

Section 3.00 ELECTRONIC CASE RECORD INFORMATION EXCLUDED FROM PUBLIC ACCESS

The following information in an electronic case record is not accessible by the public:

- A. social security numbers;
- B. operator license numbers;
- C. victim information including name, address and other contact information;
- D. informant information including name, address and other contact information;
- E. juror information including name, address and other contact information;
- F. a party's street address, except the city, state, and ZIP code may be released;
- G. witness information including name, address and other contact information;
- H. SID (state identification) numbers;
- I. financial institution account numbers, credit card numbers, PINS or passwords used to secure accounts;
- J. notes, drafts, and work products related to court administration or any office that is the primary custodian of an electronic case record;
- K. information sealed or protected pursuant to court order;
- L. information to which access is otherwise restricted by federal law, state law, or state court rule; and
- M. information presenting a risk to personal security, personal privacy, or the fair, impartial and orderly administration of justice, as determined by the Court Administrator of Pennsylvania with the approval of the Chief Justice.

COMMENTARY

The Committee's reasoning for not releasing each category of sensitive information is set forth below.

Social Security Numbers

At the outset, the Committee noted that the MDJS Policy provides that the AOPC will not release social security numbers.⁹² In addition, the Committee could not locate any controlling legal authority that required the courts and/or offices to either release or redact social security numbers from an electronic case record before permitting access to the same.⁹³ While such controlling authority is non-existent, the Committee's review of the RTKA, federal law, federal and other states court's policies (either enacted or proposed) yielded much information on this subject.

First, case law interpreting the RTKA consistently maintains that social security numbers fall within the personal security exception of the RTKA and thus should not be released.⁹⁴

Second, the Freedom of Information Act (FOIA)⁹⁵ and the Privacy Act⁹⁶ apply only to records of "each authority of the Government of the United States,"⁹⁷ and they do not apply to state case records.⁹⁸ However, even if these laws did apply to state case records, social security numbers are exempted from public disclosure under the FOIA personal privacy exemption,⁹⁹ while the Privacy Act does not appear to restrict the dissemination of social security numbers (only the collection of them).

In addition, Section 405 of the Social Security Act provides that "social security account numbers and related records that are obtained or maintained by authorized persons pursuant to any provision of law, enacted on or after October 1, 1990, shall be confidential, and no authorized person shall disclose any such social security account number."¹⁰⁰ Although, it is unclear as to whether this law is applicable to state courts, some courts such as Vermont¹⁰¹ and Minnesota¹⁰² appear to have used this statute as a basis for formulating a recommendation on

⁹² See MDJS policy, Section II.B.2.a.

⁹³ Over the past several legislative terms, several bills have been introduced concerning the confidentiality of social security numbers. For example, please see Senate Bill 1407 (2001-2002), Senate Bill 703 (2003-2004) and Senate Bill 601 (2005 and 2006).

⁹⁴ See, e.g., *Tribune-Review Publ'g Co. v. Allegheny County Hous. Auth.*, 662 A.2d 677 (Pa. Commw. Ct. 1995), *appeal denied*, 686 A.2d 1315 (Pa. 1996); *Cypress Media, Inc. v. Hazelton Area Sch. Dist.*, 708 A.2d 866, (Pa. Commw. Ct. 1998), *appeal dismissed*, 724 A.2d 347 (Pa. 1999); and *Times Publ'g Co., Inc. v. Michel*, 633 A.2d 1233 (Pa. Commw. Ct. 1993), *petition for allowance of appeal denied*, 645 A.2d 1321 (Pa. 1994).

⁹⁵ 5 U.S.C. § 552 (2006).

⁹⁶ 5 U.S.C. § 552(a) (2006).

⁹⁷ 5 U.S.C. § 551 (2006), *see also*, 5 U.S.C. § 552(f) (2006).

⁹⁸ Please note that the *CCJ/COSCA Guidelines* provide that "[a]lthough there may be restrictions on federal agencies disclosing Social Security Numbers; they do not apply to state or local agencies such as courts." See *CCJ/COSCA Guidelines*, p. 46.

⁹⁹ E.g., *Sheet Metal Worker Int'l Ass'n, Local Union No. 19 v. U.S. Dep't of Veterans Affairs*, 135 F.3d 891 (3d Cir. 1998).

¹⁰⁰ 42 U.S.C. § 405(c)(2)(C)(viii) (2006).

¹⁰¹ See Reporter's Notes following VERMONT RULES FOR PUBLIC ACCESS TO COURT RECORDS RULE 6(b)(29) which provides that "[u]nder federal law social security numbers are confidential." The Reporter specifically cites to Section 405(c)(2)(C)(viii)(1) of the Social Security Act.

¹⁰² *Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (June 28, 2004), p. 37, n.76 (citing the Social Security Act's provision that provides "[f]ederal law imposes the

the release of social security numbers.

With regard to the federal courts, the Judicial Conference Committee on Court Administration and Case Management (“Judicial Conference”) in September 2001 recommended that the courts should only release the last four digits of any social security number in electronic civil case files available to the public.¹⁰³ The Judicial Conference also recommended that the public should not have electronic access to criminal case files. However, in March 2002, the Judicial Conference established a pilot program wherein eleven federal courts provide public access to criminal case files electronically. In this pilot program, the Judicial Conference set forth that the courts shall only release the last four digits of any social security number.¹⁰⁴

The Committee’s review of other states’ policies, whether enacted or proposed, found that the redaction of all or part of social security numbers is common. For instance, the policies of the following states provide that only the last four digits of a social security number shall be released: New York,¹⁰⁵ Indiana,¹⁰⁶ and Maryland.¹⁰⁷ In addition, the policies of the following states provide that the entire social security number is protected and no part of it is released: Arizona,¹⁰⁸ California,¹⁰⁹ Florida,¹¹⁰ Vermont,¹¹¹ Washington,¹¹² Minnesota,¹¹³ Massachusetts,¹¹⁴

confidentiality of SSN whenever submission of the SSN is ‘required’ by state or federal law enacted on or after October 1, 1990.”)

¹⁰³ *Report of the Judicial Conference Committee on Court Administration and Case Management on Privacy and Public Access to Electronic Case Files*, p. 3. As a result of this report, the U.S. District Court for the Eastern District of Pennsylvania promulgated Local Rule 5.1.3 which provides that personal identifiers such as social security numbers should be modified or partially redacted in all documents filed with the court before public access is permitted. *See also* Local Rules of Practice for the Southern District of California Order 514-C which provides in part that parties shall refrain from including or shall partially redact social security numbers from pleadings filed with the court unless otherwise ordered by the court or the pleading is excluded from public access. If the social security number must be included, only the last four digits of that number should be used.

¹⁰⁴ *Remote Public Access to Electronic Case Records: A Report on a Pilot Project in Eleven Federal Courts*, prepared by the Court Administration and Case Management Committee of the Judicial Conference, p. 12.

¹⁰⁵ *Report to the Chief Judge of the State of New York* by the Commission on Public Access to Court Records (February, 2004), p. 8. The Report recommends that social security numbers should be shortened to their last four digits.

¹⁰⁶ IND. ADMIN. R. 9(F)(4)(d) provides that when a request for bulk or compiled information includes release of social security numbers, that only the last four digits of the social security number should be released. However, Rule 9(G)(1)(d) provides that “[t]he following information in case records is excluded from public access and is confidential: . . . Social Security Numbers.”

¹⁰⁷ Maryland Rule of Procedure 16-1007 provides that “. . . a custodian shall deny inspection of a case record or a part of a case record that would reveal: . . . [a]ny part of the social security number . . . of an individual, other than the last four digits.”

¹⁰⁸ ARIZ. R. 123 Public Access to the Judicial Records of the State of Arizona, Subsection (c)(3) provides in part that “documents containing social security [numbers] . . . when collected by the court for administrative purposes, are closed unless made public in a court proceeding or upon court order.” *See also Report and Recommendation of the Ad Hoc Committee to Study Public Access to Electronic Records* dated March 2001 Sections (IV)(B), (IV)(D), (V)(1) and (VI)(6).

¹⁰⁹ CAL. CT. R. 2077(c)(1) provides that “the following information must be excluded from a court’s electronic calendar, index, and register of actions: (1) social security numbers” before public access is permitted.

¹¹⁰ Order of Supreme Court of Florida, No. AOSO04-4 (February 12, 2004). Specifically, the Order lists information that shall be accessible in electronic format to the public. Social security numbers are not listed in the Order.

¹¹¹ VERMONT RULES FOR PUBLIC ACCESS TO COURT RECORDS RULE 6(b)(29). This subsection provides that “the public shall not have access to the following judicial branch records . . . records containing a social security number of any person, but only until the social security number has been redacted from the copy of the record provided to the public.” *See also* VERMONT RULES GOVERNING DISSEMINATION OF ELECTRONIC CASE RECORDS RULE §3(b).

Kansas,¹¹⁵ and Kentucky.¹¹⁶

The CCJ/COSCA Guidelines suggest that the release of social security numbers should be considered on a case by case basis to determine if access should be allowed only at the court facility (whether in electronic or paper form) under Section 4.50(a)¹¹⁷ or to prohibit access altogether under Section 4.60.¹¹⁸

The Committee concluded when it balanced all the factors outlined above that there may be a legitimate public interest in releasing social security numbers in full or part. Specifically, the release of full or partial social security numbers generally permits the users of court information to link a specific party with specific case information. That is, a social security number is used for “matching” purposes. However, the Committee maintains that the other identifiers that are releasable under this policy, such as full date of birth and partial address, will ensure that accurate matches of parties and case information can be made. In addition, the Committee is convinced that the release of any part of a social security number would cause an unjustified invasion of personal privacy as well as present a risk to personal security. Thus, the Committee recommends that the MDJS policy of restricting the release of any part of a social security number should be continued.

Operator License Numbers

The Committee notes that the MDJS policy provides that the AOPC will not release operator license numbers.¹¹⁹ The Committee found no controlling legal authority that would prohibit a court and/or office from redacting operator license numbers from an electronic case record prior to its release to the public. However, several statutes were of interest to the Committee in analyzing this issue.

First, the Driver’s Privacy Protection Act¹²⁰ (DPPA) provides that a state department of motor vehicles, and any officer, employee, or contractor, thereof, shall not knowingly disclose or otherwise make available to any person or entity personal information about any individual

¹¹² WASH. CT. GR. 31 (2006). Parties required to omit or redact social security numbers prior to filing documents with the court, except as provided in General Rule 22. Rule 22 provides that in family law and guardianship court records social security numbers are restricted personal identifiers, and as such not generally accessible to the public.

¹¹³ MN ST ACCESS TO REC RULE 8(2)(b)(1) (WEST 2006). Specifically, Rule 8(2)(b)(1) provides that remote access to social security numbers of parties, their family members, jurors, witnesses, or victims in electronic records will not be allowed.

¹¹⁴ *Policy Statement by the Justices of the Supreme Court Judicial Court Concerning Publications of Court Case Information on the Web*, (May 2003), p. 3, subsection (A)(6) which provides in part that no information regarding an individual’s social security number should appear on the Court Web site.

¹¹⁵ Kansas Rules Relating to District Courts Rule 196(d)(3) “[d]ue to privacy concerns, some otherwise public information, as determined by the Supreme Court, may not be available through electronic access. A nonexhaustive list of information generally not available electronically includes Social Security numbers....”

¹¹⁶ *Kentucky Court of Justice Access to Electronic Court Records* (December 2003) provides in part that “we decided to remove the individual’s...social security number...from public remote access.”

¹¹⁷ *CCJ/COSCA Guidelines*, p. 40.

¹¹⁸ *CCJ/COSCA Guidelines*, p. 45.

¹¹⁹ See MDJS policy, Section II.B.2.a.

¹²⁰ 18 U.S.C. §§ 2721-2725 (2006).

obtained by the department in connection with a motor vehicle record.¹²¹ The DPPA defines personal information as “information that identifies an individual, including an individual’s photograph, social security number, driver identification number....”¹²² The AOPC has reviewed the DPPA previously and determined that it is inapplicable to the judiciary and its electronic case records.

Second, the Pennsylvania Vehicle Code provides that “it is unlawful for [a]ny police officer, or any officer, employee or agent of any Commonwealth agency or local authority which makes or receives records or reports required to be filed under [title 75] to sell, publish or disclose or offer to sell, publish or disclose records or reports which relate to the driving record of any person.”¹²³ In addition, this statute provides “it is unlawful for [a]ny person to purchase, secure or procure or offer to purchase, secure or procure records or reports described [above].”¹²⁴ It appears that in order for this statute to be applicable to case records, the judiciary would have to be considered a “Commonwealth Agency.” There is no definition in Title 75 for a “Commonwealth Agency.” However, the Committee reviewed many other statutes that do define Commonwealth Agency and in its opinion the judiciary would not be considered a Commonwealth Agency under any of these definitions. Therefore, this statute is inapplicable to the courts and related offices. However, the spirit of this statute, as well as the DPPA, clearly conveys that in Pennsylvania the government should not be releasing operator license numbers to the public.

Moreover, the Committee’s research revealed that the states of California,¹²⁵ Florida,¹²⁶ Vermont,¹²⁷ and Washington¹²⁸ do not permit the release of operator license numbers.

Security issues may be raised if a person’s operator license number is used in conjunction with other personal identifiers. Specifically, if one knows some basic personal information about another such as his/her name, date of birth, and operator license number, he/she could alter the other’s driver and vehicle information maintained by PennDOT.

In addition to identity theft, personal safety is also an issue. Threats to personal safety were documented in numerous incidents that lead to the enactment of the DPPA. Specifically:

[i]n 1989 actress Rebecca Schaeffer was killed by an obsessed fan. The fan was able to locate Schaeffer’s home after he hired a private investigator who obtained the actress’s address by accessing her California motor vehicle record, which was open to public

¹²¹ 18 U.S.C. § 2721(a)(1) (2006).

¹²² 18 U.S.C. § 2725(3) (2006).

¹²³ 75 PA. CONS. STAT. § 6114(a)(1) (2006).

¹²⁴ 75 PA. CONS. STAT. § 6114(a)(2) (2006).

¹²⁵ CAL. CT. R. 2077(c)(11) provides that “the following information must be excluded from a court’s electronic calendar, index, and register of actions: (11) driver license numbers” before public access is permitted.

¹²⁶ Order of Supreme Court of Florida, No. AOSO04-4 (February 12, 2004). Specifically, the Order lists information that shall be accessible in electronic format to the public. Operator license numbers are not listed in the Order.

¹²⁷ VERMONT RULES GOVERNING DISSEMINATION OF ELECTRONIC CASE RECORDS RULE §3(b).

¹²⁸ WASH. CT. GR. 31 (2006). Parties required to omit or redact driver’s license numbers prior to filing documents with the court, except as provided in General Rule 22. Rule 22 provides that in family law and guardianship court records social security numbers are restricted personal identifiers, and as such not generally accessible to the public.

inspection. As a result, the State of California restricted the dissemination of such information to specified recipients. In addition to the Schaeffer murder, public access to personal information contained in motor vehicle records allowed antiabortion groups to contact abortion clinic patients and criminals to obtain addresses of owners of expensive automobiles.¹²⁹

The Committee concluded when it balanced all the factors outlined above that there may be a legitimate public interest in releasing operator license numbers, specifically ensuring that the “right” party is matched with the “right” case information. However, the Committee maintains that the other identifiers that are releasable under this policy, such as full date of birth and partial address, will ensure that accurate matches of parties and case information can be made. In addition, the Committee is convinced that the release of operator license numbers would cause unjustified invasions of personal privacy as well as present risks to personal security. Thus, the Committee recommends that the MDJS policy provisions restricting the release of operator license numbers should be continued.

Victim Information

The Committee notes that the MDJS policy provides that “names of juvenile victims of abuse” shall not be released.¹³⁰ Additionally, it is noted that the CCJ/COSCA Guidelines state that “parts of the court record, or pieces of information (as opposed to the whole case file) for which there may be a sufficient interest to prohibit public access [include] name, address, telephone number, e-mail, or places of employment of a victim, particularly in a sexual assault case, stalking or domestic violence case...”¹³¹

Additionally, the Committee notes that several states, such as California,¹³² Florida,¹³³ Indiana,¹³⁴ Minnesota,¹³⁵ Massachusetts,¹³⁶ as well as the federal government¹³⁷ (concerning

¹²⁹ Robert C. Lind, Natalie B. Eckart, *The Constitutionality of the Driver’s Privacy Protection Act*, 17 Communication Lawyer 18 (1999).

¹³⁰ See MDJS policy, Section II.B.2.b. This prohibition is pursuant to 42 PA. CONS. STAT. § 5988(a) which provides that “[i]n a prosecution involving a child victim of sexual or physical abuse, unless the court otherwise orders, the name of the child victim shall not be disclosed by officers or employees of the court to the public, and any records revealing the name of the child victim will not be open to public inspection.”

¹³¹ See *CCJ/COSCA Guidelines*, p. 48.

¹³² CAL. CT. R. 2077(c)(5) provides that “the following information must be excluded from a court’s electronic calendar, index and register of actions: (5) victim information” before public access is permitted.

¹³³ Order of Supreme Court of Florida, No. AOSO04-4 (February 12, 2004). Specifically, the Order lists information that shall be accessible in electronic format to the public. Victim information is not listed in the Order.

¹³⁴ IND. ADMIN. R. 9(G)(1)(e). Specifically, the Rule provides that case records excluded from public access information that tends to explicitly identify victims, such as addresses, phone numbers, and dates of birth.

¹³⁵ MN ST ACCESS TO REC RULE 8(2)(b) (WEST 2006). Remote access in electronic records to a victim’s social security number, street address, telephone number, financial account numbers or information that specifically identifies the individual or from which the identity of the individual could be ascertained is prohibited.

¹³⁶ *Policy Statement by the Justices of the Supreme Judicial Court Concerning Publications of Court Case Information on the Web* (May 2003), p. 2. The policy provides that the trial court web site should not list any information that is likely to identify victims.

¹³⁷ Title 18 U.S.C.A. § 2265(d)(3) provides that “[a] State...shall not make available publicly on the Internet any information regarding the registration or filing of a protection order, restraining order, or injunction in either the issuing or enforcing State...if such publication would be likely to publicly reveal the identity or location of the party protected under such order. A

victims in protection from abuse cases) have enacted or proposed public access policies or court rules that would prohibit the release of victim information.

The Committee concluded that although there may be a legitimate public interest in releasing victim information, such as alerting the community as to whom crimes are being committed against and where crimes are being committed, it is outweighed by the interest of protecting the victim. The Committee, therefore, opines that the release of victim information including name, address and other contact information may result in intimidation or harassment of those individuals who are victims of a crime and would cause unjustified invasions of personal privacy as well as present risks to personal security. Thus, the Committee recommends that the MDJS policy provisions restricting the release of victim information should be continued.

Informant Information

The Committee asserts that information about an informant should not be released in that doing so could put the informant and/or law enforcement personnel who may be working with an informant at risk of harm, as well as possibly impede ongoing criminal investigations. Although the Committee could not find any court policies or rules that would specifically prohibit the release of informant information, the Committee notes that several states, such as Florida,¹³⁸ Minnesota,¹³⁹ and Massachusetts¹⁴⁰ have enacted or proposed public access policies or court rules that would prohibit the release of informant information, if the informant is a witness on the case. Additionally, the CCJ/COSCA Guidelines provide that parts of the court record, or pieces of information (as opposed to the whole case file) for which there may be a sufficient interest to prohibit public access “[include] name, address, or telephone number of informants in criminal cases.”¹⁴¹

The Committee concluded when it balanced all the information outlined above that it was hard pressed to find a legitimate public interest in releasing informant information. The release of this information would be an unjustified invasion of personal privacy as well as present risks to personal security. Thus, the Committee recommends informant information should not be released.

State...may share court-generated and law enforcement-generated information contained in secure, government registries for protection order enforcement purposes.”

¹³⁸ Order of Supreme Court of Florida, No. AOSO04-4 (February 12, 2004). Specifically, the Order lists information that shall be accessible in electronic format to the public. Informant information is not listed in the Order.

¹³⁹ MN ST ACCESS TO REC RULE 8(2)(b) (WEST 2006). Remote access in electronic records to a witness’ social security number, street address, telephone number, financial account numbers or information that specifically identifies the individual or from which the identity of the individual could be ascertained will not be allowed.

¹⁴⁰ *Policy Statement by the Justices of the Supreme Judicial Court Concerning Publications of Court Case Information on the Web*, (May 2003), p. 2. The policy provides that the trial court web site should not list any information that is likely to identify witnesses (except for expert witnesses).

¹⁴¹ *CCJ/COSCA Guidelines*, p. 48.

Juror Information

The Committee notes that the CCJ/COSCA Guidelines state that “parts of the court record, or pieces of information (as opposed to the whole case file) for which there may be a sufficient interest to prohibit public access [include] names, addresses, or telephone numbers of potential or sworn jurors in a criminal case...[and] juror questionnaire information.”¹⁴² In addition, the Committee notes that Rule 630 of the Pennsylvania Rules of Criminal Procedure sets forth that “[t]he information provided on the juror qualification form shall be confidential” and further provides that “[t]he original and any copies of the juror qualification form shall not constitute a public record.”¹⁴³

Rule 632 of the Pennsylvania Rules of Criminal Procedure provides that “[t]he information provided by the jurors on the questionnaires shall be confidential and limited to use for the purpose of jury selection only....”¹⁴⁴ Rule 632 also sets forth that “the original and any copies of the juror information questionnaire shall not constitute a public record.”¹⁴⁵ Further, it states “[t]he original questionnaire of all impaneled jurors shall be retained in a sealed file and shall be destroyed upon completion of the juror’s service, unless otherwise ordered by the trial judge.”¹⁴⁶ The Rule also provides that “[t]he original and any copies of questionnaires of all prospective jurors not impaneled or not selected for any trial shall be destroyed upon completion of the jurors’ service.”¹⁴⁷

In addition, in the case of Commonwealth v. Karl Long,¹⁴⁸ the Superior Court held that there is no constitutional or common law right of access to the names and addresses of jurors. Further, the Court noted that:

“a number of states have enacted legislation with the intent to protect jurors’ privacy. New York has adopted legislation to protect the privacy of jurors by keeping empanelled jurors’ names and addresses confidential. N.Y. Judiciary Law C § 509(a)(2003); see also Newsday, Inc. v. Sise, 524 N.Y.S.2d 35, 38-89 (N.Y. 1987). Delaware has also enacted juror privacy legislation. Del.Code Ann. Tit. 10 § 4513; also Gannett, 571 A.2d 735 (holding that the media did not have the right to require announcement of juror’s names during the highly publicized trial, even though the parties have full access to such information and the proceedings are otherwise open to the public). Indiana legislation provides that the release of names and identifying information of potential jurors is within the discretion of the trial judge. Ind.Code § 2-210(5).”¹⁴⁹

¹⁴² Id.

¹⁴³ P.A.R.CRIM.P. 630(A)(2), (3).

¹⁴⁴ P.A.R.CRIM.P. 632(B).

¹⁴⁵ P.A.R.CRIM.P. 632(C).

¹⁴⁶ P.A.R.CRIM.P. 632(F).

¹⁴⁷ P.A.R.CRIM.P. 632(G).

¹⁴⁸ Please note that the Supreme Court has granted a petition for allowance of appeal in this matter. For more information, please see 884 A.2d 248-9 and 39-40 WAP 2005. See also Jury Service Resource Center v. De Muniz, --P.3d--, 2006 WL 1101064 (April 27, 2006)(Oregon Supreme Court held that the First Amendment did not require state and county officials to give full access to jury pool records).

¹⁴⁹ Id. At p. 7.

Moreover, the Committee notes that several states, such as Vermont,¹⁵⁰ Idaho,¹⁵¹ Maryland,¹⁵² Arizona,¹⁵³ Minnesota,¹⁵⁴ and Utah¹⁵⁵ have enacted or proposed public access policies or court rules that would prohibit the release of some or all juror information.

In February 2005, the American Bar Association's House of Delegates approved a series of model jury principles.¹⁵⁶ Principle 7 addresses the need for juror privacy when consistent with the requirements of justice and the public interest. More specifically, principle 7 recommends that juror addresses and phone numbers be kept under seal.¹⁵⁷

In Pennsylvania, section 4524 of the Judicial Code provides with respect to the jury selection commission that "[a] separate list of names and addresses of persons assigned to each jury array shall be prepared and made available for public inspection at the offices of the commission no later than 30 days prior to the first date on which the array is to serve."

Therefore, the Committee concluded that existing Pennsylvania legal authority as cited above requires that juror information contained in electronic case records shall not be released to the public. Moreover, the Committee notes that such a result appears to be consistent with the approach taken by other states.

¹⁵⁰ VERMONT RULES FOR PUBLIC ACCESS TO COURT RECORDS RULE 6(b)(30). This subsection provides that "the public shall not have access to the following judicial branch records...records with respect to jurors or prospective jurors as provided in Rules Governing Qualification, List, Selection and Summoning of All Jurors."

¹⁵¹ IDAHO RULES GOVERNING THE ADMINISTRATION AND SUPERVISING OF THE UNIFIED AND INTEGRATED IDAHO JUDICIAL SYSTEM, RULE 32(d)(5)&(6) records exempt from disclosure include "records of...the identity of jurors of grand juries" and "the names of jurors placed in a panel for a trial of an action and the contents of jury qualification forms and jury questionnaires for these jurors, unless ordered to be released by the presiding judge."

¹⁵² Maryland Rule of Procedure 16-1004(B)(2) provides that "...a custodian shall deny inspection of a court record used by the jury commissioner or clerk in connection with the jury selection process. Except as otherwise provided by court order, a custodian may not deny inspection of a jury list sent to the court pursuant to Maryland Rules 2-512 or 4-312 after the jury has been empanelled and sworn."

¹⁵³ ARIZ. R. 123 Public Access to the Judicial Records of the State of Arizona, Subsection (e)(9) provides that "the home and work telephone numbers and addresses of jurors, and all other information obtained by special screening questionnaires or in voir dire proceedings that personally identifies jurors summoned for service, except the names of jurors on the master jury list, are confidential, unless disclosed in open court or otherwise opened by order of the court."

¹⁵⁴ MN ST ACCESS TO REC RULE 8(2)(b) (WEST 2006). Remote access in electronic records to a juror's social security number, street address, telephone number, financial account numbers or information that specifically identifies the individual or from which the identity of the individual could be ascertained will not be allowed.

¹⁵⁵ UTAH J. ADMIN. R. 4-202.02(2)(k) provides that "public court records include but are not limited to: name of a person other than a party, but the name of a juror or prospective juror is private unless released by a judge." Moreover, subsection (4)(i) of the same Rule provides that "the following court records are private; the following personal identifying information about a person other than a party; address, email address, telephone number, date of birth, driver's license number, social security number, account description and number, password, identification number, maiden name and mother's maiden name." Rule 4-202-03 provides who has access to private records which in general appears not to be the public.

¹⁵⁶ <http://abanet.org/juryprojectstandards/principles.pdf>.

¹⁵⁷ Stellwag, Ted. "The Verdict on Juries." *The Pennsylvania Lawyer*, pp. 15, 20. May-June 2005 (quoting the chairperson of the American Jury Project to say "jurors 'should not have to give up their privacy...to do their public service.'").

Party's Address

The Committee notes that the MDJS policy provides that AOPC will not release the addresses of parties.¹⁵⁸ The Committee notes that the CCJ/COSCA Guidelines state that “additional categories of information to which a state or individual court might also consider restricting general public access include: addresses of litigants in cases....”¹⁵⁹

In addition, several states and the federal courts¹⁶⁰ have enacted or proposed public access policies or court rules that would prohibit the release of a party address or permit the release of only a partial address. Those states include: Indiana,¹⁶¹ Minnesota,¹⁶² Massachusetts,¹⁶³ Kansas¹⁶⁴, Kentucky¹⁶⁵ and Vermont.¹⁶⁶ In addition, some federal courts have begun releasing only a partial address as well.¹⁶⁷ Furthermore, the Committee notes that in Sapp Roofing Co. v. Sheet Metal Workers' Int'l¹⁶⁸ and Barger v. Dep't of Labor and Indus.,¹⁶⁹ Pennsylvania courts held that a home address falls under the personal security provision of the RTKA and thus should not be released pursuant to a request under the RTKA.

The Committee was faced with three choices: to release a full address, to release a partial address, or to restrict access to addresses. The Committee asserts that there is a legitimate public interest in releasing a party's address, specifically ensuring that the “right” party is matched with the “right” case information. However, the Committee is concerned that

¹⁵⁸ See MDJS policy, Section II.B.2.a.

¹⁵⁹ See CCJ/COSCA Guidelines, p. 49.

¹⁶⁰ *Remote Public Access to Electronic Case Records: A Report on a Pilot Project in Eleven Federal Courts*, prepared by the Court Administration and Case Management Committee of the Judicial Conference, p. 12. Although there is no restriction on the release of a party's address in civil cases, the pilot program in the eleven federal courts to provide public access to criminal case files electronically requires the redaction of all home addresses including those of parties.

¹⁶¹ IND. ADMIN. R 9(F)(4)(d) provides that a request for bulk distribution and compiled information of case records that includes a request for addresses will be complied with by only providing the zip code of the addresses. However, Rule 9(G)(1)(e) provides that “[t]he following information in case records is excluded from public access and is confidential...addresses...[of] witnesses or victims in criminal, domestic violence, stalking, sexual assault, juvenile, or civil protection order proceedings....”

¹⁶² MN ST ACCESS TO REC RULE 8(2)(b)(2) (WEST 2006). Remote access in electronic records to a party's street address will not be allowed.

¹⁶³ *Policy Statement by the Justices of the Supreme Judicial Court Concerning Publications of Court Case Information on the Web* (May 2003), p. 3. The policy provides that the trial court web site should not list an individual's address.

¹⁶⁴ Kansas Rules Relating to District Courts Rule 196(d)(3) “[d]ue to privacy concerns, some otherwise public information, as determined by the Supreme Court, may not be available through electronic access. A nonexhaustive list of information generally not available electronically includes street addresses...”

¹⁶⁵ *Kentucky Court of Justice Access to Electronic Court Records* (December 2003) provides in part that “we decided to remove the individual's address...from public remote access.”

¹⁶⁶ VERMONT RULES GOVERNING DISSEMINATION OF ELECTRONIC CASE RECORDS RULE §3(b).

¹⁶⁷ See also Local Rules of Practice for the Southern District of California Order 514-C(1)(e) which provides that “in criminal cases, the home address of any individual (i.e. victim)” is required to be removed or redacted from all pleadings filed with the court. Eastern District of Pennsylvania Local Rule 5.1.2 (electronic case file privacy) which provides in a part that in criminal cases parties should refrain from including or partially redacting home addresses from all documents filed with the court. (“If a home address must be included, only the city and state should be listed”).

¹⁶⁸ 713 A.2d 627, 630 (Pa. 1998).

¹⁶⁹ 720 A.2d 500, 502 (Pa.Comm. Ct. 1998).

releasing the entire address would cause an unjustified invasion of personal privacy as well as present a risk to personal security.

Therefore, when coupled with other identifiers accessible under this Policy, the Committee opines that the release of a partial address (city, state, and zip code only) will facilitate a requestor's need to match the "right" party with the "right" case while at the same time not raise any significant issues of personal privacy or security. Thus, the Committee recommends the same.

Witness Information

The Committee notes that the MDJS Policy provides that AOPC will not release the following information about a witness: address, social security number, telephone number, fax number, pager number, driver's license number, SID number or other identifier that would present a risk to the witness' personal security or privacy.¹⁷⁰ In addition, the Committee notes that the CCJ/COSCA Guidelines state that "parts of the court record, or pieces of information (as opposed to the whole case file) for which there may be a sufficient interest to prohibit public access" include addresses of witnesses (other than law enforcement personnel) in criminal or domestic violence protective order cases.¹⁷¹ The Committee also notes that several states have enacted or proposed public access policies or court rules that would prohibit the release of witness information. Those states include: California,¹⁷² Florida,¹⁷³ Indiana,¹⁷⁴ Minnesota,¹⁷⁵ and Massachusetts.¹⁷⁶

The Committee concluded when it balanced all the information outlined above that there may be a legitimate public interest in releasing witness information, specifically that the public's ability to ascertain who testified at a public trial. However, the Committee is convinced that the release of witness information including name, address and other contact information may result in intimidation or harassment of the witnesses and thus would be an unjustified invasion of personal privacy as well as present a risk to personal security. Thus, the Committee recommends that the MDJS policy provisions restricting the release of victim information should be extended to witnesses.

¹⁷⁰ See MDJS policy, Section II.B.2.a.

¹⁷¹ See *CCJ/COSCA Guidelines*, p. 48.

¹⁷² CAL. CT. R. 2077(c)(6) provides that "the following information must be excluded from a court's electronic calendar, index and register of actions: (6) witness information" before public access is permitted.

¹⁷³ Order of Supreme Court of Florida, No. AOSO04-4 (February 12, 2004). Specifically, the Order lists information that shall be accessible in electronic format to the public. Witness information is not listed in the Order.

¹⁷⁴ IND. ADMIN. R. 9(G)(1)(e). Specifically, the Rule provides that case records excluded from public access information that tends to explicitly identify witnesses, such as addresses, phone numbers, and dates of birth.

¹⁷⁵ MN ST ACCESS TO REC RULE 8(2)(b) (WEST 2006). Remote access in electronic records to a witness' social security number, street address, telephone number, financial account numbers or information that specifically identifies the individual or from which the identity of the individual could be ascertained is prohibited.

¹⁷⁶ *Policy Statement by the Justices of the Supreme Judicial Court Concerning Publications of Court Case Information on the Web* (May 2003), p. 2. The policy provides that the trial court web site should not list any information that is likely to identify witnesses except for expert witnesses.

SID Numbers

A SID number (or a state identification number) is a unique identifying number that is assigned by the Pennsylvania State Police (PSP) providing for specific identification of an individual through analysis of his/her fingerprints. The PSP does not release SID numbers to the public on the basis that SID numbers are criminal history record information, the release of which is controlled by the Criminal History Record Information Act (CHRIA).¹⁷⁷ Moreover, the MDJS policy provides in part that “[t]he following information will not be released:…state fingerprint identification number (SID).”¹⁷⁸

The Committee found it very instructive that the PSP does not release SID numbers to the public on the basis that SID numbers are criminal history record information, the release of which is controlled by CHRIA. Therefore, the Committee is not convinced that there is a legitimate public interest in releasing SID numbers. Therefore, the Committee recommends that the MDJS Policy of not releasing SID numbers be continued.

Financial Institution Account Numbers, Credit Card Numbers, PINS or Passwords Used to Secure Accounts

The Committee maintains when an individual provides the court or office with a financial institution account number (e.g., banking account number) and/or a credit card number that they should not be released to the public because of the financial harm that can result. The CCJ/COSCA Guidelines provide in part that examples of “documents, parts of the court record, or pieces of information (as opposed to the whole case file) for which there may be a sufficient interest to prohibit public access [include f]inancial information that provide identifying account numbers on specific assets, liabilities, accounts, credit cards, or personal identification numbers (PINs) of individuals or business entities.”¹⁷⁹ In addition, the Committee notes that the federal courts¹⁸⁰ and several states, such as Arizona,¹⁸¹ California,¹⁸² Colorado,¹⁸³ Florida,¹⁸⁴ Indiana,¹⁸⁵

¹⁷⁷ 18 PA. CONS. STAT. § 9101 et. seq.

¹⁷⁸ See MDJS Policy, Section II.B.2.a.

¹⁷⁹ See *CCJ/COSCA Guidelines*, p. 48.

¹⁸⁰ *Remote Public Access to Electronic Case Records: A Report on a Pilot Project in Eleven Federal Courts*, prepared by the Court Administration and Case Management Committee of the Judicial Conference, p. 12 and the *Report of the Judicial Conference Committee on Court Administration and Case Management on Privacy and Public Access to Electronic Case Files*, p. 3. With regard to Judicial Conference’s recommendation for public access to civil case files electronically and the pilot program in the eleven federal courts to provide public access to criminal case files electronically, both require that only the last four digits of the financial account number are releasable. See also Local Rules of Practice for the Southern District of California Order 514-C(1)(d) and Eastern District of Pennsylvania Local Rule of Civil Procedure 5.1.3.

¹⁸¹ ARIZ. SUP. CT. R. 123(c)(3). The Rule provides that “documents containing…credit card, debit card, or financial account numbers or credit reports of an individual, when collected by the court for administrative purposes, are closed unless made public in a court proceeding or upon court order.” Arizona Rule 123 Public Access to the judicial records of the state, and *Report and Recommendation of the Ad Hoc Committee to Study Public Access to Electronic Records* dated March 2001 Sections (IV)(B), (IV)(D), (V)(1) and (VI)(6).

¹⁸² CAL. CT. R. 2077(c)(2) which provides that “the following information must be excluded from a court’s electronic calendar, index, and register of actions: (2) any financial information” before public access is permitted.

¹⁸³ Colo. CJD. 05-01 Section 4.60(b) provides that “the following information in court records is not accessible in electronic format due to the inability to protect confidential information. It may be available at local courthouses…financial files – everything except for the financial summary screen.”

Minnesota,¹⁸⁶ New York,¹⁸⁷ and Vermont¹⁸⁸ either prohibit the release of this information entirely or only permit the partial release of this information (i.e., the last four digits).

The Committee opines that there is no legitimate public interest in obtaining financial account, credit card information, PINS or passwords used to secure accounts. Using the balancing test, the analysis would be concluded. In addition, the Committee stresses that releasing this information will further the threat of identity theft. The Committee, therefore, recommends that financial account and credit card information shall not be released.

Notes, Drafts, and Work Products Related to Court Administration or any Office that is the Primary Custodian of an Electronic Case Record

The Committee notes that several states including: Arizona,¹⁸⁹ Idaho,¹⁹⁰ Indiana,¹⁹¹ Minnesota,¹⁹² Vermont,¹⁹³ and Utah¹⁹⁴ have a similar provision regarding notes, drafts, and work products related to court administration or any office that is the primary custodian of an electronic case record. In addition, the CCJ/COSCA Guidelines provide in part that examples of “documents, parts of the court record, or pieces of information (as opposed to the whole case file) for which there may be a sufficient interest to prohibit public access [include] judicial, court administration and clerk of court work product.”¹⁹⁵

¹⁸⁴ Order of Supreme Court of Florida, No. AOSO04-4 (February 12, 2004). Specifically, the Order lists information that shall be accessible in electronic format to the public. Financial account numbers and credit card numbers are not listed in the Order.

¹⁸⁵ IND. ADMIN. R. 9(G)(1)(f). Specifically, the Rule provides that account numbers of specific assets, liabilities, accounts, credit cards, and personal identification numbers (PINS) shall not be released.

¹⁸⁶ MN ST ACCESS TO REC RULE 8(2)(b)(4) (WEST 2006). Remote access in electronic records to financial account numbers of parties or their family members, witnesses, jurors, or victims of criminal or delinquent acts is prohibited.

¹⁸⁷ *Report to the Chief Judge of the State of New York* by the Commission on Public Access to Court Records (February, 2004), p. 8. The Report provides that financial account numbers should be shortened to their last four digits.

¹⁸⁸ VERMONT RULES FOR PUBLIC ACCESS TO COURT RECORDS RULE 6(b)(10) & (11). These Rules provide that the public shall not have access to records containing financial information furnished to the court in connection with an application to proceed in forma pauperis (not including the affidavit submitted in support of the application) and records containing financial information furnished to the court in connection with an application for an attorney at public expense (not including the affidavit submitted in support of the application). See also VERMONT RULES GOVERNING DISSEMINATION OF ELECTRONIC CASE RECORDS RULE §3(b).

¹⁸⁹ PUBLIC ACCESS TO THE JUDICIAL RECORDS OF THE STATE OF ARIZONA, Rule 123(d)(3) provides that “notes, memoranda or drafts thereof prepared by a judge or other court personnel at the direction of a judge and used in the process of preparing a final decision or order are closed.”

¹⁹⁰ IDAHO ADMIN. R. 32(d)(15). This Rule provides that judicial work product or drafts, including all notes, memoranda or drafts prepared by a judge or a court-employed attorney, law clerk, legal assistant or secretary and used in the process of preparing a final decision or order except the official minutes prepared pursuant to law are not accessible by the public.

¹⁹¹ IND. ADMIN. R. 9(G)(1)(h). Specifically, the Rule provides that case records excluded from public access include all personal notes and email, and deliberative material, of judges, court staff and judicial agencies.

¹⁹² MN ST ACCESS TO REC RULE 4(1)(c) (WEST 2006). Case records that are not accessible by the public include “all notes and memoranda or drafts thereof prepared by a judge or by a court employed attorney, law clerk, legal assistant or secretary and used in the process of preparing a final decision or order....”

¹⁹³ VERMONT RULES FOR PUBLIC ACCESS TO COURT RECORDS RULE 6(b)(12). These Rules provide that “records representing judicial work product, including notes, memoranda, research results, or drafts prepared by a judge or prepared by other court personnel on behalf of a judge, and used in the process of preparing a decision or order” are not available for public access.

¹⁹⁴ UTAH J. ADMIN. R. 4-202.02(5)(H) provides that “the following court records are protected... memorandum prepared by staff for a member of any body charged by law with performing a judicial function and used in a decision making process.”

¹⁹⁵ See *CCJ/COSCA Guidelines*, p. 48-49.

The CCJ/COSCA Guidelines define judicial work product as:

work product involved in the court decisional process, as opposed to the decision itself. This would include such things as notes and bench memos prepared by staff attorneys, draft opinions and orders, opinions being circulated between judges, etc. Any specification about this should include independent contractors working for a judge or the court, externs, students, and others assisting the judge who are not employees of the court or the clerk of court's office.¹⁹⁶

Court administration and clerk of court work product is defined by the CCJ/COSCA Guidelines as "information...generated during the process of developing policy relating to the court's administration of justice and its operations."¹⁹⁷ The Guidelines indicate that court administration information that other states have excluded from public access include: communication logs of court personnel, meeting minutes, and correspondence of court personnel.¹⁹⁸

Although the Committee will not attempt to list every piece of information that will not be released pursuant to this provision, the Committee would note the following. This provision would prohibit the release of information pertaining to the internal operations of a court, such as data recorded in the case notes or judicial notes portions of the automated systems wherein the court and court staff can record various work product and confidential information and help desk records.

The Committee when it balanced all the factors outlined above concluded that there is no legitimate public interest in releasing this type of information. Therefore, the Committee asserts that the same should not be released.

Information Sealed or Protected Pursuant to Court Order

If there is a court order that seals a case record or information contained within that case record, the same shall not be released to the public. The Committee notes that New York¹⁹⁹ has proposed and Maryland²⁰⁰ has adopted a similar prohibition.

¹⁹⁶ See *CCJ/COSCA Guidelines*, p. 50.

¹⁹⁷ See *CCJ/COSCA Guidelines*, p. 50.

¹⁹⁸ See *CCJ/COSCA Guidelines*, p. 51. See also ARIZ. SUP. CT. R. 123(e) (restricting access to *inter alia* judicial case assignments, pre-decisional documents, and library records); CAL. CT. R. 2072(a) (excluding personal notes or preliminary memoranda of court personnel from definition of court record); FLA. J. ADMIN. R. 2.051(c) (keeping confidential *inter alia* materials prepared as part of the court's judicial decision-making process utilized in disposing of case and controversies unless filed as a part of the court record); *Report to the Chief Judge of the State of New York* by the Commission on Public Access to Court Records (February 2004), p. 1, ftnt. 2 which indicates that information captured by a case tracking system that is for internal use only is not deemed to be public case record data; proposed amendment to VERMONT RULES FOR PUBLIC ACCESS TO COURT RECORDS RULE 5(b)(14) (restricting access to *inter alia* "communications between judicial branch personnel with regard to internal operations of the court, such as scheduling of cases, and substantive or procedural issues.").

¹⁹⁹ *Report to the Chief Judge of the State of New York* by the Commission on Public Access to Court Records (February, 2004), p. 22 which provides that "sealed records may not be viewed by the public."

²⁰⁰ Maryland Rule of Procedure 16-1006(J)(1) which provides that "the custodian shall deny inspection of...a case record that: a court has ordered sealed or not subject to inspection...."

Information to which Access is Restricted by Federal Law, State Law or State Court Rule

This policy cannot supplant federal law, state law, or state court rule. Thus, if information is not releasable to the public pursuant to such authorities, the information cannot be released. The Committee did not specifically set forth in the policy each federal law, state law, or state court rule that prohibits the release of information to the public in that it suspects that to do so would require an amendment to the policy every time a law or rule was changed.²⁰¹

Information Presenting a Risk to Personal Security, Personal Privacy, or the Fair, Impartial and Orderly Administration of Justice, as Determined by the Court Administrator of Pennsylvania with the Approval of the Chief Justice.

The MDJS policy provides that “the following information will not be released:...other identifiers which would present a risk to personal security or privacy.”²⁰² Moreover, the RTKA provides that the definition of “public records” does not include “any record...which would operate to the prejudice or impairment of a person’s reputation or personal security....”²⁰³

The Committee is mindful that it is difficult to anticipate every possible public access consideration, whether related to technology, administration, security or privacy, that might arise upon implementation of a policy. Moreover, resolution of issues that may have statewide impact need to be resolved in a timely and unified fashion.

For example, in the recent past, law enforcement and court personnel raised security concerns with the AOPC about the release of certain MDJS data that jeopardized the safety of police officers and the administration of justice. The aforementioned MDJS policy provision permitted the Court Administrator to review the specific concerns and quickly take action to remedy the situation. The result being a more narrowly tailored access to MDJS criminal case data for bulk requestors that balanced the interests of transparency, security and operations of the court system. In a system as vast as ours, it is critical that such measures can be taken in a coordinated and effective manner.

It is important to note that other state court systems’ policies and rules have similarly provided for the need to promptly address unanticipated privacy and security concerns. See *[Massachusetts] Policy Statement by the Justices of the Supreme Judicial Court Concerning Publications of Court Case Information on the Web* (May 2003), p. 3; Kan.Sup.Ct. Rule 196(d)(3).

The Committee is cognizant that providing a “catchall” provision such as this could lead to a perception of overreaching, and due consideration was given before offering this

²⁰¹ See, e.g., 42 Pa.C.S. §§ 6307, 6352.1 and Pa.R.J.C.P. 160 (providing limitations on the release of juvenile case record information).

²⁰² See MDJS Policy, Section II.B.2.a.

²⁰³ PA. STAT. ANN. tit. 65, § 66.1 (West 2006).

recommendation. Notwithstanding, it is believed that such a provision used in judicious fashion is absolutely necessary to the successful implementation of this policy, as has been the case with the MDJS.