

**ARIZONA SUPREME COURT
RULE 123 AND DATA DISSEMINATION ADVISORY COMMITTEE**

MINUTES

January 29, 2008
Supreme Court Building, Phoenix, AZ

MEMBERS PRESENT:

David Bodney
David K. Byers, Vice Chair
Janna Day
Don Jacobson
Hon. Michael Jeanes, Chair
Hon. Patricia Noland
Catherine O'Grady
Hon. Rachelle Resnick
Jim Scorza
Terry Stewart
Hon. John Taylor
Karen Westover

MEMBERS ABSENT:

Patricia Sallen
Hon. Peter Swann

GUESTS:

Karl Heckart
Richard Varn
Theresa Barrett
Melinda Hardman
Regina Kaupanger
Kevin Klimas
Richard Robertson
Mark Osborn
Terry Jennings
Louise Cook

STAFF:

Tama Reily * Jennifer Greene

I. Call to order

Chairman Michael Jeanes called the meeting to order at 10:05 and welcomed the members to the committee. He reviewed the committee's operating rules and asked members to inform him or staff if they needed to send a proxy. Members and guests introduced themselves.

II. Review of Administrative Order No. 2007-101

Vice-Chairman Dave Byers identified the primary issues that led to the formation of the committee, including the need for:

- standards and processes relating to sharing data with government agencies and commercial users,

- uniform standards for posting case records and case information online -- which records or information and for how long – while protecting against identity theft, and
- recommendations about how to accommodate legitimate needs for personal identifying information in online and bulk or customized data dissemination.

With advances in automation, these and numerous related issues have surfaced that warrant consideration by a committee of stakeholders to identify appropriate adjustments to Rule 123. In recent years, the Chair and Vice-Chair have both served on related projects hosted by the Conference of Chief Justices/Conference of State Court Administrators and the Department of Justice. The guidelines developed for these projects may assist the committee with its work.

III. Overview of Arizona judicial branch databases, integration projects, and online case information

Karl Heckart, Chief Information Officer and Director of the Information Technology Division of the Administrative Office of the Courts (AOC), provided background on the types of information contained in court databases, current data sharing arrangements, as well as integration projects in the planning and development stage.

Mr. Heckart explained that Arizona courts are now in a second wave of automation. New case management systems in development will offer more standardized data, better data validation and integration with other systems, and e-filing capacity. The committee will provide timely and much-needed standards as these upgrades are designed and implemented.

Databases courts maintain are integral to various operations including managing cases, reporting protective orders to law enforcement, tracking adult probationers and

children involved in dependency and delinquency matters, e-filing, enforcing monetary penalties, disciplining attorneys, and providing online access to court records.

Case management system (CMS) data typically contains personal identifiers, including name, date of birth, address, driver's license number, state issued identification that may be biometrically based, case events, criminal charges, case outcomes, and payments made. In non-criminal cases, the CMS data contain fewer identifiers, including no biometrically-based identifiers, and the names and addresses of the parties are unverified. In the juvenile arena, the data includes names of parents or guardians and information about placement and treatment. This information is closely guarded.

The AOC maintains a central repository, known as the data warehouse, where much of this information resides. Trusted justice system partners such as probation, law enforcement, and corrections departments have direct access to portions of the data maintained in the warehouse, including sensitive personal identifiers, through a program known as "s-TRAC." A federal contractor that conducts background checks on federal job applicants also participates in s-TRAC.

In connection with the statewide penalty and restitution collections program, the AOC transmits data from the data warehouse and other production databases to collection agencies under contract with the courts, the Department of Revenue for tax refund intercepts, and MVD for vehicle registration holds. Traffic case information is reported to MVD to aid its regulation of non-commercial and commercial drivers. Child support information in the data warehouse is shared with the child support clearinghouse operation of the Department of Economic Security.

The publicly-accessible case lookup website hosted by the AOC data warehouse offers a subset of CMS information to the general public for most of the courts in Arizona. Maricopa and Pima County Superior Courts manage their own public access websites for their CMS information. The AOC's case lookup website has been in operation for seven years. It receives more than four million hits per month. Employment screening firms are among the heavier users of the website. Individual cases are viewed by party name or case number; personal identifiers are limited to name, date of birth, and residential city, state, and zip code. The site features concise descriptions of case events, outcomes, criminal and traffic charges, and payment histories.

At a cost of \$3,000 per year, subscribers can get from the AOC a monthly CD of the entire database of information available on the public access case lookup website. Approximately twelve companies currently subscribe to this service, including news media, and tenant and employment screening agencies. A number of local courts have established similar arrangements with bulk data purchasers interested in their case information.

A state law adopted in 2007 requires all courts to provide online public access to criminal case minute entries by 2010, which the Clerks of Court in Pima and Maricopa Counties already offer online. In addition to their minute entries, both Pima and Maricopa Clerks' Offices provide access to their electronic repositories of case documents (stored in an EDMS) by law enforcement, public defenders, and prosecutors in their counties. Pursuant to a Supreme Court authorized pilot project, Maricopa County is also providing litigants and their attorneys with access to the EDMS records for their

own cases. Minute entries sometimes offer sensitive data, particularly in Family Law cases. The Chair reported that a recent judicial training in Maricopa County has revealed some problem areas where some judges are still including sensitive data in certain types of minute entries, orders, and final judgments.

The Maricopa Clerk's Office has coordinated its plans to move to a paperless operation with the State Library, Archives, and Public Records agency (SLAPR); however SLAPR is not yet accepting any documents for its archives in any format other than paper or microfilm.

The Chair noted that the Maricopa County Recorder recently paid some \$5 million to a private firm to have social security numbers redacted from recorded documents going back to 1930. Ms. Noland reported that her court started using a sensitive data form for Family Law cases several years ago, but compliance by parties and attorneys was not widespread until use of the form was codified in the Family Law Rules of Procedure in 2006. Mr. Heckart explained that scanned records are not "machine readable;" in the future courts will move to machine readable electronic records, which will allow for automated redaction of sensitive data.

Mr. Heckart identified the following data integration initiatives that are either in development or planned for the near future:

- Electronic reporting of criminal case disposition to DPS;
- Electronic traffic citations;
- Mental health gun checks;
- Statewide DUI case information repository;

- Statewide expansion of the current Maricopa County Justice Web Interface (JWI) program that consolidates information about individuals from numerous sources, including California and Nevada, involved in criminal activities. Courts use this information for pre-trial release and sentencing. Through this sharing arrangement, some data is transferred to the courts' CMS systems, and some data sources are raising issues about who owns the information once it has been transferred.
- Support for judicial decision-making that would provide judges more information about offenders prior to sentencing. Due process issues remain to be resolved.

Mr. Heckart offered his suggestions on the issues the committee should resolve, including:

- Whether to remove older cases from the public access website and when,
- Whether to display pre-adjudication case information in criminal cases,
- Whether to exclude data miners from accessing the website,
- Whether to impose access restrictions for some categories of users, and
- Whether to impose restrictions on commercial use and secondary dissemination as well as how to track compliance and enforce restrictions.

III. Overview of the federal regulatory environment governing the consumer data industry and consumer data industry practices

The committee heard a presentation by Richard Varn, Esq., Executive Director of the Coalition for Sensible Public Records Access (CSPRA), an Iowa non-profit organization supported by several members of the commercial data industry. He described himself as not completely aligned with the consumer data industry. Mr. Varn stated that he is a former Iowa state legislator, former CIO for Iowa, a Senior Fellow with the Center for Digital Government, a consultant for 30 years on privacy and public records access issues, and currently works as CIO for the City of San Antonio, TX.

Mr. Varn offered suggestions about how courts could identify and accommodate

legitimate commercial needs for personal identifying information attached to case records. The Fair Credit Reporting Act (FCRA) requires companies to “follow reasonable procedures to ensure maximum possible accuracy of the information concerning the individual about whom the report relates.” 15 USC §1681e (607)(b). Under the Act, companies that do not gather enough identifiers attached to a record cannot use the record, or must reduce its use, or put caveats around its use. A recorded lien, credit history, or rental history cannot be matched to a name, so those needing to know won’t have the information unless they look it up themselves.

Underlying concerns about personal identifiers is the fact that many rights, benefits, and privileges are triggered by “single factor authentication” such as a fingerprint or other biometric identifier (something you are); a badge or token (something you own); or an account number or phrase such as a social security or driver’s license or mother’s maiden name (something you know). A single factor may be unique to the individual but is also easily copied or stolen. These practices are founded on the assumption that each person has only one name, one home address, one professional license, one driver’s license, etc. Most of the concerns could be eliminated if more authenticators were required to obtain the rights, benefits, and privileges, such as requiring multiple biometrics (a thumbprint *and* a photo), or a combination of more obscure facts about a person’s past. This change could also remove the incentive to steal unique identifiers.

People are fearful that court records and other public records are commonly used to commit identity theft, but a recent Javelin Research study found 67 percent of identity theft is perpetrated by someone who has borrowed or stolen a credit card, another 15

percent involves someone known to the victim who has taken physical documentation from the victim and used it to impersonate that person. The remaining 15 percent involves criminals operating over the web primarily from Nigeria and Russia who sell stolen identities in “kits” to other criminals. The sources of the information brokered by these criminal enterprises are numerous and impossible to protect against and include employees or hackers stealing entire databases. In fact, public records are not the most convenient source nor are they the primary source of data being used in identity theft. Unfounded claims about identity theft of public record information are promoted by the companies that want to make money on consumers’ fears by offering to monitor consumers’ credit histories and bank card statements for a fee.

Further complicating the situation is the fact that until relatively recently, there was widespread use of unique identifiers such as social security numbers for rights such as voting and driving, and many records were made of this information - many of which are not public agency records - that are still readily available. Many people believe the government should protect information in public records that has never been deemed confidential, such as birth dates, phone numbers, and addresses. Some have questioned the wisdom of expecting government to spend large amounts of taxpayer dollars to remove or protect this type of traditionally public information appearing in public records, particularly for very old records.

The rules of our society are unenforceable if we cannot accurately identify people. Without accurate data and identity security, behaviors cannot be attached to identities. This requires access to valid information. Commercial data compilers have filled a gap

that the public sector has failed to provide by making data available from multiple sources; even the FBI consults these commercial databases for its investigations.

Sixty percent of our economy is driven by consumer spending, and the availability of accurate information lowers the risks associated with extending credit, selling insurance, renting property, hiring, etc., which in turn has dampened down economic boom and bust cycles. Wal-Mart's "just-in-time" inventory process is a good example of how accurate and timely data can be used to improve lives because it reduces the need to shut down manufacturing and lay off employees temporarily due to excess inventory, thus promoting economic stability.

In designing a data access policy, the amount of authenticating factors required of applicants should be tied to the risks inherent in the transaction. A basic process would require users to identify themselves and register. For access to more sensitive data, the types of authentication required of the health care providers who seek Medicaid and Medicare reimbursements could serve as a model.

Another option is to contract with an "infomediary" to manage the data so the courts do not have to do it themselves. E-ZPass, a private company, provides this service for many states, cities and transportation authorities in the northeast that operate toll roads. Similarly, private adoption registries handle confidential court records in some states.

If the committee decides to recommend a prohibition against using court data for commercial solicitations, Mr. Varn stated that any publicly-traded company can be expected to abide by such a requirement. In his opinion, credit agencies are doing a better job of managing credit histories than they did in the past, and have become

indispensable in many cases because government never had the resources to build what they have built.

Through a well-designed process of enrollment, legitimate users of court data can be identified and permitted enhanced access. This will involve authenticating the entity or individual requesting access – are they who they say they are – and conducting some amount of background screening. Resources such as Dun and Bradstreet and LexisNexis or Westlaw can assist in determining if an applicant is operationally and financially stable and reliable.

A simple low-cost enforcement mechanism to prevent the use of bulk data for mailing lists would be “salting” the data with a fictitious record containing a mailbox that can be monitored to see if any commercial solicitations are mailed to it. The mailing can then be tracked back to the abuser.

Mr. Varn urged the committee not to confuse the access issue with the issue of reasonable use of data. He asked whether it was necessary to hide the record of an old conviction for a petty offense so it cannot be used to deny someone employment, when the conviction should not have been considered relevant to the hiring decision in the first place. The solution to this problem may be more policies relating to fair employment practices, not restrictions on access to public record information.

He also suggested that to try to control downstream use of data is almost impossible given the screen scraping technology currently available. If data is displayed on a screen it can be taken, there’s no way to effectively regulate and enforce restrictions on secondary dissemination. Tracking down information theft is harder than drug enforcement.

Mr. Varn outlined his suggested key steps for enrolling users, whether they are employees, trusted partners, or outsiders:

- Decide what level of proof is appropriate for granting them authorization to use the system (proofing).
- Decide what number, kind, and mix of factors will be required to verify the user each time they seek to access data; this should be tied to the risks inherent in the transaction or attribution (authentication).
- Decide how much access should be granted to each category of users and what consequences should be imposed for non-compliance (authorization).
- Decide what infrastructure will be needed to manage, enforce, and audit compliance with whatever process is established.

He recommended that, if possible, courts should require truncated identifiers rather than eliminating them entirely, so that they still function as unique identifiers but do not invite as much “mystery.” He suggested the committee should consider the unintended consequences of charging too much money and imposing too many restrictions. In Iowa, users who are willing to show identification and sign in are permitted to view unredacted public records on a computer terminal located at the public agency. He also recommended that the committee hear from the “end users” of commercially-compiled data to understand how their operations would be impacted if the information is not available to them.

Patricia Noland noted that electronic databases are not the only potential source of identity theft. Her courthouse still has people coming in and inputting data from hard files into their laptops, which raises issues with errors in data entry as well as identity theft. Older Family Law case files still contain information such as bank accounts and social security numbers of parties and their children.

IV. Rule 123 history and evolution

Jennifer Greene, Staff to the Committee, reviewed the history of Rule 123, which was first adopted in the mid-1990's, noting that the advent of the Internet and increased use of automation by courts have necessitated several reviews of the rule by various committees and workgroups as the courts work to integrate the rule's provisions with changes in the way information is disseminated to the public and other government agencies involved with the justice system. Earlier recommendations and findings for amendments are contained in the materials distributed to the members.

Many of the concerns about sensitive data appearing in case records have been alleviated by the new Arizona Rules of Family Law Procedure, the proposed new Probate Rules, and the recently-adopted Arizona Rules of Protective Order Procedure -- all of which incorporate some type of confidential sensitive data form. Despite these changes, sensitive data continues to be displayed in court-generated records to some extent.

In 2005, the Supreme Court approved a number of amendments establishing policies for handling sensitive data by means of a confidential sensitive data form in civil and criminal matters. However the court has not yet established an effective date for these amendments pending further review of the practicalities involved in eliminating sensitive data from court-generated records. The new committee's work will include consideration of that review and drafting any recommendations deemed necessary.

Unlike some other jurisdictions, Rule 123 does not specifically address bulk data or compiled data, beyond stating that courts need not provide case records that are not generated in the ordinary course of business. The rule specifically permits confidential record access by legally authorized government agencies. Provisions relating to commercial users were taken directly from the public record statutes, although the rule

stops short of requiring courts to determine the fair market value of records provided to commercial users and charging accordingly. The statutes governing remote electronic access fees date back to 1995, and the committee may wish to consider making a legislative proposal to update these statutes. Similarly, the provisions in the rule itself dealing with public and “value-added” remote electronic access should be reconsidered.

V. Upcoming meeting agendas

The Chair reviewed the proposed schedule and topics for upcoming meetings and it was agreed to switch the focus of the March and April meetings. Sensitive data will be considered in March and data exchanges with other government agencies will be the focus of the April meeting. As originally proposed, the February meeting will focus on responding to commercial user requests for compiled data.

Jim Scorza reported that Phoenix Municipal Court has had to conduct a lot of computer programming in response to news media requests for compiled data of all photo enforcement citations covering a number of years. The Vice-Chair suggested the committee should consider the media’s use of bulk data as separate from other types of commercial users, since Arizona case law has exempted the news media from commercial user fees under the public records statutes.

VI. Call to the public

Teresa Jennings of Reed Elsevier, parent company of LexisNexis, explained that the civil judgment information provided by Maricopa County does not include enough identifying information on the parties to enable LexisNexis to match its files with the case outcomes in these records. She offered to present information at the February

meeting on what her company feels is the essential list of personal identifiers they need to comply with FCRA requirements.

Kevin Klimas of Clarifacts, Regina Kaupanger of the National Tenant Network, and Richard Robertson of R3 Investigations, agreed to provide information and bring in some representative clients to help the committee understand the importance of commercially-available case data, court records, and personal identifiers to the end user.

Meeting adjourned at 2:00 PM.

Next Meeting: Tuesday, February 26, 2008, 10:00AM – 2:30 PM, Supreme Court building, 1501 W. Washington, Phoenix, AZ, Conference Room 119A&B.

**ARIZONA SUPREME COURT
RULE 123 AND DATA DISSEMINATION ADVISORY COMMITTEE**

MINUTES

February 26, 2008
Supreme Court Building, Phoenix, AZ

MEMBERS PRESENT:

David Bodney
Dave Byers, Vice Chair
Janna Day
Don Jacobson
Hon. Michael K. Jeanes, Chair
Hon. Patricia Noland
Catherine O'Grady
Hon. Rachelle Resnick
Patricia Sallen
James R. Scorza
Terry Stewart
Hon. Peter Swann
Hon. John Taylor
Karen Westover

GUESTS:

Jennifer Greene
Cherrill Crosley
Jeff Young
Scott M. Clark
Regina Kaupanger
Edward Byczynski
Evan Kesselman
Lori W. Kessleman
Susan Brenton
Neal T Haney
Teresa Jennings
David Withey
Louise Cook
Rich Robertson
Van Di Carlo
Risk Assessment Group
Kevin Klimas
Donna Taylor
Joan Koerber-Walker
Mark Osborn
Theresa Barrett
Janet Scheiderer

MEMBERS ABSENT:

None

STAFF:

Tama Reily * Melinda Hardman

I. Call to Order

Chairman Michael Jeanes called the meeting to order at 10:05 a.m.

Jennifer Green advised the committee of her new position in the AOC and her resulting modified role with this committee. She introduced Melinda Hardman, Court Services Division, AOC as the new staff person for this committee. Ms. Greene also reviewed the material for today's meeting.

Mr. Jeanes explained that he intends to reserve time at the end of each meeting for discussion of the issues and to seek direction from the committee for outcomes.

Members and guests introduced themselves.

II. Approval of Minutes

The minutes from the January 29, 2008 meeting were presented for approval.

MOTION: To approve the Rule 123 and Data Dissemination Advisory Committee meeting minutes for January 29, 2008. Seconded. Motion approved unanimously.

III. Commercial Data Industry Presentations

Several commercial data industry businesses made presentations to the committee, addressing such topics as: 1.) what data they want to receive from courts, 2.) what they do with the data once they receive it, and 3.) limitations they are willing to accept on use of the data.

One overarching legal requirement that applies to the commercial data industry is the Fair Credit Reporting Act (FCRA), and more specifically, 15 U.S.C. § 1681e. (b), which provides, “Whenever a consumer reporting agency prepares a consumer report it shall follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates.”

A. Tenant Screening

Regina Kaupanger, President, National Tenant Network (NTN) of Arizona explained that NTN was founded to screen prospective tenants for landlords. NTN has 30 offices nationwide. Regina explained that to properly serve its customers, NTN must maintain a timely, detailed, and accurate (FCRA compliant) database of court records. Timeliness is extremely important. Two data elements that are particularly necessary for NTN’s product are:

- the full eviction address, including street, and
- some other identifying information (in addition to name) on the person evicted, such as d.o.b. or truncated SS#.

Regina stated that when NTN is prohibited from obtaining this information from court records, NTN is unable to make a verified match of common names. For example, if a street address is not provided, NTN is unable to match civil case records to the proper person.

NTN’s proposal: NTN asked the committee to consider providing full access to bulk court records to qualified companies only, with no restrictions on use. NTN proposes that a company would be designated as qualified to receive bulk records after submission of an affidavit and appearance at a hearing.

Upon questioning by committee members, NTN agreed that if courts will provide full party addresses, NTN will not:

- use the addresses for mailing lists.
- resell the addresses

Ed Byczynski, CEO and general counsel for NTN stated that NTN's focus is on the civil court record. At a minimum, NTN would like to receive from the courts: name, address, d.o.b., disposition date, and maybe a phone number. For criminal cases, NTN would like to receive the full date of birth, not just month and year, since NTN is subject to liability for making an error in identifying someone as a criminal. The FCRA allows screening companies to report a criminal charge for only 7 years, but it does not place a limit on how long a criminal conviction can be reported. Ed recommended that NTN would agree to qualify itself to obtain full access to court data. NTN would sign an affidavit, agree not to make money by selling addresses, and submit to an ex parte hearing. NTN offered to help the committee establish this type of procedure. Ed stated that no other state uses such a certification process.

The committee also heard from Scott M. Clark, an attorney representing the residential property management industry, Jeff Young, an owner of investment real estate in Arizona; Susan Brenton, Executive Director of Manufactured Housing Communities of Arizona; and Neil Haney, President, Manufactured Housing Communities of Arizona in support of NTN's position.

B. Employment Screening

Kevin Klimas, President, Clarifacts, explained that his company is a screening service company in Arizona and primarily conducts employment screenings. The employment screening industry is regulated by the Federal Trade Commission (FTC) pursuant to the FCRA and by the states under various state laws and regulations.

Some of the services Clarifacts offers are:

- Criminal record searches
- Sex offender registry searches
- Employment applicant verifications
- Driving record history searches
- Treasury Office of Foreign Asset Control, Specially Designated Nationals search
- International searches
- Drug testing

Clarifacts conducts thousands of searches each month, primarily of criminal records. Clarifacts can narrow their search on an individual using name and d.o.b. but must have a SS# to be certain.

Kevin stated that one of the reasons companies use his services is that employers want to avoid legal exposure for negligent hiring. He explained that an employer can be held liable for the wrongful acts of an employee if the employer knew or should have known the employee would cause harm.

Donna Taylor, Vice President of Arizona Baptist Retirement Centers, which provides various levels of care to the elderly and Joan Koerber-Walker, CEO, Arizona Small Business Association spoke in support of Clarifacts' work.

C. LexisNexis (Reed Elsevier, Inc.)

Teresa Jennings, Director, State Government Affairs, Reed Elsevier, presented an overview of the LexisNexis database and how it is used. She explained that LexisNexis provides information in a variety of areas, including legal, risk management, corporate, government, law enforcement, accounting, and academic. Court records are one of many sources from which LexisNexis obtains information. According to LexisNexis, their data is used to enforce child support obligations and government assistance programs, verify the identity of individuals, locate heirs and beneficiaries of trusts and unclaimed funds, determine the location of assets for tax collection purposes, and other uses.

LexisNexis provides data to users using a three-tiered protocol system (regular, middle, high). Teresa was uncertain of the difference among these tiers but offered to obtain this information and get back to the committee. She noted, however, that as a particular record moves into the online world, and becomes more accessible, it may move between tiers.

Teresa reported that LexisNexis does resell data. She also said that LexisNexis resells data that credit bureaus and others do not wish to compile for themselves. However, Teresa was uncertain whether LexisNexis resells data for marketing purposes and promised to get back to the committee on this issue.

Teresa agreed to report back to the committee on the following specific questions:

1. If LexisNexis obtains an incomplete record that it is unable to report, due to FCRA limitations, does LexisNexis save the record and try to match it later?
2. Does LexisNexis sell addresses for mailing lists?
3. How easy is it to obtain LexisNexis data? For example, can LexisNexis stop a stalker from paying to look up an address on a person?

LexisNexis' proposal: Teresa advised the committee that LexisNexis can comply with marketing restrictions placed on the resale of their data. However, she asked the committee to keep any such restrictions or exclusions narrow since the data LexisNexis acquires goes into many different databases, and tracking can become difficult.

D. Private Investigations, Investigative Reporting, and Accessing Driving Records Under the Driver's Privacy Protection Act

- a. Richard Robertson, Owner/Investigator, R³ Investigations addressed the use of court records by private investigators. In Arizona, private investigators are licensed under A.R.S. Title 32, Chapter 24. Rich noted

that pursuant to ARS 32-2455 (A), “[N]o licensee . . . may divulge or release to anyone other than his client or employer the contents of an investigative file acquired in the course of licensed investigative activity.”

Court records are just one of many public records private investigators use. Rich often aggregates court records in a database to extract trends or groups of data. Then, for example, he can analyze the information to compare sentences given to different defendants for conviction of the same offense.

Rich also talked about his use of the Drivers Privacy Protection Act. He explained that under this law, users are liable for the downstream use of the information. One reason Rich uses the MVD database is to find someone he is attempting to serve with a summons.

Rich Robertson’s proposal: Rich feels that the Maricopa County Assessor has a good model of disseminating data, that the courts should consider adopting this model. The Assessor’s office sells data for commercial and non-commercial uses and has an established price sheet. Furthermore, Rich suggested that perhaps the supreme court could protect the reuse of court records by following the process used by law enforcement where an Executive Order has been issued that prohibits police records from being used to solicit accident victims.

- b. Jennifer Greene reported on the AZ MVD Driver’s Privacy Protection Act Program. This program is governed by state statute. Permissible uses of MVD data are set out in statute and re-dissemination is prohibited. In order to gain access to MVD data, commercial users must provide certain documentation to verify that they are a legitimate business and carry general liability insurance. Fees for the requested records range from \$4.25 – 6.25 per record, depending on whether the record is certified. SSN’s in the MVD databases are redacted to the last 4 digits. Users must agree to keep the data secure. A review panel at MVD meets monthly to review applications for access to the data.

IV. Roundtable Discussion

The following issues and concerns were raised during the committee’s roundtable discussion of the issues to date:

- We need to hear from privacy groups.
- We are concerned about: 1.) special requests for information (most of which come from the media). We charge for the first request for this type of report because of programming costs. Then subsequent requests for the same report are free; 2.) Redacting. It is very time consuming for us to redact and has imperfect results. We do not want to have to redact anything.

- There is one public. Whatever right of access we grant is to the public. There should be only one level of users. There should not be a super user who receives additional information than the public.
- What is the executive branch doing with regard to releasing addresses? Is their responsibility the same as ours? If they release addresses, and we protect addresses, that does no good.
- Our land records laws require disclosure of addresses.
- We could label a data field as “public” information, but still limit access to the field by different methods. We need to make our records as open as possible, but we need to tier the accessibility to this information so that, for example, an individual can obtain it by coming down to the courthouse, but we do not put it on our website. We should provide as much information as possible. We should not restrict how users use the information.
- We do not like to provide a report about how various judges ruled in a particular type of case. Many judges are uncomfortable with this request. They feel it interferes with their discretion.

V. Call to the public

Chairman, Michael Jeanes made a call to the public. No comments were presented.
Meeting adjourned at 2:35 PM.

Next Meeting: Tuesday, March 11, 2008, 10:00AM – 2:30 PM, Supreme Court Building,
1501 W. Washington, Phoenix, AZ, Conference Room 345 A/B.

**ARIZONA SUPREME COURT
RULE 123 AND DATA DISSEMINATION ADVISORY COMMITTEE**

MINUTES

March 11, 2008
Supreme Court Building, Phoenix, AZ

MEMBERS PRESENT:

Dave Byers, Vice Chair
Janna Day
Don Jacobson
Hon. Michael K. Jeanes, Chair
Hon. Patricia Noland
Catherine O'Grady
Hon. Rachelle M. Resnick
Patricia Sallen
Terry Stewart
Hon. John S. Taylor
Karen Westover

MEMBERS ABSENT:

David Bodney
James R. Scorza
Hon. Peter B. Swann

GUESTS:

Jennifer Greene
Kathy Sekardi
Kay Radwanski
Mike Sankey
Regina Kaupanger
Carol Schreiber
Dan Corsetti
Mike Goss
J. R. Rittenhouse
Sally Wells
Teresa Jennings
Jamie Mabery
Dorrian Jones
Rich Robertson
Mary Jane Gregory
Kevin Klimas
Mark Osborn
Janet Scheiderer
Jim Belanger

**GUESTS APPEARING
TELEPHONICALLY:**

Mel Bowers
Tracy Miller
Rick Unklesbay

STAFF:

Tama Reily * Melinda Hardman

I. Call to Order

Chairman Michael Jeanes called the meeting to order at 10:05 a.m.

Guests introduced themselves.

II. Approval of Minutes

The minutes from the February 26, 2008 meeting were presented for approval.

MOTION: To approve the Rule 123 and Data Dissemination Advisory Committee meeting minutes for February 26, 2008. Seconded. Motion approved unanimously.

III. Results of the Sensitive Data Workgroup investigation and review of pending amendments to Rule 123

Jennifer Greene provided an overview of the pending proposal for permitting online access to court records. She explained that most of the elements of the policy came from an ad hoc committee, chaired by Judge Weisberg in 2002 and from a subsequent workgroup that met under the direction of the supreme court staff attorney's office. The policy focuses on which documents and which data elements a court may post online.

The general idea is that documents are not be posted online until there is a system in place to put confidential data, filed by the parties, on a separate document and to ensure that the court does not include confidential data in its orders. This idea was first tested under the new rules of Family Law procedure, which went into effect in January 2006. Anecdotal information has surfaced that although some parties have been entering sensitive data on a sensitive data sheet, the court was then often times putting this sensitive data back into an order, thus defeating the purpose. In light of this practice, the proposal before the supreme court for handling sensitive data is being revisited by the committee.

The Weisberg committee recommended making civil and criminal documents available online to the public first then phase in other types of cases. However, all records in a given case could be made available online to parties and their attorneys involved in the case. The proposed change to Rule 123 would permit online access by the general public for both party-filed records and court-generated records in civil and criminal cases, with a few exceptions. However only court-generated orders, notices, minute entries and the like could be viewed online in Family, Probate, and Juvenile Delinquency cases.

III. Protecting sensitive data in Family Law cases: The new Arizona Rules of Family Law Procedure and the use of the confidential sensitive data sheet

Judge Colleen McNally, Presiding Family Law Judge, Superior Court in Maricopa County provided an overview of how her court is addressing some of the issues this committee is facing. She noted that Rule 43.G.1 of the AZ Rules of Fam. Law Proc., require a filing party to redact

sensitive data, and this has been a huge improvement for her court. However, there has been a tendency by the filing party to place sensitive data on a separate sheet, but still leave the sensitive data in the pleading, assuming the court will remove the data from the pleading. Judge McNally acknowledged that the court must do more to educate filers about the process. Generally, judges do not take any action when the judges notice that a lawyer has not complied with the sensitive data sheet requirements. Judges should probably take a more active role and remind lawyers of the proper procedure, however pro pers will continue to be a problem. Judge McNally also noted that her staff modified their own court forms to remove sensitive data, however other problems regarding sensitive data persist.

Judge McNally entered two Administrative Orders in February 2008: AO 2008-021 establishes a pilot program incorporating detailed procedural requirements for use of a sensitive data sheet, and making use of the sheet mandatory, rather than optional, and AO 2008-019 addresses the confidentiality of Orders to Stop Assignment filed between January 1, 2006 and December 31, 2007.

Another continuing problem, however, is foreign orders. These are often filed as an attachment to a pleading, and the Family Court has no authority to modify a foreign order by removing data.

The Superior Court in Maricopa County, Clerk's Office, Quality Control Unit recently conducted a study which showed that Social Security Numbers and bank account numbers were still appearing at a significant rate in documents filed by attorneys, pro pers, and the court in cases initiated in 2007.

Discussion ensued as to additional concerns regarding sensitive data in Family Court matters. Comments included:

- The sensitive data sheet was intended to keep certain information out of the paper file, however, since some courts have such a high volume of these cases, it is difficult to obtain full compliance. Is there any public policy reason why we should put these pleadings online?
 - There was some agreement that parties and attorneys should be given online access to their own file, but that no one else should receive online access to family law cases. However, others noted that the media and the State Bar want all documents online, including those in family law cases. For example, attorneys want to easily see how a judge has decided other cases with similar facts, the news media wants to have easy access to high profile divorce cases such as Lute Olsen's, and victims may want to follow a criminal case online without having to appear at the courthouse.
- It would be okay to post Family Law documents online, once the sensitive data is removed, however we have not yet been able to achieve this.
- There is more to be concerned with than sensitive data in Family Law cases. These cases, by their nature, can involve serious allegations, some based upon hatred, which cannot be removed from the pleadings. These cases should not be placed online, even if the sensitive data could be removed.

- By law, judges are required to address each statutory factor for custody, in writing. This information would then be available online. Family law cases are more complicated and have greater impact on people than other types of cases.
- Family law cases should be kept offline for now.

III. Protecting sensitive data in Probate proceedings: Proposed new procedural rules

J. R. Rittenhouse, Staff to the Probate Rules Committee, provided an explanation and update of the proposed AZ Rules of Probate Proc. which will become effective January 1, 2009, if adopted. She noted that many decedent's estates in AZ are handled on an informal basis with little involvement by a judicial officer. Many probate matters are handled by pro pers. Furthermore, these cases include a great deal of personal information such as medical documentation regarding a person's mental capacity in adult guardianship and conservatorship cases as well as financial information. Additionally, Probate proceedings often involve vulnerable adults who may be subject to identity theft and financial exploitation.

The proposed rules call for use of a Probate Confidential Information Form when a party files a petition or application requesting the appointment of a guardian, conservator, or personal representative. Additionally, the Rules name specific documents, including medical reports, accountings, and inventories, all of which are deemed confidential and not open to the public. In fact, very little information would be available to the public under the proposed rules, since most information in Probate files deal with medical and financial matters.

Discussion ensued as to additional concerns regarding sensitive data in Probate matters. Comments included:

- The Probate Rules Committee agreed that minor guardianships and conservatorships would not be covered by the proposed Probate rules, because, in Maricopa County and most other counties, minor guardianships start in Juvenile Court.
 - Pima County noted that in their county, minor guardianships are processed by the Probate Department of the Superior Court.
- The rules provide for a good cause exception from confidentiality, for example, for the media.
- Out-of-town relatives want to be able to check online for the status of a probate case, since personal representatives do not always send notice to everyone who is entitled to receive notice. There needs to be a balance. Perhaps we can list the name of the case online, along with the calendar events, so that someone knows when a hearing is coming up, and provide an index of the filings but not the actual pleadings.
- The Probate Rules Committee does not want to put addresses or dates of birth online in probate matters because of the concern of physical or financial abuse to a ward. However, complete address and date of birth may be necessary in order to ensure that a member of the public has located the proper case online. We need to balance a relative's need to know with possible harm to a ward. Consensus was not reached here.
- We may need to look more closely at the process for enabling an appointed conservator to obtain necessary sensitive data which is not in the court order but which is required, for example, to take to a bank. Some clerk's offices require the conservator to show

identification, then the clerk's office gives the person a certified copy of the sensitive data.

III. Protecting juvenile victims' names and other sensitive data elements in criminal case records

Sally Wells, Chief Assistant for the Maricopa County Attorney's Office explained that her office would have difficulty complying with a requirement that juvenile victims' names appear on a sensitive data sheet and be entered as initials within pleadings instead. Sometimes an indictment has many counts that do not differ except for the juvenile's name. The possibility for error and consequences of error could be great by moving between a separate data sheet and the pleading. Furthermore, a notarized or sworn document or any document that might be presented as evidence should not have blanks in it. Sally emphasized that the Maricopa County Attorney's Office must have a complete, original document.

Jamie Mabery, Division Chief, Maricopa County Attorney's Office, Victim Services explained that they must have time to notify a victim before anything gets out to the public in real time. Also, her office must be certain they have the proper name of the victim, therefore, using initials could be a problem. She also mentioned that victims' family members have complained about their names appearing in minute entries available through the Clerk of Court's website.

Mel Bowers, Navajo County Attorney, explained that his office has always identified juvenile victims by initials only in pleadings. Defense attorneys comply with this procedure also. The process has worked well for Navajo County. When a juvenile is the defendant, rather than the victim, Navajo County uses the juvenile's full name in the indictment and other pleadings.

Rick Unklesbay, Deputy Pima County Attorney, explained that his office uses juvenile victims' names in pleadings and they have not had a problem with this system. The media traditionally has not reported the juvenile's name.

Discussion ensued as to using a juvenile victim's name. Comments included:

- We need to maintain a case file with all information in it. We should just not put this information online.

Jim Belanger, President of Arizona Attorneys for Criminal Justice explained that he defends death penalty cases and is concerned about the ability to investigate these cases properly, long term. He said that he needs to be able to access information within a case 15 years out.

Jim also talked about the Federal Court PACER system and explained that this system is invaluable to attorneys. Once registered, a person can go online and pull information from all 50 states. There is a nominal charge for use of the system, which is handled by an outside service.

Discussion ensued as to additional concerns with sensitive data in criminal and juvenile matters:

- Some limited jurisdiction courts would have to double the number of their employees if criminal case information is not available online.

- Conversely, courts would need an army of staff to redact sensitive data and may be subject to liability if something is missed, unless they have immunity.
- Also, the paper file is not always available for inspection, since the judge, the attorneys, or the court reporter may have the file.
- The choices available for consideration as to how criminal records should be handled are: 1. Criminal documents go online with some specific documents not available online or a redacted version available online; 2. No criminal documents are placed online; 3. All criminal documents are placed online, without redaction; 4. All criminal documents are placed online but are available only to select groups.

III. Roundtable discussion of the issues

The following issues and concerns were raised during the committee's roundtable discussion of the issues to date:

- The original court record must be accurate and secure. The question then becomes: How do we disseminate this record? Redacting a document is much more complicated than controlling data elements online. I support a hybrid approach of limiting certain documents and certain fields from online access and possibly providing levels of access to dissemination. We cannot keep everything in the courthouse, and we cannot put everything online.
- What if we start by providing the record, online, to trusted stakeholders i.e. attorneys and parties in civil and criminal cases, then expand to other trusted stakeholders in these cases? There should be certain documents that do not go online at all. We could take steps in this process. If these first steps work well, we could expand access to the general public. Furthermore, if we attempt to put all records up at once, we could crash the network.
- We could use a registration process, starting with the bar and parties. Then we could move out with the registration process to others.
- Online access should be restricted by the intended use of the record e.g. bulk, electronic viewing, etc. We should not say that some members of the public can have online access and some cannot. The public can always have access to a file at the courthouse.
- Maricopa County is willing to provide party addresses from an individual file, but not in bulk.
- If Lexis-Nexis is required to look at individual case files in Justice Court to obtain an address, and pay \$17.00 per file, this creates a chilling effect. We can obtain the address, but it is not practical to do so.
- Maricopa County Justice Courts charge commercial users \$17.00 to access up to 10 files at one time.
- Specialized reports should come from the supreme court. The individual courts do not have time to deal with this.

The Chair explained that he will ask committee staff to prepare various proposals for the committee to vote on. He wants a record of the votes so that the Chief Justice is aware of what was, and was not, unanimous.

V. Call to the public

Chairman, Michael Jeanes made a call to the public. No comments were presented. Meeting adjourned at 2:00 PM.

Next Meeting: Tuesday, April 29, 2008, 10:00AM – 2:30 PM, Supreme Court Building, 1501 W. Washington, Phoenix, AZ, Conference Room 119 A & B.

**ARIZONA SUPREME COURT
RULE 123 AND DATA DISSEMINATION ADVISORY COMMITTEE**

MINUTES

April 29, 2008
Supreme Court Building, Phoenix, AZ

MEMBERS PRESENT:

David Bodney
Dave Byers, Vice Chair
Janna Day
Don Jacobson
Hon. Michael K. Jeanes, Chair
Catherine O'Grady
Sue Bunnin for Hon. R. M. Resnick
Patricia Sallen
James R. Scorza
Hon. Peter B. Swann
Karen Westover

MEMBERS ABSENT:

Patricia Noland
Terry Stewart
Hon. John S. Taylor

GUESTS:

Jennifer Greene
Therese Martin
John Moody
Rose Adams
Regina Kaupanger
Phil Knox
Don Thomas
John Barrett
Grace Colosimo
Sally Wells
Teresa Jennings
Dorrian Jones
Rich Robertson
Kevin Klimas
Mark Osborn
Janet Scheiderer

**GUESTS APPEARING BY
VIDEOCONFERENCING:**

Tom Clarke

STAFF:

Tama Reily * Melinda Hardman

I. Call to Order

Chairman Michael Jeanes called the meeting to order at 10:05 a.m.

II. Approval of Minutes

The minutes from the March 11, 2008 meeting were presented for approval.

MOTION: To approve the Rule 123 and Data Dissemination Advisory Committee meeting minutes for March 11, 2008. Seconded. Motion approved unanimously.

III. Discussion of Draft Policies

The committee discussed a draft policy of a pilot program for online access to civil and criminal case records. The draft policy provided that civil and criminal case records may be made available online to all parties, members of the State Bar of AZ and their staff, and private investigators, except that certain, identified documents would not be made available online due to the likelihood that these documents contain sensitive data. Online access would require registration and use of a user name and password. Simultaneously, use of a sensitive data sheet would be required with any new filings, with the expectation that eventually all civil and criminal case records could be placed online, once use of the sheet becomes routine.

Discussion ensued regarding the proposal. Comments included:

- The Weisberg Committee of 2002 concluded that a sensitive data sheet must be in place before documents are placed online.
- Maricopa County currently provides online access to case records to attorneys and parties in their case, however anyone can also access case records at the courthouse. Online access requires a registration process in which the user must provide an AZ drivers license number – which is sent to MVD for verification.
- Use of a sensitive data sheet is not realistic. Sensitive data will never be thoroughly extracted from case records.
- Providing case records, online, to a special group such as private investigators, cannot easily be monitored.
- The documents restricted from view in the proposal were identified by a sensitive data workgroup in January 2008. By comparison, the federal PACER system is not restrictive and displays most case records online.
- The proposal is too restrictive in terms of persons allowed to inspect the records and records provided for access. We should not require appearance at the courthouse to view records. There are categories of records that should be kept from the public, but these are few and far between. Certain elements, such as Social Security numbers, bank account numbers, and credit card numbers should be kept out of records. Members of the public who must drive a long distance to the courthouse should be able to access case records remotely. The convenience given to attorneys should be extended to others. There should be a reasonable fee for this convenience, and it should require logging in so we know with whom we are dealing.
- Maricopa County only keeps sealed records from the attorneys and parties. Everything else is available to them online for their own cases. When access is given to one attorney in a public or private law office, the entire office is granted access. Maricopa County has not experienced any problems, to date, as a result of this program.
- Identifying specific documents to keep from users would be an administrative nightmare.
- Perhaps we could provide access to case records, online, through a registered user process, with three levels:
 - Attorneys and parties could have complete access.

- Registered users (e.g. AZ residents) could have open access, although some documents would need to be limited from access. A fee for use could be imposed.
- Public access to court calendars, dockets, and case lookup could be free.
- We need to be careful with the definition of “case record.” Is this a document, a data element, etc.? Furthermore, we should not tie our hands that public internet access to dockets and calendars would always be free.

IV. An Overview of Data Sharing Between Courts and Law Enforcement around the Country

Tom Clarke of the National Center for State Courts gave a presentation on trends and issues in justice information sharing across the country. He reported that typically excluded data in the sharing process include SSN, account numbers, and addresses. Additional categories that are sometimes excluded are victim, witness and child contact information; medical records; custody evaluations; financial information; pre-trial and pre-sentence investigations; and search warrants. Additionally, there is a trend toward more sharing of bulk data. In order to place court records online, a state should probably operate with multiple layers of precaution, including educating people not to include sensitive data in court documents, prohibiting certain documents from being placed online at all, etc. No major state has been fully successful in redacting sensitive data.

V. Information Sharing with Justice System Partners – a look at the Integrated Criminal Justice Information System (ICJIS) for Maricopa County

Don Thomas, Director of ICJIS, John Barrett, IT Director of ICJIS, and members of the initial development team and current business team for ICJIS provided an overview of the creation and governance of the Maricopa County project.

They explained that Maricopa County had been looking for a method to share data without creating a data warehouse and without compromising each partner’s IT system. Funding for ICJIS was derived from a voter approved sales tax. Development of the philosophy and governance documents was the hardest part of the project. ICJIS must be viewed on three layers: a policy level, a business perspective, and the technology, but the middle level must drive the project. Data is distributed through a governance and rules-based process, and recipients update their systems through this process. ICJIS does not look at documents as a whole. It looks at all of the data elements within a document. Then, for each data element, a decision is made as to the point in time the data element can be shared, who can have it, and under what circumstances it can be shared. Statewide standardization is helpful in developing a policy on data sharing. The template that ICJIS developed for the data sharing process is attached to the ICJIS Criminal History and Privacy Impact Assessment for Inter-Agency Data Exchanges document. Memorandums of Understanding are of limited value in this process, because once the data is out there, there is no way to get it back. Most of the data that is presently exchanged through ICJIS was previously exchanged in paper format.

VI. Roundtable discussion of the issues

(See Discussion of Draft Policies, above.)

VII. Call to the public

Chairman, Michael Jeanes made a call to the public. Rich Robertson stated that private investigators should be granted online access to case records because private investigators are identifiable and accountable. They could be granted access using a similar system as MVD, requiring registration each time the user goes in to obtain records.

Meeting adjourned at 2:25 PM.

Next Meeting: Tuesday, May 29, 2008, 10:00 AM – 2:30 PM, Supreme Court Building, 1501 W. Washington, Conference Room 119 A & B, Phoenix, AZ.

ARIZONA SUPREME COURT
RULE 123 AND DATA DISSEMINATION ADVISORY COMMITTEE

MINUTES

May 29, 2008
Supreme Court Building, Phoenix, AZ

MEMBERS PRESENT:

Dave Byers, Vice Chair
Carol Schreiber (for Hon. Michael Jeanes)
Terry Stewart
Catherine O'Grady
Patricia Sallen
Hon. Rachelle Resnick
Hon. Patty Noland
Jim Scorza
Joan Harphant (for Don Jacobson)
Karen Westover
Janna Day
Hon. John Taylor – telephonic
David Bodney

GUESTS PRESENT:

Jennifer Greene
Mark Jensen
Rich Robertson
Regina Kaupanger
Laura Spain
Grace Ku
John Moody
Theresa Barrett
Mary Jane Gregory
Kevin Klimas
Diane Stubbs
Mike Goss

MEMBERS ABSENT:

Hon. Peter Swann

STAFF:

Tama Reily * Melinda Hardman

I. Call to Order

Vice Chair, Dave Byers, called the meeting to order at 10:05

Committee members and guests introduced themselves.

II. Approval of Minutes

The minutes from the April 29, 2008 meeting were presented for approval.

MOTION: To approve the Rule 123 and Data Dissemination Advisory Committee meeting minutes for April 29, 2008. Seconded. Motion approved unanimously.

III. Discussion of Draft Policies

Pilot Program for online access to civil & criminal case records

Dave Byers recapped the committee's last discussion on online access to civil and criminal case records which led to the current draft policy proposal that states that online access for civil and criminal cases can be made available to the attorneys and parties in a case and to residents of Arizona who have a Department of Motor Vehicle issued drivers license or state identification card and a valid credit card. The thought process is that Arizona residents are subsidizing the infrastructure of this system through their taxes, this is a reasonable first step in making these records available online, and if there would be a problem, there would be some control over local residents of Arizona. Jim Scorza noted that a third category had been proposed for parties and the attorneys associated with those parties to have access to some documents that would be excluded from the public. The practicality and logistics of this option require further consideration.

In Pima County, documents are categorized and coded by document type as they are indexed. Then the computer is instructed to display or not display according to document type. Onbase is capable of doing this as well, however the codes used by the Clerks' offices are not yet standardized, so there should be prospective application of this proposal only.

The documents that the draft policy cites as "not accessible" to the public were raised for discussion. Pima County identified the documents the Committee might consider for exclusion from the public based on the documents their office customarily sees. Booking related documents do contain a lot of sensitive information, but many booking agencies and police departments are now redacting social security numbers and other sensitive information. Booking documents are hard to restrict since they are not indexed as a separate item – generally they are attached to filings. Subpoenas and warrants contain social security numbers. Pre-sentence reports not only have social security numbers but also have victim information, mental health information, allegations by defendants and information about families. Defendants' financial statements contain sensitive information. Terms and conditions of probation documents generally do not contain personal information. Orders of protection are excluded from the policy by definition.

Discussion followed as to other concerns about non-accessible documents. Comments included:

- If a sensitive data sheet is not going to be used in criminal cases, could there still be some effort toward protecting the identities of sex crime victims by restricting or excluding cases involving sex crimes? Judge Weisberg's committee was concerned about the identity of juvenile sex crime victims.
 - There is no distinction made between the criminal cases of juveniles and adults, nor between criminal cases involving sex crimes and other types of criminal cases, so this request cannot be achieved.
- The terms and conditions of probation document should be made accessible to the public.

- Courts could be asked to eliminate sensitive information that has traditionally been included in these documents. This could eliminate the concern about many documents on the list.
- The Department of Public Safety is concerned about the 8-digit number assigned to an individual, which appears on the disposition report.
 - This item can be flagged for further review
- Rich Robertson of the Arizona Association of Licensed Private Investigators commented that this policy would only be restricting the online access to people who are required to register anyway, so all the concern about sensitivity and misuse of this information is potentially only by people who have not registered with the system.
- Who is meant by the “attorney.” Is this the attorney and the attorney’s related professionals, paralegals, and investigators?
- A representative from the Child Support Enforcement Section of the Attorney General’s office asked whether the Committee has considered input from institutional litigants, such as the public defender’s and county attorney’s offices. Her concerns were that the AG’s office needs to research children in ancillary cases where the AG’s office is not a party. They use Onbase and Agave to do that research now, but are concerned this proposal will curtail their ability to acquire information.
- Pima County has had a working relationship with the Child Support Enforcement area, and because they are a government entity they are considered a justice partner. Access is limited to those cases they need to research.
- We need to preserve access and establish an authorization process for other (probably government) entities that have legitimate business to conduct.
- Pima County noted that their office is careful to limit access to certain persons within a government entity so that access is not available agency-wide. Approval is granted from a specific internet address.
- John Moody, a private attorney, asked whether a fair distinction is being made between public and private attorneys since people within the public defender’s office, the county attorney’s office and law enforcement would have broad access, but private attorneys, with similar research purposes, would not.
 - Public defenders, private attorneys, and justice partners would only have access to their cases.
- Maricopa County stated that their current system for justice partners with access to Onbase records does not restrict them to just their cases. They have access to the electronic court record as a justice partner. The pilot Maricopa County is running right now for remote online access for the attorneys of record is set up differently than access for justice partners. People from trusted agencies are Onbase registered users, as opposed to coming in through the internet. These agencies work across multiple case types and since they are government agencies, they have been given the same access as if they came down to the public counter.
- Pima County provides access to government agencies that have specific duties and sees that simplifying their access to records is a savings all around. The level of access is determined by the area within which they work. The county attorney’s office, which covers criminal, civil, probate, and other types of cases, might be given total access, while other agencies are typically more limited in their access.

- Pima County noted that they actually do restrict some of the documents mentioned from even the justice partners.
- Pima County clarified that the proposed policy would allow registered, Arizona residents who pay a fee, including attorneys and parties who register in this manner, would be given access but would not be given access to the excluded documents.

The Vice Chair concluded that there appears to be a general consensus of the elements of this plan and called for a tentative vote to adopt a working draft of the policy, which is conceptualized as follows:

For criminal and civil cases only (the sensitive data sheet would be in place for civil cases), with excluded documents as articulated above, remote access is granted to persons with Arizona identification and a valid credit card, to trusted government entities and potentially other agents based on their legitimate need, and to persons who physically come to the court and view everything that is not otherwise sealed or redacted. Fees are yet to be determined. Parties and attorneys of record are granted free access to their cases.

Note: Although the committee wishes to include victims along with the parties and attorneys of record, current logistics and technology prevent the ability of establishing victim status.

A request was made to include transcripts on the excluded documents list. Transcripts are not offered online by any courts yet and that transcripts are owned by the court reporter. Presently, the draft policy's definition of case record includes transcripts, so it would be better to add transcripts to the excluded document list. According to earlier discussion, excluded documents would be:

- booking-related documents
- warrants
- charging documents
- pre-sentence reports
- defendant's financial statement
- disposition report
- transcripts

MOTION: To approve as a tentative concept the policy as described herein. Motion seconded. Approved unanimously.

Further discussion continued on the policy for remote online access to civil and criminal case records regarding the definitions. Comments included:

- It would be best to use the definition of "case record" found under alternative #2, which states "any pleading or document that has legal relevance to the adjudication of any aspect of a case."
- Is criminal traffic also intended under the definition of "criminal case," which presently only cites Title 13? Also, does the definition include alcohol offenses under Title 4?
 - These clarifications will be made.

- There is a problem with the case record definition under alternative #2, because of the phrase “legal relevance.” It creates an issue of who would make the determination as to what is legally relevant. Alternative #3 seems preferable because it is clear about what is included.
- We will probably need to substitute the new definition of “case record” for the definition currently found in Rule 123.
- The record that we are talking about is the record of “the case,” not probation records, or administrative papers, you could use the definition in #3, i., and add the term “generated” following “any document that is collected, received...” Adding this term eliminates the need for #3, ii.
- We could leave off the term “generate,” which eliminates this problem of being overly broad, and specifically list those documents that the court generates. We could then add on to the end of #3, iii a qualifier such as “associated with a case,” or “in connection with a judicial proceeding.” Members agreed that this last alternative was a good working definition to go forward.

Proposal for bulk/compiled data access:

Jennifer Greene summarized the proposal for a bulk/compiled data access. The definitions for the two types of data were borrowed from similar policies from other states. The requirements described in the proposal are based on a data dissemination policy used by Washington State. The only requirements are providing proof of identification and willingness to enter into the agreement as specified for that data.

The elements of the agreement as described in the draft proposal were discussed. Comments included:

- What is the concern about data being distributed in bulk to third parties?
 - It would allow for the possibility that non-legitimate parties could end up with the data, for example if the data is provided to Lexis-Nexis and they sell it to a third party.
- The proposal seems a bit too broad. What are the benefits of making the data broadly available to the public? Re-dissemination could be managed through the dissemination agreement in terms of binding the requestor to be responsible with that information.
- Regarding Bullet 2, which requires the recipient to have its customers sign a disclaimer as to the accuracy of the records provided, causes concern. These companies take the information and add to it a national database, or information derived from other sources, and that is what they pass on. So, because the information becomes co-mingled with other sources, it becomes difficult to put the disclaimer in.
- The firms disseminating information are going to have their own disclaimers which may more accurately reflect the nature of their data than merely duplicating the court’s disclaimer.
- It seems that it would be important to require the court’s disclaimer to be passed along only if the data is re-disseminated in bulk.
- Bullet 3 should more clearly state that it is the bulk database that should not be made available on the internet. If someone wants to extract certain information, and then make that available on the internet, they can do that.

- Maybe we should prohibit someone from taking court data, completely, and selling that. Once a person has the bulk court data, the person should be able to prepare reports, compile data, and add value.
- What we're trying to protect really, is a copyright interest, in the sense that the court can produce an original document/work and say that no one else can reproduce it as is – but, if you alter it a bit, then you can use it. It is risky to treat public information as a copyrightable thing that can only be borrowed, in part, safely.
- A number of the vendors want the courts to provide complete home addresses and identifying information that we do not display in our case lookup systems. Our policy must be that if we are going to give that home address and/or social security information, we do not want the vendor to turn around and display it on the internet. We need to state precisely what that information is, i.e. home address/social security number or other personal identifiers, and indicate that the information can be used for record matching purposes, but it cannot be put on the internet or on a mailing list.
- Bullet 4, which prohibits data from being resold for commercial solicitation, addresses this same point. Under this proposal a person or entity could buy the data but could not use it to send solicitations.
- Bullet 5 means the user agreement would stipulate that the Supreme Court or other court can audit the recipient of the bulk or compiled data if there is a question about the use of the data. The audit would only cover the items under the agreement.
- Bullet 6 simply requires an indemnification agreement.
- Bullet 7 describes a liability insurance requirement of \$1/\$2 million for misuse of the data.
- Should there be a distinction between misuse of information obtained in bulk versus an individual record? Perhaps – because this agreement is with commercial users.
- Maybe we could allow compiled data access to researchers or scholars under a different type of agreement.
- One effect that could come out of a liability insurance requirement would be to limit the field of who would be entering into this contract. This item will need further discussion.
- There is a provision of the public record law that permits people to come to an agency and make copies themselves if the agency does not have the equipment/staff to make the copies. The equivalent for this might be that if a person is prepared to bring in the staff to underwrite the cost to research records in a court, this may be a good solution. This could also be done by a third party.
- We need to better define the term “bulk.” If someone asks to inspect ten records, could that be viewed as a bulk records request?

The Vice Chair suggested that the committee think about these concerns and the possible alternatives for the policy between now and the next meeting.

The updated schedule for meeting dates was presented and there were no objections to the schedule.

IV. Call to the Public

Meeting adjourned at 1:40

Next meeting: Tuesday, June 24, 2008, 10:00 AM – 2:30 PM, Supreme Court Building, 1501 W. Washington, Conference Room 119 A/B, Phoenix, AZ.

**ARIZONA SUPREME COURT
RULE 123 AND DATA DISSEMINATION
ADVISORY COMMITTEE**

MINUTES

Tuesday, June 24, 2008

MEMBERS PRESENT:

Hon. Michael Jeanes
Dave Byers
David Bodney
Janna Day
Don Jacobson
Catherine O'Grady
Rachelle Resnick
Patricia Sallen
Hon. John Taylor
Hon. Eileen Willett (for Hon. Peter Swann)
Karen Westover

GUESTS PRESENT:

Alan Carlson
Peter Swire (telephonic)
Jennifer Greene
Mark Jensen
Therese Martin

MEMBERS ABSENT:

Hon. Patricia Noland
James Scorza

I. Call to Order

The June 24, 2008 meeting of the Rule 123 & Data Dissemination Committee was called to order by Michael Jeanes, Chair, at 10:05 am.

Members and guest presenters introduced themselves.

II. Approval of Minutes

The minutes from the May 29, 2008 meeting were presented for approval.

Motion: To approve the minutes from the May 29, 2008 meeting of the Rule 123 & Data Dissemination Advisory Committee as presented. Seconded. Approved unanimously.

III. Privacy Concerns of Litigants, Victims, Witnesses, and Others

Two privacy experts spoke to the committee about public access to court records, privacy concerns, and some of the legal elements involved.

A. Alan Carlson, President of the Justice Management Institute, discussed some of the main concerns that have been created with the advent of electronic access to court records. In addition to identity theft, he pointed to the issue of mistaken matching of individuals to information, such as might occur where similar/same names are shared by different individuals, and concerns that are specific to criminal case records.

The following concerns and comments were raised regarding Mr. Carlson's presentation:

- If a judge seals the criminal record of an individual who later applies for a professional license, potential clients/patients could have a legitimate concern about such information having been kept from them.
 - One way to prevent that situation would be to make the criminal record available only to law enforcement, licensing agencies, and/or other relevant entities, but not the general public.
 - But that creates policy issues such as who gets to have access and under what circumstances.
- Part of the problem with electronic records is that they do not go away. Even if a record is expunged or sealed, there is always the chance that the information has already gone into some type of public or commercial database beforehand.
- What is the state of the law on expunging records in Arizona?
 - If you are a juvenile offender and you stay out of trouble, you can have your juvenile record sealed, but as an adult criminal you have to show malicious prosecution to get your record expunged.
 - If a juvenile record is expunged, it will still show up on a background search.
- Are there states in which you cannot see a criminal case record online?
 - Some states allow you to see criminal case records at the court but not through the State's criminal history system.

B. Peter Swire, Law Professor at Ohio State University and former Chief Counsel for Privacy Issues for the Clinton Administration addressed issues of legality and specific considerations regarding what information should be public and what should not. He also talked about the need for different industries to develop their own procedures for privacy management, such as was done in the health care field where HIPAA standards were established to protect patients' medical records.

Questions and comments included the following:

- It does not make a lot of sense for the courts to suppress some information, such as date of birth, when that information is so widely available in a variety of ways.
 - We need to keep in mind that some of this data can serve as "keys" that allow access to further information on a person's identity. And, while we are on the verge of date of birth becoming much less useful, until there is a "next generation" method, criminals will continue to use what has been working up to this point.
- Who has responsibility when the information of an individual was made publically available and someone commits criminal activity using that individual's identity?

- It falls on the county records offices from which the information came. There should be clear procedures and an obligation on the local courts to manage these types of situations when they occur.
- We cannot come up with a general rule though that applies across the board, because there are so many different circumstances in individual cases. It needs to be looked at on a case by case basis.
- The rule then could be that each court must establish a process that a citizen can petition the court to have records changed.
 - There is a model for this under the Fair Credit Reporting Act, where the debtor or individual challenges an item on his/her credit report. In this act there are procedures in place to allow this to be handled on a case by case basis. It is a fundamental right for people to have the opportunity to clear their name when it has been incorrectly represented.
- There do not seem to be any rules or requirements for courts to have procedures to correct records in these situations.
 - The original Weisberg Committee did have a proposal to add a provision to the rule that sets out an administrative process for correcting records that are displayed online.
- Some people have a perception that there is a duty on the part of the court to make records available on the internet, and there are others that say this is a matter of convenience that we are trying to provide to citizens within our state.
 - It could pose a problem that you are excluding other states from access to online records in Arizona. For example, the media might challenge this practice in a high visibility case. If it was challenged under the Dormant Commerce Clause, it would be helpful for the Committee to have established a basis as to why it is making information available online to only this group of people, because you are treating Arizona citizens differently from non-Arizona citizens.
 - Just articulate what your policy is and why; include a statement that says it is not having any impact on the access to court records, nothing has changed, it has been that way ever since Arizona became a state.
 - There is also an economic aspect to our limiting availability to Arizona citizens; they are the taxpayers paying for the system, the records, and the display of those records.
- If there is going to be a charge for accessing records online, the money received should go back to the entity paying for the system.
- The Dormant Commerce Clause should receive further thought because of the economic ramifications and the business that surrounds this information. If a rule specifically provides a benefit to an Arizona citizen that is not at all provided to out of state citizens, and there is a business generated from that, then it is discriminatory on its face.
- A similar concern was at the root of discussion on the meaning of A.R.S. § 12-304, which exempts state and local governments from having to pay fees in courts. The statute excludes federal agencies. There are attorneys on both sides of the issue with regard to whether the federal government should be charged. Research into the legislative intent of the statute found that the intent was specifically intended to exempt state and local government from fees because the Arizona taxpayers pay for the judicial system in this state, and this excludes the federal government.

- But your example falls into the market participant exception of the Dormant Commerce Clause, which allows the state and local government to participate if they are the consumer of the information.
- If we cannot restrict the information, then we may need to return to having nothing available on the internet, and anyone who wishes to view records would need to come to the courthouse, or request records in writing via mail.
- In this era of technology, that may not be acceptable to a lot of people. There is also some value, from the courts' and clerks' perspectives to allowing internet access because it cuts down on traffic in the offices.
- We also have the law that was passed a year ago by the state Legislature which requires that minute entries of all criminal cases be available online by 2010.
- Are there any studies out there that have looked at the efforts of other states and the impact their actions have had on the concerns we are discussing?
 - There are not really any compiled facts about other states. We would have to look at each state separately to obtain information on their procedures/results because no one is compiling all of the states' data. What tends to happen is the most recent state that has developed a new rule is where we find the most recent research.
- What are the most realistic privacy concerns/dangers we should be aware of and how could we address them?
 - As background checks continue to proliferate and as it is harder to live life without proving identity, there will likely be increased cases of stolen identities and criminal acts committed under stolen identities. Court records are one of the areas vulnerable this.

III. Roundtable Discussion

Proposal for Removing Sensitive Data:

Melinda Hardman provided a review of the current draft proposal for removing sensitive data from case records, and a brief explanation of how today's draft came to be. She noted that while previous discussion by the committee had suggested excluding criminal cases from the proposal, they remain in today's draft for further direction from the committee. Items, (a) through (d) in the first paragraph were drawn from the process used in Oklahoma. The second paragraph, concerning the filer of the sensitive data sheet, is based on the provision currently in effect for the Arizona Family Law Rules. Paragraph 3 was derived from the recently issued report by a New Jersey committee which suggested that in lieu of a sensitive data form there would be a certificate on the initial pleading to remind people to be cautious of what they were filing. Paragraph 4, which addresses redaction of sensitive data, stemmed from the committee's earlier discussions about the lack of time and resources available to courts/clerks to take on responsibility of redacting information. The last portion of the proposal involves enforcement of noncompliance and the sealing process, and this will need further direction by the committee.

The following issues and concerns were raised regarding the sensitive data proposal:

- Does the proposal apply to law enforcement and civil traffic citations?

- Yes, due to the fact that the clerks do not have the ability or the manpower to do the redacting.
 - If that is the case, it would have a significant impact on electronic filing for field citations and would require rule modifications in other areas.
- Can the clerk’s office make redactions in cases of noncompliance by courts/council, perhaps with a fee attached?
 - The clerk’s office cannot make modifications to original records without a court order.
 - Can we change that by writing a new rule/policy to allow sensitive data to be redacted without a court order?
 - Any policy such as this would need to be carefully crafted; a judicial officer is the appropriate party to make determinations about whether to redact an original court record.
- California passed a statute that allowed the court to create a “public record” that was distinguished from the “official record;” the public version being the redacted version. This is another option to consider.
- We need to clarify whether there is a distinction between *modifications* and *redactions* of a court record.
- In terms of modification versus redaction, the Maricopa county Recorder just spent in excess of \$5 million to go through and *redact* social security numbers out of electronic records that date back to 1935. However, the original hard copy records were not modified and remain intact in the Recorder’s Office.
- Making any modification to a court record without a court order is a Class 6 felony.
- Maricopa County described a 20 year old probate case in which the court ordered a redaction of the “original” record, so the original, *as filed*, no longer exists. In its place is a modified “original,” pursuant to court order. Today, since documents are scanned, this process would be carried out by printing the scanned electronic version of the original copy as it exists in the system; the electronic version would then be deleted from the system. The newly printed copy could then have a social security number blacked out, be rescanned, and become the new original record.
- We need to be alert to the fact that there could be victim information in civil lawsuits that are filed as a result of a criminal act.
- The Arizona Traffic Ticket and Complaint (ATTC) form provides all the key information for identity theft, including social security number, drivers’ license number, date of birth, address, and phone number. The proposal that was put forth in an earlier rule change petition, which addressed the ATTC separately, was that the person filing an ATTC would be exempt from the sensitive data requirement. We have since heard other objections to using the sensitive data sheet from the Maricopa County Attorney’s Office.
- For juvenile victims of sex crimes, we could carve those cases out from our pilot project, and simply not display those kinds of criminal records online.
- The issue might be resolved by changing the definition we are using for criminal cases in our electronic access policy. On the civil side, where people tend to be represented by attorneys, we could hope for some success by introducing a procedural rule. However, as we heard previously from prosecutors, it becomes more difficult in the criminal arena due to the implications of reading the wrong version of the pleading, when there are redacted and un-redacted versions. This raises the possibility of appellate issues.

- Michael Jeanes will look into the process of sealing of the records and how this could be accomplished.
- If we are going to recommend a rule that forbids public access to certain kinds of information, we should have a provision based on some requisite standard or compelling need that allows for a member of the public to petition the court to have the information unsealed.
- However, there needs to be evidence that a record does exist.
- The original Rule 123 states:

“the sensitive data form shall be accessible by the public only on a showing of good cause, pursuant to the administrative process set forth in Rule 123. Good cause may include access by a media representative for purposes of research on a news story.”

- The sensitive data proposal states that “the sensitive data sheet shall be confidential.” The form that was devised in Maricopa County says “confidential,” and instructs parties not to send a copy to the other party in the action. Maybe we could clarify that it is confidential but will still be served on an opposing party.
- Why does the other party need the information?
- The judge has access to the information on the form, so it does not seem necessary for the opposition to have it.
- Maybe we need to notify the opposition of the *category* of information that is marked as sensitive, rather than revealing the actual information.
- Is the sensitive data sheet intended for all civil cases? For our purposes, maybe we need to better define what a civil case is. For example, does it include probate cases?
 - The definition we are using for civil cases is the one we established in the Remote Electronic Access Policy (provided in today’s meeting materials), which excludes family court, probate and so forth. The sensitive data policy would apply to the Rules of Civil Procedure.
- We might need to draft the sensitive data sheet or some key provisions of it, because what we are doing is giving civil litigants a notice that says “in the course of this civil litigation, you may be obliged to file certain sensitive information, or you may choose to file certain sensitive information, or you may inadvertently file sensitive information. You are hereby on notice that the following information shall not be filed unless otherwise ordered by the court, and then list those items. . . .”
- What is the basis for excluding criminal cases from the sensitive data protections? While we are removing juvenile victims’ files completely, we are leaving adult victims with their addresses and telephone numbers accessible to the general public.
- Maybe we need to consider two different policies, one that deals with civil, and one that deals with criminal cases. The criminal side could focus on victim information, not on social security numbers.

Michael Jeanes, Chair, suggested that, as there seems to be some consensus that we need to consider sensitive data concerns in each civil and criminal cases, Melinda and Jennifer will work on redrafting the sensitive data policy to address criminal and civil cases separately.

Proposal for a Policy to Govern Distribution of Court Records to Criminal Justice Courts:

Jennifer addressed the committee on this draft proposal which borrows from existing policies as well as the recommendations from other states. Right now under Rule 123 public agency employees whose agency has some statutory basis for looking at non-public court records, can access those records. In practice, we also share confidential records with treatment agencies, federal probation offices, and other law enforcement agencies under that policy. The intent of this proposal is to have a more specific policy for sharing case records with other public agencies.

Some of the other states have distinguished between law enforcement and other kinds of public agencies. The agencies would be required to enter into non-disclosure agreements with the record custodian that ensures that everybody at the outside agency understands the confidential nature of what they are accessing and that they must observe certain restrictions on re-dissemination. This borrows from the kinds of policies we already have in place that permit our probation officers to look at the Department of Public Safety Criminal History Records database but is not quite as strict.

Questions and Comments on the proposal included the following:

- Is the purpose of this proposal to allow a broader access to those agencies which we have identified as public purpose agencies that may not have had access to the information previously?
 - Yes.
- Does this apply to bulk and compiled data?
 - No, just case records, whether paper or electronic.
- It is key to be very clear about what we mean by *record*. Is it documents or data? We have not been consistent with our definitions - we need to go back and make sure we are consistent throughout all of the policies.
- So, would this policy govern a University professor who is doing research in a certain area, or is he/she governed by the bulk data policy?
 - He/she would be governed by the bulk data policy.
- What about public health and/or public protection agencies? Should we add them to the policy?
 - Perhaps A(2) covers what you are asking
- It seems like it would be clearer to say public safety or public health.
- What about non-profit organizations that are non-governmental?
 - Maybe just remove the word “non-profit” under A(2) and just say “or an organization whose principal”
 - But, the definition seems to become too broad this way.
 - Maybe we could say governmental or quasi-governmental agency...
- In the beginning of this Committee’s work, some presenters made a clear distinction between the bulk data vendors and those entities working on government-related matters. That is the reason this proposal was developed separately.
- In order to release certain files currently, for example, juvenile files, we have to have a court order. These are often the types of records that ASU wants to access. So, some of this is already taken care of in other manners.

- There is also the issue of volume, because many of these requests are such large volumes of work, and this proposal does not allow us the option to decline the request on the basis of workload.
- It seems like we cover some of these issues in the proposed bulk data policy, under section C, which addresses denial of requests for data.
 - But we could limit eligibility to government or quasi-governmental agencies and for purposes of law enforcement or other purposes that are of benefit to the court.
- Then where do you put public defenders and county attorneys?
 - They would be included in this proposal.
- The problem with that is then you are treating public attorneys differently from private attorneys.
 - If there is concern that this creates a disparity, could we just draft a sentence to include those private attorneys?
- What should be done about grand jury indictments and search warrants that have not been sealed?
 - There are statutes that apply to those matters, as far as when they are public and when they are not.
 - Maybe we need to add a comment to the policy to clarify this.
- What would prevent a media representative from requesting records for purposes of research if they signed the disclosure statement?
 - I think the definition needs to be more restrictive in terms of the purposes for the records request. For example, anything court-related is legitimate.
- Under what authority are the inter-governmental agreements and inter-governmental systems presently operating for the sharing of information?
 - There are statutory allowances for intergovernmental agreements that delineate all the specifics of financial and data transferring information.
- So, under what authority does the court enter into those kinds of agreements?
 - A.R.S. § 11-952.

At this point, the Chair stated that the policy will be redrafted, taking into consideration the comments and concerns discussed today, and reviewed at the next meeting. Some additional comments regarding other policies were made:

- On the remote access document, section B(4), where it says “any federal, state, or local government entity may be provided remote electronic access at no charge...” there may be a conflict with 12-304. It also creates a question, when we are talking about an exception court, whether it is a federal, state, or local entity, and we do not have to charge them, how do we verify that they are that entity?
- Also on the remote access document, section A(2), where the last sentence cites A.R.S. Title 14, can we add A.R.S. 32, because that also governs probate matters?
- There has been some concern voiced by judges of superior courts that we may not have included all necessary documents on the “not accessible to the public” list. Can we have someone pull a criminal case file to do an inventory of the file just to be sure?
- With regard to consistency, another thing we should think about is that in some instances of the e-filing system, we are saying, “Do not share your password with anyone.” But in

others, a law firm for instance, we imply it is okay to share your password with legal assistants. That can be confusing.

- Also, on the proposal for the bulk data, section A(2) of the definitions, the first sentence reads “custodian of court data means the person responsible for maintaining the court’s case management system,” but the case management “system” is what the AOC (IT) manages.

IV. Call to the Public

Chairman, Michael Jeanes, made a call to the public. No comments were offered. Meeting adjourned at 2:31.

Next meeting: Tuesday, July 22, 2008, 10:00am – 2:30pm, Supreme Court Building, 1501 W. Washington, Phoenix, AZ, Conference Room 119 A/B.

**Arizona Supreme Court
Rule 123 and Data Dissemination
Advisory Committee**

MINUTES

Tuesday, July 22, 2008

MEMBERS PRESENT:

Michael Jeanes
Dave Byers
Patricia Noland
Patricia Sallen
Karen Westover
Donald Jacobsen
James Scorza
Rachelle Resnick
David Bodney
Jana Day
Catherine O'Grady

GUESTS PRESENT:

Jennifer Greene
Carol Schreiber
Mark Jensen
Regina Kaupanger
Rich Robertson
Therese Martin
Mark Osborn
Carol Boone
Diane Stubbs

MEMBERS ABSENT:

Terry Stewart
Honorable Peter Swann
Honorable John S. Taylor

STAFF:

Melinda Hardman
Tama Reily

I. Call to Order

The July 22, 2008 meeting of the Rule 123 & Data Dissemination Advisory Committee was called to order by Michael Jeanes, Chair, at 10:05 am.

Mr. Jeanes discussed the Committee's progress in reaching its goal of presenting completed material to the Arizona Judicial Council (AJC) in November. Given the current pace, and the tight deadline, he suggested proceeding diligently while remaining conscious of the timeline. Whatever the final product, at the point it is believed to be ready for forwarding to the Chief Justice and AJC, he suggested making it available on this Committee's website, as well as forwarding it to other courts/entities for comment and feedback in order that

problems with implementation can be addressed prior to sending it to the Arizona Judicial Council.

Members were reminded of three articles Melinda sent out that deal with PACER, the Dormant Commerce Clause, and other topics concerning electronic information. Members were encouraged to look through the articles (website links were included) as they are applicable to the Committee's topic.

Catherine O'Grady briefed the Committee on what she found in her review of the Dormant Commerce Clause. The clause was described as an implicit restriction on states so that states' actions do not burden or discriminate against interstate commerce. Courts evaluate possible offenses by looking at a statute on its face and whether it favors in-state residents over out of state residents. The Committee's proposal could be construed as favoring in-state citizens; however, this could be overcome by the Market Participant Exception, which states that if the State is actually involved, not as a regulator, but as a participant in the market, then that would be an exception to the Dormant Commerce Clause. There are other possible arguments against the policy that could be made under the Privileges and Immunities Clause of the Constitution, as well as the Equal Protection Clause of the constitution, but it is more likely that the Dormant Commerce Clause that would be used to challenge the Committee's particular Rule.

Mr. Jeanes reminded the Committee that the proposal to limit online service/access to Arizona residents was simply a means for identification in the registration process, and noted that if it resulted in a potential offense of the Dormant Commerce Clause, there would need to be another process established. The Arizona resident limitation was also intended to offer some control over who has access to the records. However, as a preventative measure, a privileges and immunities analysis should be completed to ensure there is some rationale behind the in- state/out of state distinction in the registration process.

II. Approval of Minutes

The minutes from the June 24, 2008 meeting were presented for approval. It was noted that member Terry Stewart was not included on the member attendance list as being absent, and a correction was needed to the spelling of Hon Eileen Willett.

Motion: To approve the minutes from the June 24, 2008 meeting of the Rule 123 & Data Dissemination Advisory Committee with corrections as discussed.
Seconded. Approved unanimously.

III. Possible Amendments to Rule 123

Mr. Jeanes suggested the Committee review, item by item, the proposed amendments to Rule 123 (presented in today's meeting materials), and resolve those items that could easily be determined. Those that require more intensive discussion/study should be assigned to a workgroup for review. He noted that proposed amendment 9 would be addressed at the August meeting when Nancy Swetnam, AOC Certification and Licensing Director, will address the Committee.

1. Access to original transcripts. Comments and concerns for this item included the following:

- Transcripts do not get imaged, so they are not be part of the electronic case record.
- Maricopa County charges 50¢ per page for a typed transcript once it is filed in as part of the record.
- Should audio recordings be addressed?
- Audio recordings are included under Rule 123 because it covers “any media.”
- There are 2 separate recordings in cases. Some are used in lieu of a court reporter, others are used by the courtroom clerk to aid in completion of their minute entry. We should distinguish which is the recording of record.
- We have administrative orders that state that if there is either a court reporter, or the court is running FTR, then that is the official record. If the Clerk is doing something specifically for the minutes, that is not a part of the official record, it is just a working document for the purpose of producing minutes.
- But, since the other recordings do exist, they would probably fall under the definition of a public record. We might want to have them included in the destruction schedule because they are more transient.

The Committee agreed that this item requires further research in order to determine whether changes to Rule 123 on this issue are necessary. Jennifer will review and report back to group.

2. Prohibited access to bench books. Consensus was to make no changes on this item.

3. HB2159/employee records. Comments and concerns for this item included the following:

- HB 2159 probably applies to the courts, and therefore Rule 123 is inconsistent with this bill.
- This bill only says that disciplinary records are subject to the public records law. Therefore, Rule 123 is not necessarily inconsistent with the bill.
- Disciplinary records should be protected, however, we can leave Rule 123 as is and indicate that it governs HB 2159
- When other agencies make these records available, they do so with the authority to redact.
- All agreed they do not see a need to change Rule 123.

Consensus was to make no changes on this item.

4. Commercial use fees for court records. Consensus was to make no changes on this item.

5. Require redaction of information identifying victims. Consensus was to make no changes on this item.

6. Redaction of case management data. Comments and concerns for this item included the following:

- The Rule distinguishes the case file records from administrative records and it defines a case record as anything pertaining to a particular case. But, the data that is entered in a case management system about a particular case would then be a case record, not an administrative record.
- As we are moving toward electronic filing, the case management system is going to be the repository of the data that has been filed. There will be no other record/information out there. It is the official record.

Consensus was to make no changes on this item.

7. Restrict search warrants from online access. Comments and concerns for this item included the following:

- Search warrants often cover private property – vehicles, homes, and bank accounts, so they will include the type of information we have on our list of exclusions.
- In the Remote Electronic Access Policy, we excluded warrants.

Consensus was, the Committee will make no changes on this item.

8. Judges included in “employee records.” There is disagreement as to whether there needs to be a change to this section. For now, recommend a change in the language to read “personnel” instead of “employees.” Melinda will research why the issue was brought to light.

9. Close some CLD administrative records. Will be addressed at next meeting, when Nancy Swetnam of CLD will address the Committee.

10. Close defensive driving school records. Defer discussion, as with # 9, above.

11. Serving a sensitive data sheet. Will be addressed in today’s afternoon session, where sensitive data is on the agenda.

12. Broadening of proposed immunity provision to cover courts that do not have clerks. (123(g)(5)). There is agreement that some modification is appropriate. Melinda will draft possible language for a modification and bring to the next meeting for discussion.

13. Are state bar records governed by Rule 123? Discussion included the following comments:

- The state bar is considered a private, non-profit entity. It was created by the judicial branch as a non-profit corporation under Rule 31, but they are not required to follow the public records law, the open meeting law, and so forth.

There was consensus among the members that state bar records are not included under Rule 123.

14. Record retention schedules – paper case files /online case management data

Jennifer briefed the Committee on the background of this issue. She explained that there have been problems with our Public Access-Case Lookup website (hereinafter “Public Access”), where a case record is older than the record retention schedule for that particular kind of case. Some courts are not devoting manpower to going back into the case management system and deleting old cases. Some courts are uncertain as to whether they should delete anything. Whatever a court’s case management database has in it is going to be reflected in the Public Access website. Many courts do not destroy paper records even though the destruction schedule allows destruction at a set time, according to type of document.

There are two main questions to consider on this issue:

1. When paper case records are destroyed, should the electronic record also be destroyed for consistency?
2. Even if paper records are not destroyed, should we establish a system to automatically destroy electronic records at their destruction date?

Comments and questions regarding this issue included:

- We have seen at least a few instances where a member of the public wanted something from a case file that was on the Arizona Judicial Branch Public Access website, but when the person went to the underlying court to obtain the file, the court no longer had the file.
- Based upon the records retention schedule, a court is allowed to delete or destroy the documents themselves, but does that apply to the case management files?
- There is a 3rd element, which is: Even if a court is going to delete the records, there are legitimate reasons for the judicial branch to keep data for decades to identify trends, conduct studies, and prepare reports. But should availability at that point be limited to court officials, for study purposes?
- One possibility, at least in terms of limited jurisdiction courts, would be that when a paper record is destroyed, the electronic version could be archived and retained as an administrative record (versus a case record).
- We need to approach this by first looking at what we should do with the case look-up systems (should the case look-up systems remove cases on the destruction date), and what we should do with the case management data.

Melinda noted that she worked with the limited jurisdiction court records retention schedule subcommittee when they revised that schedule in 2006. It was the intent of the subcommittee that, in limited jurisdiction courts, when the case record is destroyed, all record of it in a case management system be destroyed at the same time. However, it was also recommended that the court keep a permanent report that lists the destroyed cases.

Because this issue requires extensive examination, Chair, Michael Jeanes, assigned a workgroup of Don Jacobson, Patti Noland, and Carol Schreiber to review the issue and report back to the Committee at the next meeting.

15. AOC maintaining archive of case management data. Combined with # 14, above. Assigned to workgroup.

III. Roundtable Discussion

Proposal for Remote Electronic Access to Civil & Criminal Case Records

Modifications to the proposal, based on discussion at the last meeting, were reviewed and discussed. Discussion on the proposal included the following comments/concerns:

- In the policy governing public and non-public records, we defined *case record* as “all existing documents...regardless of physical form or characteristics” Maybe we should stay with that definition and change item A(1)(i) to “any *record* that is collected.”
- Should we supplant the existing definition in Rule 123 with our definition of *case record* here?
- One of the problems is that the *case record* definition in Rule 123 does include other things that are a legitimate part of a case record, but when we move to electronic access, we are saying we are not going to provide access to everything in a case record. Should we even be using the term *case record*? What we are really dealing with is a “subset” of the case record. Maybe we should use the terms *clerk record*, *record*, and *case record* if we want to distinguish what is administrative.
- Current Rule 123 actually does a good job of making a distinction between administrative and case records.
- The definition we have proposed is a good one for *case record*, and we should consider recommending its use in place of the definition of *case record* under existing Rule 123.
- Take section 1 (i, ii, and iii) of the definitions section of this electronic access proposal and make it the new definition of *case record* currently found in 12(B) in Rule 123.
- That would leave the definition of *record* untouched in Rule 123.
- Is there something missing from the definition of *case record* in Rule 123 if we went with this proposed definition of *case record* in the Rule? We could substitute this new definition of *case record*, perhaps substituting the word *record* for *document* in i, for the old definition.
- So, we are in agreement; we will replace the existing Rule 123 definition of *case record* with the definition in section A(1), but change the word *document* to *record*.
- Also, we need to add a semicolon in subpart ii, before the final “and.”
- One other change we should make is in section A(2), to include Title 32 after Title 14 on Probate Proceedings.
- We also need to do away with the concept that this proposal is a pilot. The proposal will be permanent.

Concerns about the changes made to the definition of “criminal case” included:

- The statement “criminal case does not involve any case in which a minor child is a victim” is problematic.
- We could add the statement under section B(2) and say any document related to a criminal case where a minor child is involved.
- Our intent for excluding cases involving minors was to protect them in cases involving sexual abuse, but what about cases where murder is involved? There does not seem to be protective value in excluding that.
- From a practical standpoint, the clerk’s office does not know if a case involves a minor unless it is a dangerous crime against children, or other type of sexual assault, because in those cases it is designated in the charging document.
- Maybe the Missouri Draft, under tab 4 of the binder, would be helpful. It pertains to victim information with respect to stalking, aggravated stalking, domestic assault, sexual assault, and so forth.
- While it is important to protect certain kinds of sensitive data from being available electronically, at the same time, losing public access to precisely those kinds of high profile, important cases presents another problem. There does not seem to be a way under this proposal that would allow the public to obtain access electronically.
- Should we have a process whereby a party could petition, in certain types of criminal cases, to keep the documents from being posted online?
- But that would need to be done at the time of the original filing, otherwise the case is going to be up online. From the time a document is filed electronically until it is available on the clerk’s website can be minutes.
- Would it work to have the standard rule be that in certain cases, the case is not available electronically, but a person could petition to have the case opened/available online?
- What about including adult cases where sexual abuse/assault is involved? The Missouri policy includes both adult and juvenile victims.
- This is manageable because it is not about redacting or removing, but just denying electronic access to specific cases.
- Another problem though, is that about half of the counties in Arizona still have multiple defendant cases under the same case number. So, there might be multiple victims, one of which may be a sexual assault victim, and this policy would require the entire case to be inaccessible.
- But, we are only talking about limiting remote electronic access.
- For a petition to open up such a case, what standard are we setting for that, or what needs to be presented to make a request for access?
- There is language in the sealing of records rule about the judge weighing the public good versus the individual’s private interest, essentially balancing the two. It might be good to follow along those lines.
- Counsel and parties should still have full access.
- We need to define clearly that the case numbers, party names, etc. of a case not posted online will still be publically available so that the public knows that a record exists, and if a a member of the public chooses to file a motion for the court to unseal the case, they have the necessary information to do so.
- Having something in the initiating document from the prosecutor highlighting the fact that this is one of those cases, so that it is easily identifiable to the clerk’s office

that something must be done in the system so that the case does not get posted online for the public would be helpful.

- Do we need to amend the civil and criminal rules to require counsel, during the process of filing cases of this kind, to designate them as not suitable for electronic distribution?
- Could we include a provision that allows a party to petition the court to disallow electronic access, and even if that means that the case has been online for 3 days, it would be better to take it off line on the fourth day than to be without a remedy.
- Maybe we do not want to burden the bench with having to consider all these cases. It would be better to have a clear rule that identifies what type of cases are displayed on the Internet and what type of cases are not displayed.
- Maybe it makes more sense if there is a motion provision to have it relate to appealing to the bench to put something online with respect to those areas we previously excluded.
- So, basically, we would identify those cases by charge that would not go up, but the parties could file a motion to have the case accessible online.
- So, we are all in agreement.
- We are now talking about all sex crimes, rape – adult and juvenile.

Section B (1) comments included the following:

- It reads that “parties and attorneys may be provided remote electronic access at no charge” That is a significant policy change.
- What about just removing the phrase “at no charge?”
- It is agreed that this statement will be removed.
- Can this section include officers of the court who are arbitrators?
- If we are going to include them, it should be in section B(1), where it reads “...in which they are a named party...” and insert *arbitrators* directly following that statement. It is agreed to make this addition.
- Section B(2), we say members of the public will pay “the necessary fee,” but in paragraph 1, we say they will not pay a fee.
- But, with the modification to 1, as discussed, this is still consistent.
- We could say “any established fee” instead of “necessary fee.” It is agreed to make this change.

Section B (3) lists three alternatives.

- Alternative #2 is good, but where it says “no such information shall be accessible,” we should list what that information is, instead of stating “no, or limited information” will be available in the following case types”
- In the second line, after the word “registering,” there should be a comma.
- State law now requires (as of January 2010) all criminal minute entries must be on the web, by judge.
- Did we resolve how we are going to handle date of birth? It is listed in alternative #2.
- The privacy advocates have said d.o.b. is out there, everywhere already, so there is no need to protect it. In some ways, d.o.b. can actually protect people, for example,

in situations where it becomes a means of identifying and/or distinguishing one John Smith from another John Smith.

Section B (4)

- How do we know and/or how can we verify that an individual is actually a federal employee?
- Pima County requires a letter, either on letterhead or via email, issued from the agency in question. The agency is then contacted by phone and we verify with their IT department that the IP address is for an individual and is not accessible to others.
- Are there some people who should be entitled to access, but who will not have an Arizona driver's license, for example, a federal employee from California? Should there be a separate mechanism for them?
- Maybe we need to reformat this whole policy into 3 sections, defining persons who are parties to the case, registered users, and non-registered users. Then, item B (4) would fit under that second category of registered users.

Section D.

- In section D, alternative # 1, seems to conflict with the statement in B (2) about sharing of passwords. We need to be consistent throughout the policy, so that anyone who accesses something should have their own id/password – whether for filing or access.
- We need to set up an alternate process for pro pers.
- We could reword the language at the top of #2, because it infers that the attorney of record on the staff of a private firm can extend access to any other attorney or person working on behalf of that private firm. Maybe we need to modify that to say that at the time of registration, the attorney must name any others who would be working on the case.
- In section D, alternative #3 is good because it allows denial of access, and includes a warning that unauthorized access could be reported to the County Attorney. It must be modified to apply to any level of court.
- There is also some useful disclaimer language in alternative # 2; could we add the second and third sentence, beginning at “This site is a replication . . .” to alternative #3?
- Also, a little further down, where it says the clerk's office “makes no guarantees concerning the information . . .” could also be applicable.

It is agreed that alternative # 3 will be used, with the addition of the 2 statements discussed from alternative #2.

Section E.

- Regarding the subscription fee, we need to keep it simple and not get into charging for minutes or the number of pages.

- But the funding model for this statewide portal project is up in the air, and we do not have enough information to address cost. Maybe we need to put off discussion of fees for now.
- The Pima County recorder has a onetime \$20 registration fee, and this keeps people from just doing malicious surfing.
- Maybe it would be better for us to establish an annual fee, but it depends on the actual intent of the fee; is it trying to make the system self-sustaining, or is it just a registration fee to serve as an identifier and discourage people who are just seeking to play around in the system?
- The other option is to say that a fee will be established by the individual court, because we do not want to put a fee into a rule. It could include something like “ a fee not to exceed”
- The statute that allows the board of supervisors to establish fees allows a fee up to the cost of providing the service. A fee cannot generate a profit.

There is a lot more to consider on this issue, so we need to table it for now and address it at another time.

Section G:

- Where it says “in paper or imaged format,” can we change “imaged” to electronic, because e-file documents are not imaged?
- Also, it needs to be worded differently to clearly say that there is no effect on access to records at the courthouse.

IV. Call to the Public

Chairman, Michael Jeanes, made a call to the public.

Meeting adjourned at 2:41

Next meeting: Tuesday, August 26, 2008, 10:00am – 2:30pm, Supreme Court Building, 1501 W. Washington, Phoenix, AZ, Conference Room 119 A/B.

**ARIZONA SUPREME COURT
RULE 123 AND DATA DISSEMINATION
ADVISORY COMMITTEE**

MINUTES

Tuesday, August 26, 2008

MEMBERS PRESENT:

Dave Byers
Michael Jeanes
David Bodney
Janna Day
Donald Jacobson
Patricia Noland
Rachelle Resnick
Patricia Sallen (telephonically)
James Scorza
Terry Stewart
Karen Westover

GUESTS PRESENT:

Jennifer Greene
Rich Robertson
Mark Jensen
Daniel Romm
Regina Kaupanger
Therese L. Martin
Nancy Swetnam
Diane Stubbs
Enric Volante

MEMBERS ABSENT:

Catherine O'Grady
Honorable Peter B. Swann
Honorable John S. Taylor

STAFF:

Melinda Hardman
Tama Reily

I. CALL TO ORDER

The August 26, 2008 meeting of the Rule 123 & Data Dissemination Advisory Committee was called to order by Michael Jeanes, Chair, at 10:00 a.m.

II. APPROVAL OF MINUTES

The minutes from the July 22, 2008 meeting of the Rule 123 & Data Dissemination Advisory Committee were presented for approval.

Motion: To approve the minutes from the July 22, 2008 meeting of the Rule 123 &

Data Dissemination Advisory Committee as presented. Approved unanimously.

III. ROUNDTABLE DISCUSSION

Proposal for Remote Electronic Access to Civil & Criminal Case Records

Changes that were made to the proposal since the last meeting were reviewed by the committee. Discussion included the following comments:

- The absence of the word “data” in the definition of “case record” raises a question. The committee previously agreed that “record” would be defined to include both documents and data, however, “data” is not used in this proposal. After discussion, consensus was to add the phrase “in paper or electronic format” to the definition of the term “case record.”
- Members agreed that all Opinions of the appellate courts must be made available to anyone, without registering, except that any Appendix to an Opinion in a criminal case in which a minor child is alleged to be the victim, shall not be provided by remote electronic access.
- Docket information should be provided in all case types unless otherwise restricted by rule or law.
- Section B should be simplified to say, for example, “the court will provide remote electronic access to case records under the following conditions...” and then define the levels of access in sections 1, 2, and 3.
- To make these access provisions work effectively, judges will need to receive additional training on compliance with Supreme Court Rule 125.
- Where 2(a)(viii) sets forth the requirement that the prosecuting agency shall “advise the clerk that the case is subject to this provision,” there is a question of whether this notice requirement should also be placed in the civil and criminal rules, as opposed to appearing in Rule 123, only. The committee agreed that the requirement of the prosecuting agency to advise the clerk that the case is one in which a minor child is alleged to be the victim of sexual assault should also be added to the civil and criminal rules, and the report should note this recommendation.
- Extended discussion on the registration process for remote electronic access ensued. Comments centered on:
 - Whether the registrations process should be different for the general public, attorneys, and parties.
 - Online versus phone registration.
 - The process by which a court would assign user names and passwords.
 - In-state attorneys registering with their bar number and whether out-of-state attorneys should be issued an Arizona bar number.

- It was suggested that the details of the registration process should not be included in the Rule, but that the Rule should refer to “guidelines” that would be established by the Arizona Judicial Council (AJC). This way, the guidelines could be changed more easily. An Appendix to the report could contain the details of what this committee has worked on to date on these issues.
- Extended discussion regarding fees for remote electronic access. Discussion included the following concerns:
 - Upon what should the fee be based?
 - Should there be a charge per document?
 - What about a variance in fees from county to county?
 - Should the fee be based upon the frequency of use?

After lengthy discussion on registration and fees, Mr. Jeanes suggested that a workgroup be formed to review all the aspects of these issues. Several members agreed to participate on this workgroup, including Patti Noland, Terry Stewart, and Dave Byers. Michael Jeanes noted that someone from his staff will participate as well. Members of the AJC Commission on Technology or its subcommittees should also be asked to participate. This workgroup’s recommendations should be completed by May 2009.

IV. Possible Amendments to Rule 123

Nancy Swetnam, Director, AOC Certification & Licensing Division, addressed the committee regarding issues facing her Division regarding public record requests. She also expressed concern about certain provisions of current Rule 123. Ms. Swetnam was asked to provide a draft of modifications she would like to see made to the Rule. Jennifer Greene volunteered to work with her on this issue.

Report of Records Retention Workgroup

Donald Jacobson reported on the findings of the Records Retention Workgroup and presented the workgroup’s draft proposal. The committee agreed to adopt the draft language of the workgroup.

Discussion of Possible Amendments to Rule 123

Jennifer Greene informed the committee of a recent amendment to Rule 123 regarding digital recordings of court proceedings. Rule 123 was revised in 2006 to provide that electronic verbatim recordings made by a courtroom clerk or at the direction of the clerk and used in preparing minute entries are closed. Additionally, an original transcript filed with the Clerk of Court is presently made available to the public at the same copy rate per page at which all copies are provided. A member of the public may choose to obtain a copy of the transcript from the court reporter at a lower statutory rate per page. Finally, transcripts should not be made available by remote electronic access due to the sensitive information often contained in them. Therefore,

there is no need to modify Rule 123 further regarding recordings of court proceedings or transcripts.

Mr. Jeanes noted that the remaining proposals listed on the agenda will need to be tabled until the next meeting. Members were asked to review the policy drafts in the interim, and come prepared to discuss them at the next meeting.

V. Call to Public/Adjourn

Chairman, Michael Jeanes, made a call to the public.

No comments were made.

Meeting adjourned at 2:30 p.m.

Next Meeting: Tuesday, September 23, 2008, 10:00am - 2:30pm, Supreme Court Building, 1501 W. Washington, Phoenix, AZ, Conference Room 345 A/B

**ARIZONA SUPREME COURT
RULE 123 AND DATA DISSEMINATION
ADVISORY COMMITTEE**

DRAFT MINUTES

Tuesday, September 23, 2008

MEMBERS PRESENT:

Jennifer Greene for Dave Byers
Michael Jeanes
David Bodney
Janna Day
Donald Jacobson
Rachelle Resnick
James Scorza
Terry Stewart
Honorable John S. Taylor – telephonic
Karen Westover

GUESTS PRESENT:

Rich Robertson
Marc Osborn
Regina Kaupanger
Therese L. Martin

MEMBERS ABSENT:

Catherine O’Grady
Patricia Sallen
Honorable Peter B. Swann
Patricia Noland

STAFF:

Melinda Hardman
Tama Reily

I. CALL TO ORDER

The September 23, 2008 meeting of the Rule 123 & Data Dissemination Advisory Committee was called to order by Michael Jeanes, Chair, at 10:03 am.

Mr. Jeanes discussed the timeline necessary for the committee to meet its charge from Chief Justice McGregor. Final drafts of the policy proposals need to be ready for review at the October 30, 2008 meeting in order to complete the committee’s report/recommendations, for presentation to the Arizona Judicial Council (AJC) at their December 2, 2008 meeting. This actually requires that the package go out to AJC by November 15th. The deadline for submission of the rule change petition is January 10, 2009. The petition will then go out for public comment until approximately May 20, 2009. Following that period, the committee might need to hold a couple of meetings to review the public comments received.

In addition, he noted another issue the committee needs to address today is the question of what provisions should be included in the Rule, and what should be included in administrative code.

II. APPROVAL OF MINUTES

The minutes from the August 26, 2008 meeting of the Rule 123 & Data Dissemination Advisory Committee were presented for approval.

Motion: To approve the minutes from the August 26, 2008 meeting of the Rule 123 & Data Dissemination Advisory Committee as presented. Approved unanimously.

III. ROUNDTABLE DISCUSSION OF POLICIES

Proposal for Remote Electronic Access to Civil & Criminal Case Records:

Changes made to the proposal since the last meeting were reviewed. Several non-substantive grammatical and/or terminology changes were discussed and will be added to the document prior to the next meeting.

Proposal for Bulk/Compiled Data Access:

The current draft proposal was reviewed and lengthy discussion ensued centering on which items should be included in the bulk data policy. Numerous grammatical and/or terminology changes were agreed upon, and will be incorporated into the document and reviewed at the next meeting.

Marc Osborn, on behalf of LexisNexis, had several concerns/requests for the committee as follows:

- It would be helpful to relax restrictions on the electronic access policy so that bulk data users, such as LexisNexis, can have the same type of remote electronic access to court records as Arizona residents without going through the approval process.
 - The committee is open to this suggestion if the technology is available to accomplish it, however, a technology group will need to look at this issue and advise the committee further. Security concerns regarding such access could be addressed in the bulk data contract.
- Rather than requiring prior approval for each re-dissemination of data to third parties, the agreement with bulk data recipients could specify the types of bulk data transactions that are prohibited.
 - The committee addressed this issue in item # 3 of the bulk data policy, by prohibiting a bulk data recipient from re-disseminating the data for unrestricted access on the Internet with the “personal identifiers set forth in Rule 123(j)(4), Rules of the Supreme Court.”
- To ensure current and accurate information, bulk data for re-dissemination should be updated as new data is received.

- The committee addressed this issue in item #5 of the bulk data policy by requiring the recipient of bulk data to update its database within 48 hrs. of receipt of new data.
- Requiring subscribers to provide disclosure statements to third parties when procuring records is not a workable process.
 - The committee did not resolve this concern.

Proposal for Removing Sensitive Data in Case Records:

Mr. Jeanes reminded the committee that this proposal is strictly intended to keep sensitive data out of *online* court records. The committee agreed to eliminate all elements of the draft proposal except to require filers to refrain from including social security numbers, financial account numbers, juvenile victim's names, and victims' locating information in civil cases, to grant the court authority to impose sanctions for violation of this requirement, and to require prosecuting agencies to advise the clerk when a charging document involves a minor child alleged to be the victim of sexual assault so that these cases can be kept offline.

Proposal for Distributing Court Records to Court Partners

The committee was unable to address this proposal during today's meeting. Due to the impending deadline, Mr. Jeanes requested that committee members review this proposal over the next week to ten days and send their comments to Melinda so that suggested modifications can be incorporated prior to the next meeting on October 30, 2008. Discussion could then focus on making final revisions at that time.

Rule vs. ACJA

Mr. Jeanes again raised the question of what should be added to and/or removed from Rule 123, and what should be included in administrative code. One of the considerations in this decision is that the court can only consider rule changes one time per year, whereas administrative code changes can be made more often if necessary. Both the administrative code and rules are equally accessible to the public and are published on the supreme court website. Another consideration is that the supreme court has indicated it would like to limit rules to strictly procedural issues that occur during court proceedings and include court administrative matters in administrative code. Under this definition, most of existing Rule 123 should actually be moved to administrative code. On the other hand, the committee could recommend to the court that everything stay in Rule 123 rather than code.

Discussion included the following comments:

- Maybe the details of items such as bulk data agreements are better dealt with in code, but it seems that there should be at least a broad definition of bulk data from a public records perspective in rule. This would seem to provide a little more importance to the topic than placing everything in the administrative code.
- We can recommend to the court that there be additions to Rule 123 that say, for example, that there are bulk data access requirements which were placed in the code.

- We previously discussed that the remote electronic access policy, including fees and registration and probably the user agreement should go into code.
- We do not want to put operational issues, whether it be fees or something similar, into the rules because of the time involved in obtaining a rule changed.

The committee agreed to leave the bulk of its recommendations in Rule 123 but to place administrative or operational issues in the administrative code.

V. Call to Public/Adjourn

Chairman Michael Jeanes made a call to the public.

No comments were made.

Meeting adjourned at 2:33 p.m.

Next Meeting: Thursday, October 30, 2008, 10:00am - 2:30pm, Supreme Court Building, 1501 W. Washington, Phoenix, AZ, Conference Room 345 A/B

**ARIZONA SUPREME COURT
RULE 123 AND DATA DISSEMINATION
ADVISORY COMMITTEE**

MINUTES

Thursday, October 30, 2008

MEMBERS PRESENT:

Dave Byers
Mark Jensen (for Michael Jeanes)
David Bodney
Mark Bolton (for Janna Day)
Donald Jacobson
Patricia Noland
Rachelle Resnick
Patricia Sallen
Terry Stewart
Honorable John Taylor
Karen Westover

GUESTS PRESENT:

Michelle Carpenter
Dan Corsetti
Jennifer Greene
M.J. Gregory
John Moody
Dorrian Jones
Regina Kaupanger
Marc Osborn
Rich Robertson

MEMBERS ABSENT:

Catherine O'Grady
James Scorza
Honorable Peter B. Swann

STAFF:

Melinda Hardman

Tama Reily

I. CALL TO ORDER

The October 30, 2008 meeting of the Rule 123 & Data Dissemination Advisory Committee was called to order by Vice Chair, Dave Byers, at 10:01 am.

Members and guests introduced themselves.

Mr. Byers stated the goals of the meeting and reviewed the timeline for presenting the committee's final proposal to the Arizona Judicial Council (AJC).

II. APPROVAL OF MINUTES

The minutes from the September 23, 2008 meeting of the Rule 123 & Data Dissemination Advisory Committee were presented for approval.

MOTION: To approve the minutes from the September 23, 2008 meeting of the Rule 123 & Data Dissemination Advisory Committee as presented. Motion seconded. Approved unanimously.

III. ROUNDTABLE DISCUSSION OF REMAINING/PENDING ISSUES

The committee reviewed the list of pending items and determined what action, if any, was needed. The items were decided as follows:

- HB2159: This issue was taken to the presiding judges last week and the presiding judges determined there is no need to amend Rule 123 in light of this bill. Their position should be analyzed by a workgroup of this committee to confirm that nothing has been overlooked. The workgroup should articulate why there is no need to amend the rule, and if the workgroup determines there is a need to amend, the workgroup should file a comment to the rule petition. Volunteers for the workgroup are Don Jacobson, Rachelle Resnick, Karen Westover, and David Bodney.
- Certification & Licensing concerns: Legal Services has been working with Nancy Swetnam, Certification & Licensing Division Director, and believes her primary concern is covered in the proposed amendment to Rule 123(e) Access to Administrative Records, as follows:

(13) Certification records. Proprietary materials required to be submitted to the supreme court by applicants for certification or licensing are closed.

Suggestion was made to put the onus on the filer of proprietary material to identify it as such.

MOTION: To specify that proprietary material required to be submitted to the supreme court by applicants for certification and licensing are closed and to require the filer of such records to identify them as proprietary. Motion seconded. Approved unanimously.

- Amending (e)(7): Should (e)(7) be amended to include closing any logs of files reviewed in clerks' offices? Discussion concluded the rule should be amended to provide that if logs are maintained, the logs are closed. The committee emphasized there is no obligation to maintain a log of files reviewed in clerks' offices.

MOTION: To modify (e)(7) to say that patron records maintained by a court or clerk are closed. Motion seconded. Vote: 5-4-0.

- Government Partner Policy: Discussion centered on recommended amendments to Rule 123 to clarify that the rule governs access to court records by court employees and bulk data requests, in addition to access by the public. Further language will be included in an Arizona Code of Judicial Administration (ACJA) section to provide details of the various types and limitations of access.
- Draft Rule 123(h)(5): Attention is brought to page 34, paragraph 5, of the draft report, under *Correcting Data Errors*. The language that appears here is verbatim to that which appears in the pending but unapproved Rule 123 Petition. Should this language remain? Committee consensus was the language should remain.
- Draft Rule 123(j)(1)(B): Should courts be authorized to enter into an agreement with a private entity familiar with the courts' databases to run special reports? The proposed language is:
 - A CUSTODIAN MAY CONTRACT WITH A PRIVATE OR PUBLIC INSTITUTION FOR THE PROVISION OF BULK DATA UNDER THIS POLICY.

Committee consensus was to include the provision but also include specialized reports of compiled data for which the custodian may contract with an outside institution.

- LexisNexis letter: LexisNexis' letter of concerns regarding data and record retention timeframes was considered. Suggestion was made to LexisNexis representative, Marc Osborn, that LexisNexis should review the court record retention schedules currently in place, and if LexisNexis is not comfortable with the timeframes in these schedule, LexisNexis could consider petitioning the court for a change to the schedules. A records retention schedule packet was provided to Mr. Osborn today. LexisNexis did not raise additional concerns, either from their letter of October 22, 2008 or otherwise.
- Adult victims: Should adults be included in the provision keeping records containing juvenile victims' (of sexual assault) names off of remote electronic access? Attention was directed to the registered users section of the final report, page 27-28, (B)(i)(a), which states "**family law, paternity, or other matters arising out of Title 25**" are excluded from access. The committee was in consensus that this was satisfactory and that records containing adult victims' names need not be specifically excluded from remote electronic access.

General comments and/or concerns regarding the draft report were discussed. Several minor, non-substantive language changes were suggested.

Further amended items were as follows:

- On proposed amendment to Rule 123(e) Access to Administrative Records:

MOTION: To return language under Rule 123(e)(1) from *Personnel Records* to *Employee Records*. Motion seconded. Approved unanimously.

- In Appendix D: Recommended Provisions for New ACJA Section on Public Records:

MOTION: To form a task group that will work to designate a suitable, one-time registration fee for remote online access to case records. Motion seconded. Approved unanimously.

- With discussion concluded, a motion was made to accept the final draft report with the modifications proposed today.

MOTION: To approve the Final Report of the Advisory Committee on Supreme Court Rule 123 and Data Dissemination as amended. Approved unanimously.

IV. Call to the Public/Adjourn

Mr. Byers made a call to the public.

Janet DelTufo from the First Amendment Coalition of Arizona expressed her desire that all case records should be available to the public through remote electronic access. Mr. Byers explained to Ms. DelTufo that the committee had heard from groups concerned with privacy and identity theft, and, as a result, the committee determined that the rule modifications being presented are appropriate.

Rich Robertson, of R3 Investigations, asked for clarification of the terms “bulk” and “compiled” data. In addition, Mr. Robertson expressed the opinion that it is a function of the court to compile reports that provide the specific information requested by a user. Mr. Byers explained that a court is not required to create and/or provide such customized reports. This goes far beyond the statutory requirements of making information available to the public. Mr. Byers also noted that Rule 123 includes a provision for appealing a denial of a request for information.

**ARIZONA SUPREME COURT
RULE 123 AND DATA DISSEMINATION
ADVISORY COMMITTEE**

DRAFT MINUTES

Monday, April 13, 2009

MEMBERS PRESENT:

Dave Byers
Michael Jeanes
David Bodney
Janna Day
Donald Jacobson
Patricia Noland (telephonic)
Rachelle Resnick
Patricia Sallen
James Scorza
Honorable Peter B. Swann
Karen Westover

GUESTS PRESENT:

Michelle Carpenter
Jennifer Greene
Dorrian Jones
Regina Kaupanger
Therese Martin
Barry Neel
Marc Osborn
Diane Gunnels Rowley
Sally Wells

MEMBERS ABSENT:

Catherine O'Grady
Terry Stewart
Honorable John Taylor

STAFF:

Melinda Hardman
Tama Reily

I. CALL TO ORDER

The April 13, 2009 meeting of the Rule 123 & Data Dissemination Advisory Committee was called to order by Chair, Michael Jeanes, at 10:04 am.

Members and guests introduced themselves.

Mr. Jeanes noted that the committee's Rule Petition had been out for comment until April 1, 2009, and that all comments were compiled for the committee's review today. Changes agreed to in this meeting will be incorporated in an amended petition, which will be filed by May 8, 2009.

II. APPROVAL OF MINUTES

The minutes from the October 30, 2008 meeting of the Rule 123 & Data Dissemination & Advisory Committee were presented for approval.

MOTION: To approve the minutes from the October 30, 2008 meeting of the Rule 123 & Data Dissemination & Advisory Committee as presented. Motion seconded. Approved unanimously.

III. ROUNDTABLE DISCUSSION OF COMMENTS RECEIVED & POSSIBLE AMENDMENTS TO RULE PETITION

The committee began with a review of comments received on technical issues relating to Rule 123, Rules of the Supreme Court, Rule 2.3, Rules of Criminal Procedure, and Rule 5(f), Rules of Civil Procedure. After discussion, changes were incorporated where indicated.

MOTION: To adopt the amendments to Rule 123, Rules of the Supreme Court, as discussed. Motion seconded. Approved unanimously.

MOTION: To adopt the amendments to Rule 2.3, Rules of Criminal Procedure. Motion seconded. Approved unanimously.

MOTION: To adopt the amendments to Rule 5(f), Rules of Civil Procedure. Motion seconded. Approved unanimously.

Comments received on more substantive issues were discussed as follows:

Remote Electronic Access to Case Records; Section (g)(1)(A)

Sally Wells, Chief Assistant County Attorney, shared the concerns of the Maricopa County Attorney's Office regarding the remote access section of the proposal. Specifically, they feel that section (g)(1)(A), does not sufficiently define the categories of „users“ and the access granted them, nor does it clearly allow the prosecutorial agencies the access necessary for criminal justice purposes. They wish to ensure that prosecutorial agencies have „party“ access to cases statewide, in which they may not be a party, and are requesting revision of the categories and access granted as described.

There was extensive discussion on how to define prosecutorial agencies and other government entities, in order to allow the level of access warranted for their purposes. Both Pima and Maricopa Counties reported they already have agreements with County Attorneys' offices in other counties for remote access, and in Pima County, agencies such as Child Protective Services (CPS) have been granted remote access to certain records on a limited basis. In Pima County a „memo of understanding“ outlines the access granted, because it varies among agencies. For instance, CPS does not warrant the same access as a prosecutorial agency. Members agreed there appears to be a need for a category of government entities, to which the court can grant remote access to records.

It was noted that the language under *General Provisions* in section (c)(6), which states that government agencies may be granted access to court records “in order to serve a public purpose,”

could address the issue of access to cases in which the agency may not be a party. Members concluded that rather than adding language to an existing subsection, it would be clearer to add a category under (g)(1) that allows various government and trusted partners to be granted the appropriate level of access, based on serving a public purpose, which can be defined through a memo of understanding with an individual county.

It was further noted that a request for remote electronic access by a researcher should be handled through an Order of the Presiding Judge and should not be included in this new category.

MOTION: To create a new subsection (B) under (g)(1) creating a category for various government entities and trusted partners to be granted access to court records in order to serve a public purpose, and which will be defined through a memo of understanding with an individual county. Motion seconded. Approved unanimously.

Mr. Jeanes asked that members with language suggestions for this subsection forward them to Melinda.

Bulk Data; Section (j)(1)(B)

Comments submitted on behalf of the Courthouse News Service concerned the definition of „bulk data“ and the language used to describe the dissemination of bulk data by outside vendors. Of primary concern was the possibility that an outside vendor contracting with a court to compile bulk data reports could result in the courts“ inadvertently contributing to discriminatory media access to the data if the vendor releases the bulk data. Members discussed the implications and opted to change the language in order to clarify its meaning. The alternative method of complying with a bulk data request, set forth in (j)(1)(B) was revised so that it reads “*A custodian may contract...to provide specialized reports...*” Members also determined that changes should be made to (j)(1)(A) as follows:

A custodian may release bulk data to an individual, a private company, or a public organization under this policy. Before releasing bulk data, a custodian shall require the recipient to execute a dissemination contract and disclaimer containing provisions specified by the supreme court.

At this time, a member raised a question regarding (j)(3)(B), where only month and year of birth were listed as permissible to release in bulk. A motion was made to change this provision to allow the full date of birth to be released in bulk.

MOTION: To modify section (j)(3)(B) to read “Date of Birth.” Motion seconded. Motion passed 9:2:0

Remote access to sex crimes cases; Section (g)(1)(B)(ii)(h)

Judge Ron Reinstein, Chair of the Commission on Victims in the Courts, submitted a comment requesting language changes in section (g)(1) that would exclude remote access to all sex crime cases, whether the victim is an adult or juvenile. After lengthy discussion, Mr. Jeanes polled the committee and a majority of the members present decided the

original language that restricts only juvenile records from remote access should be retained. It was noted that this decision applies to the proposed language in Rule 2.3 (B), Rules of Criminal Procedure as well. There was some discussion of whether the statutes identified in the original petition are actually limited to juveniles or whether an adult could be charged with these offenses. Member consensus was that AOC staff should review the statutes and make sure the citations in the proposal reflect the committee's intent of excluding only cases in which a juvenile is alleged to be the victim of sexual assault.

Correcting Data Errors; Section (h)(5)

The committee discussed the comment filed by the Arizona Association of Superior Court Clerks (AASCC) regarding the difficulty presented for the Clerks if the term "data errors" is not more clearly defined. It was suggested that the language could be revised to be similar to that of Minnesota's Rule, which is as follows:

Correction of case records: An individual who believes that a case record contains clerical errors may submit a written request for corrections to the court administrator of the court[Clerk] that maintains the record with a copy served on all parties to the case. Such request shall be no more than 2 pages in length. The court administrator[Clerk] shall promptly do one of the following:

- a) correct a clerical error for which no court order is required*
- b) forward the request to the court to be considered informally*
- c) forward the request to the party or participant who submitted the record containing the alleged clerical error, who in turn may seek appropriate relief from the court. Upon forwarding under clause „b“the court may either correct the error on its own initiative or direct that the request will only be considered pursuant to a motion requesting correction. The courts directive may also establish appropriate notice requirements for a motion and the request for correction authorized in this subdivision need not be exhausted before other relief be.*

A suggestion was made that, rather than using the term „Clerk“, the term „Custodian of Records“, which is already defined in the Rule, should be used.

Members discussed whether it would be prudent to require all of the steps described by Minnesota for correction of a simple clerical error, such as an incorrect date of birth. There were several points of concern raised regarding the number of steps involved, and the Clerks' role in changing a record without an order from the court. It was noted that Civil Rule 60 covers this issue – with a subsection (a) for clerical mistakes and a subsection (b) for correcting errors in the record of judgment. It was agreed to have AOC staff draft similar language as Minnesota, taking into account the existing language in Civil Rule 60.

Rule 5(f), Rules of Civil Procedure for the Superior Courts of Arizona

The committee addressed several comments received on Rule 5(f). Comments concerned the ambiguity of terms such as „victim“, „filer“, and „other locating information“, as well as the difficulty presented if certain victim information is to be excluded from civil rules cases. In order to provide clarification, the following agreements were reached:

- Remove proposals 3 and 4 in Rule 5(f)(A)
- Remove the juvenile victim's information noted in Rule 123(b)(15) in the definition of „Sensitive Data“.
- Replace „filer“ with “a person making a filing with the court.”

After reviewing all posted comments, a guest reported receiving a suggestion that the definition of „judge“ in subsection (b)(10) be expanded to include the types of hearing officers that are appointed to hear disciplinary cases and other matters that come before various boards. Members discussed the usefulness of adding a reference to “hearing officer” and “master” after the term „arbitrator“. It was agreed that the list would not be exclusive if the definition were modified with the term “*including*” following „judicial officer“, and “*hearing officer, master*” following the term „arbitrator“.

Following this item, members concluded that the revisions discussed today lent more clarity to the terms and processes set forth in the rule amendments and a motion was made to accept the changes.

MOTION: To include the changes and modifications to Supreme Court Rule 123, Criminal Rule 2.3, and Civil Rule 5(f) as discussed today. Motion seconded. Approved unanimously.

An amended version of the Rule Petition will be produced as quickly as possible and will be distributed to members for review. The filing deadline is May 8th, so members will be asked to review the petition as soon as possible and bring any problems to Melinda's attention.

IV. Call to the Public/Adjourn

Mr. Jeanes made a call to the public.

Meeting adjourned at 1:50 pm.