes of this rule, "sensitive data" means social security number, bank account number, credit card number, other financial account number, a juvenile victim's name, and a victim's address and telephone number or other locating information.

(3) *Sensitive Data Form.* The sensitive data form shall be in substantially the following form:

[No changes proposed for the sensitive data form itself]