



ADMINISTRATIVE OFFICE of PENNSYLVANIA COURTS

**ELECTRONIC CASE RECORD
PUBLIC ACCESS POLICY
OF THE UNIFIED JUDICIAL SYSTEM
OF PENNSYLVANIA**

**JANUARY 1, 2007
Amended January 1, 2013**

TABLE OF CONTENTS

ACKNOWLEDGMENTS	i
PROLOGUE	ii
POLICY	1
EXPLANATORY REPORT	7
Section 1.00 Definitions	20
Section 2.00 Statement of General Policy	25
Section 3.00 Electronic Case Record Information Excluded From Public Access	26
Section 3.10 Requests for Bulk Distribution of Electronic Case Records	42
Section 3.20 Requests for Electronic Case Record Information from Another Court or Office	45
Section 4.00 Responding To a Request for Access to Electronic Case Records	46
Section 5.00 Fees	48
Section 6.00 Correcting Data Errors	51
Section 7.00 Continuous Availability of Policy	55
Additional Recommendations Concerning Paper Case Records	56

ACKNOWLEDGMENTS

The Administrative Office of Pennsylvania Courts' Public Access Ad Hoc Committee would like to thank the many individuals and organizations who assisted our efforts in developing a proposed public access policy governing electronic case records. The Committee is particularly appreciative of the thoughtful comments that were offered in response to solicitations for public input. This input was extremely beneficial to the Committee as it refined its final proposal.

The Committee would also like to thank the many AOPC staff who tirelessly provided administrative and research assistance, specifically Deb Weber, Cynthia Screen, Kay Shaffer, Michael Callaghan, Erin Loucks, Shannon Black and Michael Crotty. The Committee is also grateful for the technical guidance and expertise offered by Amy J. Ceraso, Director of Judicial Automation, and her staff.

The Committee sincerely appreciates the guidance and wisdom offered by Chief Justice Emeritus Stephen A. Zappala, as the Committee worked toward developing final policy recommendations.

And finally, the Committee wishes to acknowledge the support, patience and foresight of Zygmunt Pines, Court Administrator of Pennsylvania, who recognized and stressed the critical importance of creating a thorough process to ensure the integrity of the courts' information while continuing to provide public access.

PROLOGUE

By

**Chief Justice Emeritus Stephen A. Zappala
Court Administrator of Pennsylvania Zygmunt A. Pines**

Efforts by the Administrative Office of Pennsylvania Courts (AOPC) to develop a proposed statewide public access policy for case records of the magisterial district courts, criminal divisions of the courts of common pleas and appellate courts commenced in 2002. Appointed by the Court Administrator of Pennsylvania, an internal AOPC ad hoc committee was established to accomplish the objective of crafting a policy that balances the equally important interests of transparency, privacy and security.

Initially, the Committee concentrated its labors in identifying the scope of the proposed policy, concluding that its sole focus should be on electronic case record information (i.e., data captured by the Unified Judicial System's appellate, criminal common pleas and magisterial district court case management systems). Information contained within the automated case management systems of the Unified Judicial System is not the official court file, but merely a derivative of that file. Electronic case record information supplements, but does not replace the official case file maintained by the court that has jurisdiction over the matter. Accordingly, the Committee preserves the concept of open records by permitting unrestricted access to paper case records, even though certain electronic case record information may be restricted, in whole or in part.

To assist in framing the issues attendant to an electronic case records public access policy, the AOPC looked to the pioneering work of 19 other state court systems and the federal judiciary, as well as the model guidelines for access to court records issued by the Conference of Chief Justices and Conference of State Court Administrators in 2002. These paradigms, in conjunction with analysis of case law, legislation, and journal articles, provided the underpinnings from which the Committee could construct a proposed policy. They also confirmed what the Committee suspected early on -- that its experience would be no different (that is, no less complicated) than that of other court systems.

During its pursuit of crafting a sound proposal, the Committee sought an annual opportunity to gather with those interested in the subject of public access to court records and keep abreast of the latest developments. This opportunity was presented at an annual conference on privacy and public access to court records in Williamsburg,

Virginia (hosted by William and Mary Law School, the National Center for State Courts and the Administrative Office of the United States Courts). Initiated in 2001, this conference is attended by jurists and staff from state and federal courts, law professors, access and privacy advocates, data collection companies, and others who are involved in efforts to develop policies on public access to court records.

In the summer of 2005, the Committee completed its task of developing a proposed policy. It recognized the critical importance of gathering public input, particularly from the citizens of Pennsylvania, about the proposal. Accordingly, on September 17, 2005, the proposed policy was published in the *Pennsylvania Bulletin* and on an interactive page of the Pennsylvania Judiciary's website (www.courts.state.pa.us) for a 60 day public comment period. A total of 70 comments were received – including responses from the general public, media, private attorneys, bar associations, public interest groups, data harvesters, government officials and staff.

The comments not only came from a wide range of constituencies but also expressed differing and quite frankly conflicting views. For example, some commentators contend that *absolutely no* case information should be available on the Internet whereas others suggest that *all* case information (including victim and witness information, social security numbers, etc.) should be available on the Internet. The Committee recognized that whatever policy is finally promulgated will be to the chagrin of some constituencies. Nonetheless, the Committee attempted to find as much “common ground” as it could in reviewing the various comments.

However, the Committee believed that additional public input was needed to assist it in resolving some issues on which a substantial number of comments were received, but the Committee required further information and in some cases clarification. Not surprisingly, many other court systems have struggled with these issues as well, usually only to arrive at different conclusions. The specific issues were:

- What specific amendments should be made to Section 6.00 (Correcting Data Errors) to delineate the procedure that an individual must follow to correct an error in an electronic case record?
- Whether providing electronic case record information that contains a party's full date of birth will sufficiently ensure that the “right” party is matched with the “right” case?
- Whether electronic case record information concerning pre-convictions should be available to the public?

The Committee received this additional public input through a public hearing held on March 2, 2006 at 9 a.m. in Courtroom 1 of the Commonwealth Court of Pennsylvania in Harrisburg's Capitol Complex.

The public hearing presented an opportunity to witness first-hand the divergent views taken by those who testified and the inherent difficulty in reconciling the interests of transparency and personal privacy/security in crafting a statewide policy. Despite a late winter storm, the public hearing provided the opportunity to hear from 21 individuals representing a wide variety of interests and perspectives.

In response to the extensive public comment received, the Committee recommends the following:

- Correction of Data Errors: Many comments received on the proposed policy indicated that the Section 6.00 (Correcting Data Errors) should provide specific procedures for requestors to follow. Specifically, it was suggested that this section set forth in detail the process by which an individual can ask a court or office to correct an alleged error in an electronic case record and the procedure that the court or office must follow in responding to said request. In response, the Committee has set forth a specific correction of data errors procedure that borrows heavily from the correction of errors section in the Criminal History Record Information Act (CHRIA).
- Date of Birth: An overwhelming number of those who commented on the proposed policy indicated that release of only a year of birth and age was not sufficient to match the “right” party with the “right” case. Many expressed concern that releasing only the year of birth would result in an innocent person being wrongly associated with criminal case records because s/he shares the same name and birth year as the defendant. Therefore, the Committee amended the report to provide that a party’s full date of birth is releasable.

As a correlative action, the Committee has removed Section 3.00(B) from the proposed policy. This section provided that the electronic case record information available at the public access terminal in the courthouse may include, in addition to all the other information that the policy deems accessible, a party’s full date of birth and address. As noted in the commentary, the Committee believed that providing this information would not greatly increase the risk of harm to an individual because one could only get this information if s/he traveled to the courthouse (recognizing that this information is already available at the courthouse in the paper files). In addition, the Committee noted that the benefit of providing these two additional pieces of information was to enable individuals to distinguish one “John Smith” from another without needing to review the paper file.

As noted above, the Committee has learned through written comments and testimony that providing access to the full date of birth will sufficiently accomplish the goal of permitting an individual to distinguish one individual from other given

all the other electronic case record information about the person and case that is releasable to the public. Therefore, the Committee does not believe that there is a need to provide a “higher” level of access to electronic case records at the courthouse. Thus, individuals accessing the public access terminal in the courthouse will have the same access to electronic case record information as those who are accessing the information remotely. If additional information is needed, the individual should review the official court record (paper file).

In addition, the Committee noted that in order to comply with the provisions of former Section 3.00(B) the AOPC’s Judicial Automation Department would have had to overcome some technological hurdles.

- Release of Preconviction Information: The Committee received many comments on both sides of this issue. Many comments set forth a concern that releasing this electronic case record information on the Internet will impede individuals who are arrested but not convicted of a crime in acquiring employment and housing. Other comments set forth that the public has a great interest in knowing when criminal charges are filed against a member of the public and therefore this information should be available. It has become apparent to the Committee that these views are diametrically opposed, and thus, there is no middle ground to be had.

The Committee informally surveyed 16 other state court systems and the federal judiciary to ascertain how they have resolved this issue in either their proposed or enacted public access rule or policies. The results revealed that 14 of the 16 states and the federal judiciary do permit release of preconviction information to the public. Specifically, these states include: Alaska, Arizona, California, Colorado, Florida, Indiana, Maryland, Missouri, New Hampshire, New York, North Carolina, Utah, Wisconsin, and Washington.

The Committee did find that Connecticut and Minnesota do not release pre-conviction information. The Committee was informed that in Connecticut the decision not to release this information on the Internet was made in part out of a concern for youthful offenders whose records would eventually become not available to the public based upon the disposition of these cases. The concern was that once information is made available on the Internet, the information may remain available even though the “paper” record has become non-public. Interestingly, the Connecticut legislature has introduced a bill this term that would require its judiciary to release this information.

With regard to Minnesota, the decision to not release this information appears to be related to the fact that there is a high percentage of African American citizens who are arrested for various crimes that result in a very low conviction rate. As such, releasing this information to the public may result in undue harm to these

individuals who will eventually be found not guilty of any crime. Nonetheless, the Committee was informed that Minnesota does release on the Internet court calendar information that does provide information regarding pre-conviction cases. This calendar information is not searchable and must be manually scrolled through to ascertain information about a specific case or individual, but it is available on the Internet.

Additionally, the Committee noted that over 3.2 million web docket sheets of CPCMS cases have been accessed by the public via the Internet, and CPCMS is currently installed in 66 of the 67 counties (Philadelphia implementation is scheduled for later this year)*. The AOPC has been releasing preconviction information from the Magisterial District Judge System (MDJS) for over a decade, apparently without incident.

The Committee also explored the concept of restricting access to preconviction electronic case record information with the AOPC's Judicial Automation Department. Based on the information that is captured by CPCMS, it would be extremely difficult to define exclusive criteria for when a record should not be posted on the web portal page. The difficulty in distinguishing between what constitutes a "preconviction" record versus a "post-conviction" record is dependent upon what court dispositions would fall within each category. For example, if a case has a guilty disposition but sentencing is deferred (such that the guilty plea may be withdrawn prior to sentencing), is that a preconviction record? Are accelerated rehabilitative disposition cases "adjudicated" at the time of entrance to the program or after completion? Given the complexity of the automated rules, it might be the case that the preconviction data would have to be manually selected by the individual counties, leaving room for error.

In light of the above, it is the Committee's recommendation that preconviction information should continue to be available to the public. However, given the serious concerns that were raised in the proposal's public comment period, this issue should continue to be monitored and assessed.

- Other Actions: In response to public commentary received, the Committee made a number of other minor changes to the proposal that was published in September 2005, a summary of which is appended to its report.

The dedication and commitment by the Committee to the principles of open records, interests in individual privacy and security, and public trust and confidence is

* Since the issuance of this report, CPCMS was implemented in Philadelphia County as of September 18, 2006.

reflected in the product of its proposed policy and report. We thank the Committee for its thorough research and analysis.

Without question, however, the Committee's work is not yet complete. The Committee has identified additional areas concerning public access to court record information that require attention (e.g, court staff and public education, sensitive data sheets), not to mention the issues that may arise upon the policy's implementation and subsequent technological advances. We are, therefore, recommending to the Supreme Court that the AOPC continue to dedicate its time and efforts to this important matter for the Unified Judicial System and the citizens of our Commonwealth.

ELECTRONIC CASE RECORD PUBLIC ACCESS POLICY
OF THE UNIFIED JUDICIAL SYSTEM OF PENNSYLVANIA

Section 1.00 DEFINITIONS

- A. "CPCMS" means the Common Pleas Criminal Court Case Management System.
- B. "Custodian" is the person, or designee, responsible for the safekeeping of electronic case records held by any court or office and for processing public requests for access to electronic case records.
- C. "Electronic Case Record" means information or data created, collected, received, produced or maintained by a court or office in connection with a particular case that exists in the PACMS, CPCMS, or MDJS and that appears on web docket sheets or is provided in response to bulk distribution requests, regardless of format. This definition does not include images of documents filed with, received, produced or maintained by a court or office which are stored in PACMS, CPCMS or MDJS and any other automated system maintained by the Administrative Office of Pennsylvania Courts.
- D. "MDJS" means the Magisterial District Judge Automated System.
- E. "Office" is any entity that is using one of the following automated systems: Pennsylvania Appellate Court Case Management System (PACMS); Common Pleas Criminal Court Case Management System (CPCMS); or Magisterial District Judge Automated System (MDJS)."
- F. "PACMS" means the Pennsylvania Appellate Court Case Management System.
- G. "Party" means one by or against whom a civil or criminal action is brought.
- H. "Public" includes any person, business, non-profit entity, organization or association.

"Public" does not include:

- 1. Unified Judicial System officials or employees, including employees of the office of the clerk of courts, prothonotary, and any other office performing similar functions;
- 2. people or entities, private or governmental, who assist the Unified Judicial System or related offices in providing court services; and

3. any federal, state, or local governmental agency or an employee or official of such an agency when acting in his/her official capacity.
- I. "Public Access" means that the public may inspect and obtain electronic case records, except as provided by law or as set forth in this policy.
- J. "Request for Bulk Distribution of Electronic Case Records" means any request, regardless of the format the information is requested to be received in, for all or a subset of electronic case records.
- K. "UJS" means the Unified Judicial System of Pennsylvania.
- L. "Web Docket Sheets" are internet available representations of data that have been entered into a Unified Judicial System supported case management system for the purpose of recording filings, subsequent actions and events on a court case, and miscellaneous docketed items.

Section 2.00 STATEMENT OF GENERAL POLICY

- A. This policy covers all electronic case records.
- B. The public may inspect and obtain electronic case records except as provided by law or as set forth in this policy.
- C. A court or office may not adopt for electronic case records a more restrictive access policy or provide greater access than that provided for in this policy.

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.

Section 3.10 REQUESTS FOR BULK DISTRIBUTION OF ELECTRONIC CASE RECORDS

- A. A request for bulk distribution of electronic case records shall be permitted for data that is not excluded from public access as set forth in this policy.
- B. A request for bulk distribution of electronic case records not publicly accessible under Section 3.00 of this Policy may be fulfilled where: the information released does not identify specific individuals; the release of the information will not present a risk to personal security or privacy; and the information is being requested for a scholarly, journalistic, governmental-related, research or case preparation purpose.
 - 1. Requests of this type will be reviewed on a case-by-case basis.
 - 2. In addition to the request form, the requestor shall submit in writing:
 - (a) the purpose/reason for the request;
 - (b) identification of the information sought;
 - (c) explanation of the steps that the requestor will take to ensure that the information provided will be secure and protected;
 - (d) certification that the information will not be used except for the stated purposes; and
 - (e) whether IRB approval has been received, if applicable.

Section 3.20 REQUESTS FOR ELECTRONIC CASE RECORD INFORMATION FROM ANOTHER COURT OR OFFICE

Any request for electronic case record information from another court should be referred to the proper record custodian in the court or office where the electronic case record information originated. Any request for electronic case record information concerning multiple magisterial district judge courts or judicial districts should be referred to the Administrative Office of the Pennsylvania Courts.

Section 4.00 RESPONDING TO A REQUEST FOR ACCESS TO ELECTRONIC CASE RECORDS

- A. Within 10 business days of receipt of a written request for electronic case record access, the respective court or office shall respond in one of the following manners:
 - 1. fulfill the request, or if there are applicable fees and costs that must be paid by the requestor, notify requestor that the information is available upon payment of the same;
 - 2. notify the requestor in writing that the requestor has not complied with the provisions of this policy;
 - 3. notify the requestor in writing that the information cannot be provided; or
 - 4. notify the requestor in writing that the request has been received and the expected date that the information will be available. If the information will not be available within 30 business days, the court or office shall notify the Administrative Office of Pennsylvania Courts and the requestor simultaneously.
- B. If the court or office cannot respond to the request as set forth in subsection A, the court or office shall concurrently give written notice of the same to the requestor and Administrative Office of Pennsylvania Courts.

Section 5.00 FEES

- A. Reasonable fees may be imposed for providing public access to electronic case records pursuant to this policy.
- B. A fee schedule shall be in writing and publicly posted.
- C. A fee schedule in any judicial district, including any changes thereto, shall not become effective and enforceable until:

1. a copy of the proposed fee schedule is submitted by the president judge to the Administrative Office of Pennsylvania Courts; and
2. the Administrative Office of Pennsylvania Courts has approved the proposed fee schedule.

SECTION 6.00 CORRECTING DATA ERRORS

- A. A party to a case, or the party's attorney, seeking to correct a data error in an electronic case record shall submit a written request for correction to the court in which the record was filed.
- B. A request to correct an alleged error contained in an electronic case record of the Supreme Court, Superior Court or Commonwealth Court shall be submitted to the prothonotary of the proper appellate court.
- C. A request to correct an alleged error contained in an electronic case record of the Court of Common Pleas, Philadelphia Municipal Court or a Magisterial District Court shall be submitted and processed as set forth below.
 1. The request shall be made on a form designed and published by the Administrative Office of Pennsylvania Courts.
 2. The request shall be submitted to the clerk of courts if the alleged error appears in an electronic case record of the Court of Common Pleas or Philadelphia Municipal Court. The requestor shall also provide copies of the form to all parties to the case, the District Court Administrator and the Administrative Office of Pennsylvania Courts.
 3. The request shall be submitted to the Magisterial District Court if the alleged error appears in an electronic case record of the Magisterial District Court. The requestor shall also provide copies of the form to all parties to the case, the District Court Administrator and the Administrative Office of Pennsylvania Courts.
 4. The requestor shall set forth on the request form with specificity the information that is alleged to be in error and shall provide sufficient facts including supporting documentation that corroborates the requestor's contention that the information in question is in error.
 5. Within 10 business days of receipt of a request, the clerk of courts or Magisterial District Court shall respond in writing to the requestor, all parties to the case, and Administrative Office of Pennsylvania Courts, in one of the following manners:

- a. the request does not contain sufficient information and facts to adequately determine what information is alleged to be error; accordingly, the request form is being returned to the requestor; and no further action will be taken on this matter unless the requestor resubmits the request with additional information and facts.
 - b. the request does not concern an electronic case record that is covered by this policy; accordingly, the request form is being returned to the requestor; no further action will be taken on this matter.
 - c. it has been determined that an error does exist in the electronic case record and that the information in question has been corrected.
 - d. it has been determined that an error does not exist in the electronic case record.
 - e. the request has been received and an additional period not exceeding 30 business days is necessary to complete the review of this matter.
6. A requestor has the right to seek review of a final decision under subsection 5(a)-(d) rendered by a clerk of courts or a Magisterial District Court within 10 business days of notification of that decision.
- a. The request for review shall be submitted to the District Court Administrator on a form that is designed and published by the Administrative Office of Pennsylvania Courts.
 - b. If the request for review concerns a Magisterial District Court's decision, it shall be reviewed by the judge assigned by the President Judge.
 - c. If the request for review concerns a clerk of courts' decision, it shall be reviewed by the judge who presided over the case from which the electronic case record alleged to be in error was derived.

SECTION 7.00 CONTINUOUS AVAILABILITY OF POLICY

A copy of this policy shall be continuously available for public access in every court or office that is using the PACMS, CPCMS, and/or MDJS.

Effective January 1, 2013

EXPLANATORY REPORT

ELECTRONIC CASE RECORD PUBLIC ACCESS POLICY OF THE UNIFIED JUDICIAL SYSTEM OF PENNSYLVANIA

INTRODUCTION

With the statewide implementation of the Common Pleas Criminal Court Case Management System (CPCMS) in process, the Administrative Office of the Pennsylvania Courts (AOPC) faced the complicated task of developing a uniform public access policy to criminal case records for Pennsylvania's Unified Judicial System (UJS). Public access to case records is a subject well known to the AOPC. Specifically, the AOPC has been providing information to the public from the judiciary's Magisterial District Judge Automated System (MDJS) pursuant to a public access policy covering MDJS records since 1994.¹ For over a decade now, the AOPC has endeavored to provide accurate and timely MDJS information to requestors without fail.

Like many other state court systems as well as the federal courts, Pennsylvania is confronted with the complex issues associated with public access to case records. Should information found in court files be completely open to public inspection? Or do privacy and/or personal security concerns dictate that some of this information be protected from public view? How is the balance struck between the benefits associated with publicly accessible court data and the threat of harm to privacy and personal security? Should paper case records and electronic case records be treated identically for public access purposes? Does aggregation of data present any special concerns or issues? The above mentioned issues are a mere sampling of the many serious, and often competing, factors that were weighed in the development of this policy.

Through an ad hoc committee ("Committee") appointed by the Court Administrator of Pennsylvania, the AOPC crafted a public access policy covering case records. A summary of the administrative, legal, and public policy considerations that guided the design of the policy provisions follows herewith.

Administrative Scope of the Public Access Policy Governing Case Records

First and foremost, the Committee was charged with determining the scope of this public access policy. After extensive discussions, the Committee reached agreement that at present the public access policy should cover electronic case records as defined in the policy.²

¹ The *Public Access Policy of the Unified Judicial System of Pennsylvania: District Justice Records* was originally adopted in 1994, but was later revised in 1997.

² Electronic Case Records mean information or data created, collected, received, produced or maintained by a court or office in connection with a particular case that exists in the PACMS, CPCMS, or MDJS and that appears on the web docket sheets or is provided in response to bulk distribution requests, regardless of format.

Concerning paper case record information, the Committee first noted that if this policy was applicable to all paper case records then each document that is contained in the court's paper file would have to be carefully scrutinized and possibly redacted pursuant to the policy provisions before it could be released to the public. Depending on individual court resources, such a policy may cause delays in fulfilling public access requests to case records, result in the inadvertent release of non-public information, or impede the business of a filing office or court responsible for the task of review and redaction.³

The Committee is hopeful, however, that the information contained in paper case records concerning a single case will continue to enjoy an acceptable level of protection provided by "practical obscurity," a concept that the U.S. Supreme Court spoke of in United States Department of Justice v. Reporters Committee for Freedom of the Press.⁴ This notion of practical obscurity centers on the effort required to peruse the paper case file for detailed information at the courthouse in person, as opposed to obtaining it instantaneously by a click of the computer mouse.

At the heart of this issue is the question of whether access to paper records and electronic records should be the same. The Committee researched how other state court systems are addressing this issue. It appears that two distinct schools of thought have emerged. One school (represented by the New York⁵ and Vermont⁶ court systems) believes records should be treated the same and the goal is to protect certain information regardless of what form (paper or electronic) that information is in. The other school of thought (represented by the Massachusetts⁷ and Minnesota⁸ court systems) believes there is a difference between maintaining "public" records for viewing/copying at the courthouse and "publishing" records on the Internet.

The Committee further narrowed the scope of the public access policy concerning electronic case records by covering only those records that are created and maintained by one of the UJS' automated case management systems, as opposed to any and all electronic case records created and maintained by courts within the UJS. The Committee is aware that some judicial districts currently have civil automated case management systems in place, but the scope and design of those systems is as different as the number of judicial districts employing

³ The Committee's research revealed that some jurisdictions have proposed or enacted rules/procedures to provide for the redaction of paper records without requiring court staff to redact the information. For example, a number of state court systems are proposing the use of sensitive data sheets to be filed by litigants (e.g., Washington and Arizona). These data sheets contain the personal identifiers (e.g., social security number, etc.) that are normally found throughout a complaint or petition. The data sheets appear to obviate the need for redaction on the part of the filing office or court and protect sensitive data. Another approach taken by the federal court system is the redaction, fully or partially, of sensitive data in the pleadings or complaint by litigants or their attorneys prior to filing (e.g., U.S. District Court for the Eastern District of Pennsylvania Local Rule of Civil Procedure Rule 5.1.3.). It is the opinion of the Committee that the UJS should move in the direction of creating sensitive data sheets (like Washington and Arizona), especially as electronic filing becomes more the norm.

⁴ 489 U.S. 749, 780 (1989).

⁵ *Report to the Chief Judge of the State of New York* by the Commission on Public Access to Court Records (February, 2004).

⁶ VERMONT RULES FOR PUBLIC ACCESS TO COURT RECORDS § 1 - 8 (2004).

⁷ *Policy Statement by the Justices of the Supreme Judicial Court Concerning Publications of Court Case Information on the Web* (May 2003).

⁸ MN ST ACCESS TO REC RULE 1-11 (WEST 2006).

them. Crafting a single policy that would take into account the wide differences among those systems led to the decision to limit the scope to the PACMS, CPCMS and MDJS.

Legal Authority Pertinent to the Public Access Policy Governing Electronic Case Records

Article V, Section 10(c) of the Pennsylvania Constitution vests the Supreme Court with the authority to, *inter alia*, prescribe rules governing practice, procedure and the conduct of all courts. Section 10(c) extends these powers to the administration of all courts and supervision of all officers of the Judicial Branch. Rule of Judicial Administration 505(11) charges the AOPC with the supervision of "all administrative matters relating to the offices of the prothonotaries and clerks of court and other system and related personnel engaged in clerical functions, including the institution of such uniform procedures, indexes and dockets as may be approved by the Supreme Court." Rule of Judicial Administration 501(a) provides in part that "[t]he Court Administrator [of Pennsylvania] shall be responsible for the prompt and proper disposition of the business of all courts. . . ." Rule of Judicial Administration 504(b) sets forth that "the Court Administrator shall. . . exercise the powers necessary for the administration of the system and related personnel and the administration of the Judicial Branch and the unified judicial system." In addition, Rule of Judicial Administration 506(a) provides that "[a]ll system and related personnel shall comply with all standing and special requests or directives made by the [AOPC] for information and statistical data relative to the work of the system and of the offices related to and serving the system and relative to the expenditure of public monies for their maintenance and operation."

Moreover, 42 Pa.C.S. § 4301(b) provides in part that "all system and related personnel engaged in clerical functions shall establish and maintain all dockets, indices and other records and make and file such entries and reports, at such times, in such manner and pursuant to such procedures and standards as may be prescribed by the Administrative Office of Pennsylvania Courts with the approval of the governing authority." 42 Pa.C.S. § 102 provides that system and related personnel of our Unified Judicial System is defined as including but not limited to clerks of courts and prothonotaries. Under the auspices of the aforementioned legal authority, this policy was created.

As part of its preparations to devise provisions governing access to electronic case records, the Committee researched and reviewed the applicable body of law concerning the public's right to access case records and countervailing interests in personal privacy and security.

Common Law Right to Access

A general common law right to inspect and copy public judicial records and documents exists. And while this common law right to access has been broadly construed, the right is not absolute. In determining whether this common law right to access is applicable to a specific document, a court must consider two questions.⁹

⁹ See Commonwealth v. Fenstermaker, 530 A.2d 414, 418-20 (Pa. 1987).

The threshold question is whether the document sought to be disclosed constitutes a public judicial document.¹⁰ Not all documents connected with judicial proceedings are public judicial documents.¹¹ If a court determines that a document is a public judicial document, the document is presumed open to public inspection and copying. This presumption of openness may be overcome by circumstances warranting closure of the document. Therefore, the second question a court must address is whether such circumstances exist and outweigh the presumption of openness.¹²

Circumstances that courts have considered as outweighing the presumption of openness and warranting the closure of documents include: (a) the protection of trade secrets;¹³ (b) the protection of the privacy and reputations of innocent parties;¹⁴ (c) guarding against risks to national security interests;¹⁵ (d) minimizing the danger of unfair trial by adverse publicity;¹⁶ (e) the need of the prosecution to protect the safety of informants;¹⁷ (f) the necessity of preserving the integrity of ongoing criminal investigations;¹⁸ and (g) the availability of reasonable alternative means to protect the interests threatened by disclosure.¹⁹

These types of considerations have been found to outweigh the common law right to access with respect to the following records: transcript of bench conferences held in camera;²⁰ working notes maintained by the prosecutor and defense counsel at trial;²¹ a brief written by the district attorney and presented only to the court and the defense attorney but not filed with the court nor made part of the certified record of appeal;²² and private documents collected during discovery as well as pretrial dispositions and interrogatories.²³

On the other hand, examples of records wherein the common law right to access has prevailed include arrest warrant affidavits,²⁴ written bids submitted to the federal district court for the purpose of selecting lead counsel to represent plaintiffs in securities litigation class action;²⁵ search warrants and supporting affidavits;²⁶ transcripts of jury voir dire;²⁷ pleadings and settlement agreements.²⁸

¹⁰ Id. at 418.

¹¹ In re Cendant, 260 F.3d 183, 192 (3d Cir. 2001) (stating that documents that have been considered public judicial documents have one or more of the following characteristics: (a) filed with the court, (b) somehow incorporated or integrated into the court's adjudicatory proceedings, (c) interpreted or the terms of it were enforced by the court, or (d) required to be submitted to the court under seal).

¹² See Fenstermaker, 530 A.2d at 420.

¹³ In re Buchanan, 823 A.2d 147, 151 (Pa. Super. Ct. 2003), citing Katz v. Katz, 514 A.2d 1374, 1377-78 (Pa. Super. Ct. 1986).

¹⁴ Id.

¹⁵ Id.

¹⁶ Id.

¹⁷ Fenstermaker, 530 A.2d at 420.

¹⁸ Id.

¹⁹ Id.

²⁰ Id. at 418.

²¹ Id.

²² Commonwealth v. Crawford, 789 A.2d 266, 271 (Pa. Super. Ct. 2001).

²³ Stenger v. Lehigh Valley Hosp. Ctr., 554 A.2d 954, 960-61 (Pa. Super. Ct. 1989), citing Seattle Times v. Rhinehart, 467 U.S. 20, 33 (1984).

²⁴ Fenstermaker, 530 A.2d at 420.

²⁵ In re Cendant, 260 F.3d at 193.

²⁶ PG Publ'g Co. v. Copenhefer, 614 A.2d 1106, 1108 (Pa. 1992).

Federal Constitutional Right to Access

The United States Supreme Court has recognized a First Amendment right of access to most, but not all, court proceedings and documents.²⁹ To determine if a First Amendment right attaches to a particular proceeding or document, a two prong inquiry known as the “experience and logic test” must guide the decision to allow access or prohibit it. The “experience” prong involves consideration of whether the place and process have historically been open to the press and general public.³⁰ The “logic” prong involves consideration of “whether public access plays a significant positive role in the functioning of the particular process in question.”³¹

With respect to the “logic” test, courts have looked to the following societal interests advanced by open court proceedings:

- (1) promotion of informed discussion of governmental affairs by providing the public with a more complete understanding of the judicial system;
- (2) promotion of the public perception of fairness which can be achieved only by permitting full public view of the proceedings;
- (3) providing significant therapeutic value to a community as an outlet for concern, hostility, and emotion;
- (4) serving as a check on corrupt practices by exposing the judicial process to public scrutiny;
- (5) enhancement of the performance of all involved; and
- (6) discouragement of perjury.³²

If the court finds that a First Amendment right does attach to a proceeding or document, *there is not an absolute right to access*. Rather, the court may close a proceeding or document if closure is justified by overriding principles. For instance, in criminal cases, closure can occur if it serves a compelling government interest and, absent limited restrictions upon the right to access to the proceeding or document, other interests would be substantially and demonstrably impaired.³³ For example, a court may be able to withhold the release of the transcript of the jury voir dire until after the verdict is announced if in the court’s opinion it was necessary to protect

²⁷ U.S. v. Antar, 38 F.3d 1348, 1358 (3d Cir. 1994).

²⁸ Stenger, 554 A.2d at 960, citing Fenstermaker, 530 A.2d 414; Bank of Am. Nat'l Trust v. Hotel Rittenhouse Associates, 800 F.2d 339 (3d Cir. 1987); In re Alexander Grant and Co. Litigation, 820 F.2d 352 (11th Cir. 1987).

²⁹ In re Newark Morning Ledger Co., 260 F.3d 217, 220-21 (3d Cir. 2001), citing Richmond Newspapers v. Va., 448 U.S. 555, 578 (1980); Nixon v. Warner Communications, Inc., 435 U.S. 589, 597 (1978); Antar, 38 F.3d at 1359-60; Press-Enterprise v. Super. Ct. of Cal., 478 U.S. 1, 11-12 (1986) [hereinafter Press-Enterprise II]; Leucadia, Inc. v. Applied Extrusion Techs., Inc., 998 F.2d 157, 161 (3d Cir. 1993); U.S. v. Criden, 675 F.2d 550, 554 (3d Cir. 1982); U.S. v. Smith, 787 F.2d 111, 114 (3d Cir. 1986); Douglas Oil Co. of Cal. v. Petrol Stops, 441 U.S. 211, 218 (1979). But see U.S. v. McVeigh, 119 F.3d 806 (10th Cir. 1997) (declining to decide whether there is a First Amendment right to judicial document, noting the lack of explicit Supreme Court holdings on the issue since Press Enterprise II, 478 U.S. 1, 11-12 (1986)).

³⁰ In re Newark Morning Ledger, 260 F.3d at 221 n.6., citing Press-Enterprise II, 478 U.S. at 8-9.

³¹ Id., citing Press-Enterprise II, 478 U.S. at 8-9.

³² Id., citing Smith, 787 F.2d at 114 (summarizing Criden, 675 F.2d at 556).

³³ In re Newark Morning Ledger, 260 F.3d at 221, citing U.S. v. Smith, 123 F.3d 140, 147 (3d Cir. 1997) (quoting Antar, 38 F.3d at 1359).

the jury from outside influences during its deliberations.³⁴

Examples of proceedings or documents in which the courts have found a First Amendment right to access include: the voir dire examination of potential jurors,³⁵ preliminary hearings,³⁶ and post trial examination of jurors for potential misconduct.³⁷

Examples of proceedings or documents wherein the courts have not found a First Amendment right to access include: a motion for contempt against a United States Attorney for leaking secret grand jury information,³⁸ sentencing memorandum and briefs filed that contained grand jury information,³⁹ and pretrial discovery materials.⁴⁰

The defendant's Sixth Amendment right to a public trial may also warrant closure of judicial documents and proceedings; however, this right is implicated when the defendant objects to a proceeding being closed to the public. Courts have held that a proceeding can be closed even if the defendant does object, for the presumption of openness may be overcome by an overriding interest based on findings that closure is essential to preserve higher values and is narrowly tailored to serve that interest.⁴¹

Pennsylvania Constitutional Right to Access

The Pennsylvania Supreme Court has established that courts shall be open by virtue of provisions in the Pennsylvania Constitution. Specifically, this constitutional mandate is found in Article I, § 9 which provides in part that "[i]n all criminal prosecutions the accused hath a right to...a speedy public trial by an impartial jury of the vicinage[,]" and Article I, § 11 which provides in part that "[a]ll courts shall be open...."⁴² Specifically, in Fenstermaker, the Court held that

[t]he historical basis for public trials and the interests which are protected by provisions such as Pennsylvania's open trial mandate have been well researched and discussed in two recent opinions of the United States Supreme Court, Gannett Co. v. DePasquale, [citation omitted] and Richmond Newspapers, Inc. v. Virginia, [citation omitted] and can be briefly summarized as follows: generally, to assure the public that justice is done even-handedly and fairly; to discourage perjury and the misconduct of participants; to prevent decisions based on secret bias or partiality; to prevent individuals from feeling that the law should be taken into the hands of private citizens; to satisfy the natural desire to see justice done; to provide for community catharsis; to promote public confidence in government and assurance that the system of judicial remedy does in fact work; to promote the stability of government by allowing access to its workings, thus

³⁴ Antar, 38 F.3d at 1362.

³⁵ Richmond Newspapers, 448 U.S. 555 (1980).

³⁶ Press-Enterprise II, 478 U.S. 1 (1982).

³⁷ U.S. v. DiSalvo, 14 F.3d 833, 840 (3d Cir. 1994).

³⁸ In re Newark Morning Ledger, 260 F.3d 217.

³⁹ Smith, 123 F.3d at 143-44.

⁴⁰ Stenger, 554 A.2d at 960, citing Seattle Times, 467 U.S. at 33.

⁴¹ E.g., Waller v. Georgia, 467 U.S. 39, 45 (1984), citing Press-Enterprise Co. v. Super. Ct. of Cal., 464 U.S. 501, 510 (1984) [hereinafter Press-Enterprise I].

⁴² Fenstermaker, 530 A.2d at 417 (citing PA. CONST. art. I, §§ 9, 11).

assuring citizens that government and the courts are worthy of their continued loyalty and support; to promote an understanding of our system of government and courts.

These considerations, which were applied by the United States Supreme Court in its analysis of the First and Sixth Amendments [of the United States Constitution] in Gannett and Richmond Newspapers apply equally to our analysis of Pennsylvania's constitutional mandate that courts shall be open and that an accused shall have the right to a public trial.⁴³

With regard to the right to a public trial, the Court has held that in determining whether a court's action has violated a defendant's right to a public trial, a court must keep in mind that such a right serves two general purposes: "(1) to prevent an accused from being subject to a star chamber proceeding;⁴⁴ and (2) to assure the public that standards of fairness are being observed."⁴⁵ Moreover, the right to a public trial is not absolute; rather, "it must be considered in relationship to other important interests...[such as] the orderly administration of justice, the protection of youthful spectators and the protection of a witness from embarrassment or emotional disturbance."⁴⁶ If a court determines that the public should be excluded from a proceeding, the exclusion order "must be fashioned to effectuate protection of the important interest without unduly infringing upon the accused's right to a public trial either through its scope or duration."⁴⁷

With regard to the constitutional mandate that courts shall be open, "[p]ublic trials, so deeply ingrained in our jurisprudence, are mandated by Article I, Section 11 of the Constitution of this Commonwealth [and further that] **public trials include public records** [emphasis added]."⁴⁸ Courts in analyzing Section 11 issues have held that there is a presumption of openness which may be rebutted by a claim that the denial of public access serves an important government interest and there is no less restrictive way to serve that government interest. Under this analysis, "it must be established that the material is the kind of information that the courts will protect and that there is good cause for the order to issue."⁴⁹ For example, a violation of Section 11 was found when a court closed an inmate/defendant's preliminary hearing to the public under the pretense of "vague" security concerns.⁵⁰

In at least one case, the Court set forth in a footnote that Article 1, § 7 is a basis for public access to court records.⁵¹ Section 7 provides in part that "[t]he printing press shall be free to every person who may undertake to examine the proceedings of the Legislature or *any branch*

⁴³ Id., citing Commonwealth v. Contankos, 453 A.2d 578, 579-80 (Pa. 1982).

⁴⁴ During the reign of Henry VIII and his successors, the jurisdiction of the star chamber court was illegally extended to such a degree (by punishing disobedience to the king's arbitrary proclamations) that it was eventually abolished. Black's Law Dictionary (1990).

⁴⁵ Commonwealth v. Harris, 703 A.2d 441, 445 (Pa. 1997), citing Commonwealth v. Berrigan, 501 A.2d 226 (Pa. 1985).

⁴⁶ Commonwealth v. Conde, 822 A.2d 45, 49 (Pa. Super. Ct. 2003), citing Commonwealth v. Knight, 364 A.2d 902, 906-07 (Pa. 1976).

⁴⁷ Id., citing Knight, 364 A.2d at 906-07.

⁴⁸ Commonwealth v. French, 611 A.2d 175, 180 n.12 (Pa. 1992).

⁴⁹ R.W. v. Hampe, 626 A.2d 1218, 1220 (Pa. Super. Ct. 1993), citing Hutchinson v. Luddy, 581 A.2d 578, 582 (Pa. Super. Ct. 1990) (citing Publicker Industries, Inc. v. Cohen, 733 F.2d 1059, 1070 (3d Cir. 1983)).

⁵⁰ Commonwealth v. Murray, 502 A.2d 624, 629 (Pa. Super. Ct. 1985) *appeal denied*, 523 A.2d 1131 (Pa. 1987).

⁵¹ French, 611 A.2d at 180 n.12.

of government and no law shall ever be made to restrain the right thereof.”

Legislation Addressing Public Access to Government Records

The Freedom of Information Act (FOIA), codified in Title 5 § 552 of the United States Code, was enacted in 1966 and generally provides that any person has the right to request access to federal agency records or information. All agencies of the executive branch of the United States government are required to disclose records upon receiving a written request for them, except for those records (or portions of them) that are protected from disclosure by the nine exemptions and three exclusions of the FOIA. This right of access is enforceable in court. The FOIA does not, however, provide access to records held by state or local government agencies, or by private businesses or individuals.⁵²

The Privacy Act of 1974⁵³ is a companion to the FOIA. The Privacy Act regulates federal government agency record-keeping and disclosure practices and allows most individuals to seek access to federal agency records about themselves. The Act requires that personal information in agency files be accurate, complete, relevant, and timely. The subject of a record may challenge the accuracy of information. The Act requires that agencies obtain information directly from the subject of the record and that information gathered for one purpose is not to be used for another purpose. Similar to the FOIA, the Act provides civil remedies for individuals whose rights may have been violated. Moreover, the Act restricts the collection, use and disclosure of personally identifiable information (e.g., social security numbers) by federal agencies.⁵⁴

Pennsylvania’s Right to Know Act⁵⁵ (RTKA) gives Pennsylvanians the right to inspect and copy certain executive branch records. The RTKA was originally enacted in 1957 but was substantially amended by Act 100 of 2002. Records that are available under the RTKA include “any account, voucher or contract dealing with the receipt or disbursement of funds by an agency or its acquisition, use or disposal of services or of supplies, materials, equipment or other property and any minute, order or decision by an agency fixing the personal or property rights, privileges, immunities, duties or obligations of any person or group of persons.”⁵⁶ However, records that are not available under the RTKA include:

any report, communication or other paper, the publication of which would disclose the institution, progress or result of an investigation undertaken by an agency in the performance of its official duties, except those reports filed by agencies pertaining to safety and health in industrial plants; any record, document, material, exhibit, pleading, report, memorandum or other paper, access to or the publication of which is prohibited, restricted or forbidden by statute law or order or decree of court, or *which would operate to the prejudice or*

⁵² *United States Department of Justice Freedom of Information Act Reference Guide* (May 2006), available at <http://www.usdoj.gov/04foia/referenceguidemay99.htm>.

⁵³ 5 U.S.C. § 552a (2006).

⁵⁴ United States House of Representatives *A Citizen’s Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records* (First Report 2003).

⁵⁵ PA. STAT. ANN. tit. 65, §§ 66.1-66.9 (West 2006).

⁵⁶ PA. STAT. ANN. tit. 65, § 66.1 (West 2006).

*impairment of a person's reputation or personal security, or which would result in the loss by the Commonwealth or any of its political subdivisions or commissions or State or municipal authorities of Federal funds, except the record of any conviction for any criminal act [emphasis added].*⁵⁷

While these federal and state laws are not applicable to court records, the Committee consulted these statutory provisions in drafting the policy.

Other Court Systems' Approaches Concerning Public Access to Electronic Case Records

The Committee looked to the policies, whether adopted or proposed by rule or statute or otherwise, of other court systems (federal and state) for guidance and in doing so found a wide variety of practices and approaches to public access. Not surprisingly, the process of putting court records online has produced remarkably disparate results. Courts have made records available in many forms ranging from statewide access systems to individual jurisdictions providing access to their records. Some court systems provide access to both criminal and civil records, while others make distinctions between the treatment of those types of records or restrict users' access to records that may contain sensitive personal information. As noted previously, some states distinguish between electronic and paper records, while others do not.

In particular, the Committee reviewed the policies (whether proposed or fully adopted) of: the Judicial Conference Committee on Court Administration and Case Management (including the Report of the Federal Judicial Center entitled *Remote Public Access to Electronic Criminal Case Records: A Report on a Pilot Project in Eleven Federal Courts*), the U.S. District Court for the Eastern District of Pennsylvania and the Southern District of California, Alaska, Arizona, California, Colorado, Florida, Georgia, Indiana, Idaho, Kansas, Kentucky, Maryland, Massachusetts, Minnesota, Missouri, New York, North Carolina, Washington, Utah, and Vermont.

Additionally, the Committee closely reviewed the materials disseminated by the National Center for State Courts (NCSC) project titled "Developing a Model Written Policy Governing Access to Court Records." Perhaps as an indication of the difficulties inherent in drafting policy provisions to govern public access to court records in a single jurisdiction (let alone nationwide), the NCSC project shifted its focus from developing a model policy to guidelines for local policymaking.⁵⁸ The final report of this NCSC project was entitled "Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts" (CCJ/COSCA Guidelines). As noted in the title, the CCJ/COSCA Guidelines were adopted by the Conference of Chief Justices and the Conference of State Court Administrators.

As it wrestled with and attempted to appropriately balance the thorny issues and significant challenges associated with the development and implementation of a statewide

⁵⁷ Id.

⁵⁸ The Committee notes that, in its opinion, there was a shift in the treatment of paper and electronic records and the balance between open records versus privacy protections between the various draft versions of the CCJ/COSCA Guidelines submitted for review and comment.

access policy, the Committee was grateful for the insight and thought-provoking discussions these policies engendered.

Policy Perspectives Weighed in Devising the Public Access Policy Governing Electronic Case Records

Increasingly in today's society, the courts are witness to the tension between the importance of fully accessible electronic case records and the protection of an individual's privacy and personal security. The two important, but at times seemingly incompatible, interests are perhaps better categorized as the interest in *transparency* (i.e., opening judicial branch processes to public scrutiny) and the competing interests of *personal privacy and personal security*.

Case records capture a great deal of sensitive, personal information about litigants and third parties (e.g., witness, jurors) who come in contact with the courts. The tension between transparency and personal privacy/security of case records has been heightened by the rapidly increasing use of the Internet as a source of data, enhanced automated court case management systems, and other technological realities of the Information Age.

Prior to the widespread use of computers and search engines, case record information was accessible by traveling to the local courthouse and perusing the paper files, presumably one at a time. Thus, most information contained in the court records enjoyed "practical obscurity." In the latter part of the twentieth century, the proliferation of computerized case records was realized. As a result, entire record systems are swept by private organizations within seconds and data from millions of records are compiled into enormous record databases, accessible by government agencies and the public.⁵⁹

Cognizant of today's technological realities, the Committee explored the inherent tension between the transparency of case records and the interest in personal privacy and security to more clearly understand the values associated with each.

The Values of Transparency

The values of transparency can be described as serving four essential functions: 1) shedding light on judicial activities and proceedings; 2) uncovering information about public officials and candidates for public office; 3) facilitating certain social transactions; and 4) revealing information about individuals for a variety of purposes.⁶⁰

With regard to access to electronic case records, the Committee focused primarily on the first function of transparency, which aids the public in understanding how the judicial system works and promotes public confidence in its operations. Open electronic case records "allows the citizenry to monitor the functioning of our courts, thereby insuring quality, honesty, and

⁵⁹ Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 Minn. L. Rev. 1137 (2002) (noting that more than 165 companies compile "digital biographies" on individuals that by a click of a mouse can be scoured for data on individual persons).

⁶⁰ *Id.* at 1173.

respect for our legal system."⁶¹ Transparent electronic case records allow the public to assess the competency of the courts in resolving cases and controversies that affect society at large, such as product liability, medical malpractice or domestic violence litigation.⁶² Information that alerts the public to danger or might help prove responsibility for injuries should be available, as should that which enables the public to evaluate the performance of courts and government officials, the electoral process and powerful private organizations.⁶³

The key to assessing the complete release of electronic case record data appears to hinge upon whether there is a legitimate public interest at stake or whether release is sought for "mere curiosity."⁶⁴ While this measure has been applied to analysis of the propriety of sealing individual court records, it should apply by extension to the broader subject of public access to electronic case record information. Analysis of whether release of electronic case record information satisfies a legitimate public interest should center on whether the effect would be to serve one of the four essential functions of transparency. Any other basis for release might serve to undermine the public's trust and confidence in the judiciary.

The values inherent in the transparency of electronic case records are the root of the "presumption of openness" jurisprudence. The Committee gave that presumption due consideration throughout its undertaking.

Privacy and Personal Security Concerns Regarding the Release of Electronic Case Records

The Committee debated at length as to where the line is drawn between transparency and privacy/personal security. Unfortunately, no legal authority exists that provides a "bright line" rule. Moreover, given that our society continues to witness and adopt new technology at a fast pace, the Committee worked to identify the privacy and personal security concerns that the release of electronic case record information triggers.

According to a national survey conducted a decade ago, nearly 80% of those polled were concerned or very concerned about the threat to their privacy due to the increasing use of computerized records.⁶⁵ Concerns about advances in information technology have resulted in greater public support for legislative protection of confidential information.⁶⁶ The Committee noted that the last two legislative sessions of the Pennsylvania General Assembly have resulted in the introduction of more than forty bills that seek to restrict access to private and/or personal information.

Case records contain considerable amounts of sensitive personal information, such as

⁶¹ *Id.* at 1174 (citing *In re Cont'l Ill. Sec. Litig.*, 732 F.2d 1302, 1308 (7th Cir. 1984)).

⁶² *Id.* at 1174-75.

⁶³ Stephen Gillers, *Why Judges Should Make Court Documents Public*, N.Y. Times, November 30, 2002, p 17.

⁶⁴ George F. Carpinello, *Public Access to Court Records in New York: The Experience Under Uniform Rule 216.1 and the Rule's Future in a World of Electronic Filing*, 66 ALB. L. REV. 1089, 1094 (2003) (citing *Dawson v. White & Case*, 584 N.Y.S.2d 814, 815 (N.Y. App. Div. 1992), wherein financial information concerning defendant's partners and clients was sealed as disclosure would not benefit a relevant and legitimate public interest).

⁶⁵ Barbara A. Petersen and Charlie Roberts, *Access to Electronic Public Records*, 22 FLA. ST. U.L. REV. 443, n. 247 (1994).

⁶⁶ *Id.* at 486.

social security numbers, financial information, home addresses, and the like. This information is collected not only with respect to the litigants but others involved in cases, such as witnesses and jurors. The threat to privacy is realized in the assembling of individual "dossiers" which can track the private details of one's life, including spending habits, credit history, and purchases.⁶⁷

Personal security issues arise from the ease with which sensitive data can usually be obtained. The threat of harm can either be physical or financial. By accessing home address information, individuals may be the subject of stalking or harassment that threatens their physical person.⁶⁸ Financial harm is documented by the fastest growing consumer fraud crime in the United States -- identity theft. "According to CBS News, approximately every 79 seconds an identity thief steals someone's identity, opens an account in the victim's name and goes on a buying spree."⁶⁹ The United States Federal Trade Commission reports that 10.1 million consumers have been victims of identity theft in 2003.⁷⁰ In addition, a recent study by the financial industry reveals that 9.3 million people were victims of the crime of identity theft in 2004.⁷¹ The U.S. Department of Justice estimates that identity bandits may victimize up to 700,000 Americans per year.⁷² In Eastern Pennsylvania, a regional identity theft task force was established to aid federal, state and local authorities to curb the growing incidence of identity theft.⁷³

Recent newspaper accounts have recorded that the personal information of hundreds of thousands of individuals has been accessed by unauthorized individuals -- raising the realistic concern of the possibility of widespread identity theft. Commercial entities -- specifically Choicepoint and LexisNexis -- have collectively released the personal information of 445,000 people to unauthorized individuals.⁷⁴ The University of California-Berkeley reported the theft of a laptop computer that contained the dates of birth, addresses, and social security numbers of 98,369 individuals who applied to or attended the school.⁷⁵ Boston College alerted 120,000 alumni that computers containing their addresses and social security numbers were hacked by an unknown intruder.⁷⁶ A medical group in San Jose California reported the theft of computers that contained the information of 185,000 current and past patients.⁷⁷

Conclusion

After a thorough evaluation of the legal authority and public policy issues attendant to public access of electronic case record information, the Committee devised a balancing test for

⁶⁷ Solove, *supra* note 59, at 1140.

⁶⁸ Robert C. Lind and Natalie B. Eckart, *The Constitutionality of Driver's Privacy Protection Act*, 17 *Communication Lawyer* 18 (1999). *See also*, Solove, *supra* note 59, at 1173.

⁶⁹ David Narkiewicz, *Identity Theft: A Rapidly Growing Technology Problem*, *The Pennsylvania Lawyer*, May – June 2004, at 58.

⁷⁰ Bob Sullivan, *Study: 9.3 Million ID Theft Victims Last Year*, MSNBC.com, January 26, 2005.

⁷¹ *Id.*

⁷² *ID Theft Is No. 1 Fraud Complaint*, CBSNEWS.com, January 22, 2003.

⁷³ Jim Smith, *Regional Task Force to Tackle ID-Theft Crimes*, phillynews.com, November 13, 2002.

⁷⁴ John Waggoner, *Id theft scam spreads across USA*, USATODAY.com, February 22, 2005; *LexisNexis Id theft much worse than thought*, MSNBC.com, April 12, 2005.

⁷⁵ *Thief steals UC-Berkeley laptop*, CNN.com, March 31, 2005.

⁷⁶ Hiawatha Bray, *BC warns its alumni of possible Id theft after computer is hacked*, Boston Globe, March 17, 2005.

⁷⁷ Jonathon Krim, *States Scramble to Protect Data*, Washington Post, April 9, 2005.

evaluating the release of electronic case record information. And while a perfect balance cannot be struck between transparency and personal privacy/security, the Committee attempted to reach a reasonable accommodation protective of both interests.

In determining whether electronic case record information should be accessible by the public, the Committee evaluated first whether there was a legitimate public interest in release of the information. If such an interest was not found, the inquiry ended and the information was prohibited from release.

If such an interest was found, the Committee next assessed whether the release of this information would cause an unjustified invasion of personal privacy or presented a risk to personal security. If the answer to this inquiry was no, the information was released. If the answer was yes, the Committee weighed the unjustified invasion of personal privacy or risk to personal security against the public benefit in releasing the information.

Section 1.00 DEFINITIONS

- A. “CPCMS” means the Common Pleas Criminal Court Case Management System.
- B. “Custodian” is the person, or designee, responsible for the safekeeping of electronic case records held by any court or office and for processing public requests for access to case records.
- C. “Electronic Case Record” means information or data created, collected, received, produced or maintained by a court or office in connection with a particular case that exists in the PACMS, CPCMS, or MDJS and that appears on web docket sheets or is provided in response to bulk distribution requests, regardless of format. This definition does not include images of documents filed with, received, produced or maintained by a court or office which are stored in PACMS, CPCMS or MDJS and any other automated system maintained by the Administrative Office of Pennsylvania Courts.
- D. “MDJS” means the Magisterial District Judge Automated System.
- E. “Office” is any entity that is using one of the following automated systems: Pennsylvania Appellate Court Case Management System (PACMS); Common Pleas Criminal Court Case Management System (CPCMS); or Magisterial District Judge Automated System (MDJS).”
- F. “PACMS” means the Pennsylvania Appellate Court Case Management System.
- G. “Party” means one by or against whom a civil or criminal action is brought.
- H. “Public” includes any person, business, non-profit entity, organization or association.

“Public” does not include:

1. Unified Judicial System officials or employees, including employees of the office of the clerk of courts, prothonotary, and any other office performing similar functions;
2. people or entities, private or governmental, who assist the Unified Judicial System or related offices in providing court services; and
3. any federal, state, or local governmental agency or an employee or official of such an agency when acting in his/her official capacity.

- I. “Public Access” means that the public may inspect and obtain electronic case records, except as provided by law or as set forth in this policy.
- J. “Request for Bulk Distribution of Electronic Case Records” means any request, regardless of the format the information is requested to be received in, for all or a subset of electronic case records.
- K. “UJS” means the Unified Judicial System of Pennsylvania.
- L. “Web Docket Sheets” are internet available representations of data that have been entered into a Unified Judicial System supported case management system for the purpose of recording filings, subsequent actions and events on a court case, and miscellaneous docketed items.

2013 COMMENTARY

The definition of “electronic case records” was amended to exclude images of documents filed with, received, produced or maintained by a court or office which are stored in PACMS, CPCMS or MDJS and any other automated system maintained by the Administrative Office of Pennsylvania Courts.

While the Judiciary is presently piloting, on a limited basis, e-filing in the statewide case management systems, design and development efforts have not advanced to allow for online publication or bulk dissemination of images of e-filed documents.

2007 COMMENTARY

In adopting the definitions to the above terms, the Committee considered Pennsylvania law, other states’ laws and public access policies, and the CCJ/COSCA Guidelines. In most cases, the definitions that the Committee chose to adopt are found in one of the above-mentioned sources. The following list sets forth the source for each of the above definitions.

Subsection B, Custodian, is derived from Arizona’s definition of custodian which is the “person responsible for the safekeeping of any records held by any court, administrative office, clerk of court’s office or that person’s designee who also shall be responsible for processing public requests for access to records.”⁷⁸ To ensure that this definition would encompass any court or office that is the primary custodian of electronic case records the Committee chose to replace the phrase “any court, administrative office, clerk of court’s office” with “any court or office.”

Subsection C, Electronic Case Record, the Committee opines it is necessary to set forth a term for those records that exist within one of the UJS’ automated case management systems

⁷⁸ ARIZ. SUP. CT. R. 123(b)(6).

(PACMS, CPCMS, or MDJS). This definition is derived from Minnesota’s definition of “case record.”⁷⁹ Nonetheless, this definition includes responses to requests for bulk distribution of electronic case records as well as web docket sheets as defined in this policy. However, paper documents concerning a single case produced from the PACMS, CPCMS, or MDJS are not included in this definition except as otherwise provided for in this definition.

Subsection E, Office, is a Committee-created term. The Committee wanted to ensure that the Policy applies only to the office that is the primary custodian of an electronic case record, regardless of the title of the office. The Committee also wanted to avoid creating an obligation on the part of an office that possessed only a copy of a record to provide access to a requestor.

Subsection G, Party, is a Committee-created term. The Committee wanted to clarify who a party to an action is. This definition is a combination of the definition for party set forth in 42 Pa.C.S. § 102⁸⁰ and Seventh Edition of Black’s Law Dictionary.⁸¹

Subsection H, Public, is a variation of a provision in the CCJ/COSCA Guidelines.⁸² The most significant difference is that the CCJ/COSCA Guidelines provide for two additional classes of individuals and/or entities that are included in the definition of “public.” The first class is “any governmental agency for which there is no existing policy defining the agency’s access to court records.”⁸³ In the Committee’s judgment, all government requestors should be treated differently than non-government requestors. Thus, the Committee chose not to adopt this statement, as further explained below.

The second class is “entities that gather and disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to nature or extent of access.”⁸⁴ The Committee opines that any person or entity that falls within this category would also fall within our definition of the public. Therefore, this statement was thought to be redundant.

In the judgment of the Committee every member of the public should be treated equally when requesting access to electronic case records. The Policy creates three categories of individuals and entities that do not fall within the definition of the “public;” thus, the Policy’s provisions are not applicable to them. Specifically, these three categories are (1) court employees, (2) those who assist the courts in providing court services (e.g., contractors), and (3) governmental agencies.

⁷⁹ *Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (June 28, 2004), p. 2.

⁸⁰ “A person who commences or against whom relief is sought in a matter. The term includes counsel for such a person who is represented by counsel.” See 42 Pa.C.S. § 102.

⁸¹ “One by or against whom a lawsuit is brought.” Black’s Law Dictionary Seventh Edition 1144 (Bryan A. Garner, et al. eds. 1999).

⁸² Steketee, Martha Wade and Carlson, Alan, *Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts*, October 18, 2002, available at www.courtaccess.org/modelpolicy [hereinafter *CCJ/COSCA Guidelines*], p. 10.

⁸³ *Id.*

⁸⁴ *Id.*

With regard to court employees and those who assist the courts in providing court services (e.g., contractors), the Committee asserts that they should also have as much access to electronic case records as needed to perform their assigned duties and tasks.

With regard to requests from governmental agencies, the Committee noted that AOPC's practice when responding to government requests for MDJS information has been to place few restrictions on fulfilling said requests. AOPC has provided to governmental agencies the following information: social security numbers, driver license numbers, dates of birth, and many other pieces of sensitive information that MDJS Policy prohibits access to by public (non-government) requestors. The Committee considers this to be consistent with the approach taken by other branches of Pennsylvania's government. Specifically, the RTKA provides that a requestor is defined as "a person who is a resident of the Commonwealth and requests a record pursuant to this act."⁸⁵ Thus, it appears that the intent of the RTKA is for it to be only applicable to public (non-governmental) requestors.

Although the Committee is aware that the RTKA does exclude non-residents of Pennsylvania,⁸⁶ it sees no reason to limit the definition of public to exclude non-residents of the Commonwealth (for example, an executor in New York asking for court records concerning a Pennsylvania resident in order to settle an estate).

The Committee also noted that the CCJ/COSCA Guidelines provide that the policy "applies to governmental agencies and their staff where there is no existing law specifying access to court records for that agency, for example a health department....If there are applicable access rules, those rules apply."⁸⁷ Thus, the CCJ/COSCA Guidelines provide that unless there is specific legal authority governing the release of court records to a particular governmental agency, the governmental agency should be considered a member of the public for the purposes of access to information.

The Committee maintains that limitations upon the information provided to public requestors is a result of a balance struck between providing access to public information, and protecting the privacy and safety of the individuals whose information the courts and related offices possess. With regard to governmental entities, no such balance needs to be struck in that providing access to restricted information to another governmental agency does not presumably endanger individuals' safety or privacy. To ensure that the requests are for legitimate governmental reasons, all government requestors should be required to complete a government request form, a separate form from that used by public requestors. This government request form should require the requestor to state the reason for the request, in contrast to the public request form, which should not. The justification for requiring more information about governmental requests lies with the much greater access afforded to governmental entities. However, information pertaining to these requests and the court's response to the same should not be accessible to the public.

⁸⁵ PA. STAT. ANN. tit. 65, § 66.1 (West 2006).

⁸⁶ Id.

⁸⁷ *CCJ/COSCA Guidelines*, p. 11.

Nonetheless, while in the Committee's judgment government requestors should be provided with greater access to information, there are some pieces of information that absolutely should not be released -- for example, information sealed or protected pursuant to court order. Therefore, the Committee recommends that government requestors continue to be provided with greater access to information than public requestors, but such access should not be completely unrestricted.

Lastly, the Committee decided with regard to foreign government requestors that if a foreign government is permitted access pursuant to law, then access will be provided.

When the Committee was considering whether to include or exclude litigants and their attorneys in the definition of the "public," the Committee noted that the current MDJS practice is to treat litigants and their attorneys the same as non-litigants or non-attorneys. However, it is noted that the CCJ/COSCA Guidelines provides that the parties to a case and their attorneys do not fall within the definition of the term "public."⁸⁸ Therefore, in the CCJ/COSCA Guidelines, they will have nearly unrestricted access to the electronic case records, whereas the public's access will be restricted.

Subsection I, Public Access, is a Committee created term because the Committee was unable to find an existing definition that was deemed adequate.

Subsection J, Request for Bulk Distribution of Electronic Case Records, is derived from the CCJ/COSCA Guidelines.⁸⁹ This definition includes all requests regardless of the format the requestors want to receive the information in (i.e., paper, electronic, etc.). It appears that this is a term of art that is commonly used nationwide.⁹⁰

Subsection M, Web Docket Sheets, is a term created by the Administrative Office of Pennsylvania Courts. Currently, web docket sheets for the appellate and criminal divisions of the courts of common pleas are located at <http://ujportal.pacourts.us/>.

⁸⁸ *CCJ/COSCA Guidelines*, p. 10.

⁸⁹ *CCJ/COSCA Guidelines*, p. 29.

⁹⁰ For example this term is used by Indiana (Ind. Admin. R.9(C)(9)), Minnesota (*Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (June 28, 2004), p. 15; MN ST ACCESS TO REC RULE 8(3) (WEST 2006).), and California (Cal. CT. R. 2073(f)).

Section 2.00 STATEMENT OF GENERAL POLICY

- A. This policy covers all electronic case records.
- B. The public may inspect and obtain electronic case record except as provided by law or as set forth in this policy.
- C. A court or office may not adopt for electronic case records a more restrictive access policy or provide greater access than that provided for in this policy.

COMMENTARY

For the reasons stated in the Introduction, paragraph A sets forth that this policy covers electronic case records as defined in Section 1.00.

The language of subsection C is suggested in the CCJ/COSCA Guidelines, which provide “[i]f a state adopts a policy, in the interest of statewide uniformity the state should consider adding a subsection...to prevent local courts from adopting different policies...This not only promotes consistency and predictability across courts, it also furthers equal access to courts and court records.”⁹¹ The Committee opines it is essential for the Unified Judicial System to have this provision in the policy to prevent various courts and offices from enacting individual policies governing electronic case records.

The Committee also notes that subsection C applies to fees in that the level of fees may be a means of restricting access. Therefore, a court or office charged with fulfilling public access requests must comply with the fee schedule provisions contained in Section 5.00 of this policy.

⁹¹ *CCJ/COSCA Guidelines*, pp. 24-25.

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 PA.R.CRIM.P. 630(A)(2), (3).

¹⁴⁴ PA.R.CRIM.P. 632(B).

¹⁴⁵ PA.R.CRIM.P. 632(C).

¹⁴⁶ PA.R.CRIM.P. 632(F).

¹⁴⁷ PA.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. Commw. 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, fn. 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.

Section 3.10 REQUESTS FOR BULK DISTRIBUTION OF ELECTRONIC CASE RECORDS

- A. A request for bulk distribution of electronic case records shall be permitted for data that is not excluded from public access as set forth in this policy.

- B. A request for bulk distribution of electronic case records not publicly accessible under Section 3.00 of this Policy may be fulfilled where: the information released does not identify specific individuals; the release of the information will not present a risk to personal security or privacy; and the information is being requested for a scholarly, journalistic, governmental-related, research or case preparation purpose.
 - 1. Requests of this type will be reviewed on a case-by-case basis.

 - 2. In addition to the request form, the requestor shall submit in writing:
 - (a) the purpose/reason for the request;
 - (b) identification of the information sought;
 - (c) explanation of the steps that the requestor will take to ensure that the information provided will be secure and protected;
 - (d) certification that the information will not be used except for the stated purposes; and
 - (e) whether IRB approval has been received, if applicable.

2013 COMMENTARY

An Institutional Review Board (“IRB”) ascertains the acceptability of and monitors research involving human subjects. An IRB will typically set forth requirements for research projects, such as where the information is to be kept, who has access, how the information is codified, and what information is needed for matching purposes. If there is IRB approval documentation setting forth the information required under Subsection B(2), such documentation may be sufficient to satisfy the “writing” requirement of this subsection.

2007 COMMENTARY

In the judgment of the Committee, the number of electronic case records that may be requested by the public should not be limited. AOPC’s practice has been to fulfill requests for bulk distribution of electronic MDJS case records regardless of the number of records involved. In addition, the Committee’s recommendation and analysis on this issue closely mirrors the CCJ/COSCA Guidelines, which permit the release of bulk distribution of court records.²⁰⁴ In

²⁰⁴ See CCJ/COSCA Guidelines, pp. 34, 35, and 39.

addition, the Committee notes that several states, including California,²⁰⁵ Indiana,²⁰⁶ and Minnesota²⁰⁷ permit the release of bulk data. Some states such as Kansas²⁰⁸ and Colorado²⁰⁹ (in part) do not permit the release of bulk data. Moreover, the RTKA provides that “[a] policy or regulation may not include any of the following: a limitation on the number of public records which may be requested or made available for inspection or duplication.”²¹⁰ Therefore, the Committee recommends that requests for bulk distribution of electronic case records continue to be fulfilled.

With regard to these requests, the Committee believes that the Judicial Automation Department may in the future implement in the Court's automated systems (PACMS, CPCMS, and MDJS) various "canned" reports which a user can produce for requestors in response to a request. However, until the development of these "canned" reports or in a situation where the request cannot be fulfilled with one of these "canned" reports, the requestor should be referred to the AOPC.

A request for bulk distribution of electronic case records is defined as a request for all, or a subset, of electronic case records. Bulk distribution of electronic case record information shall be permitted for data that are publicly accessible as specified in the policy (e.g., date of birth, a party's address limited to city, state and ZIP code).

In addition, a request for bulk distribution of information/data not publicly accessible may be permitted where: the information released does not identify specific individuals; the release of the information will not present a risk to personal security or privacy; and the information is being requested for a scholarly, journalistic, governmental-related, research or case preparation purpose.

The court, office or record custodian will review requests for this type of information/data on a case-by-case basis. For example, a requestor may want to know the offense location of all rapes for a given year in Pennsylvania, but he does not want any personal information about the victims (such as name, social security number, etc) because he is conducting a study to see if most rapes occur in apartment buildings, single-family structures, or in public areas (such as malls or parking lots). This request could be fulfilled if the information released does not identify any of the victims; there is no risk to the personal security or privacy of the victims involved; and the information is being requested for a scholarly, journalistic, governmental-related, research or

²⁰⁵ See CAL. CT. R. 2073(f) which provides that “a court may provide bulk distribution of only its electronic calendar, register of actions and index. ‘Bulk distribution’ means distribution of all, or a significant subset, of the court’s electronic records.”

²⁰⁶ IND. ADMIN. R. 9(F) permits the release of bulk or compiled data.

²⁰⁷ MN ST ACCESS TO REC RULE 8(3) (WEST 2006).

²⁰⁸ Kansas Rules Relating to District Courts Rule 196(e) “Bulk and Compiled Information Distribution – Information in bulk or compiled format will not be available.”

²⁰⁹ Colo. CJD. 05-01 provides in Section 4.30 that bulk data will not be released to individuals, government agencies or private entities. Bulk data being the entire database or that subset of the entire database that remains after the extraction of all data that is confidential under law. However, Section 4.40 provides that requests for compiled data for non-confidential data will be entertained. There are numerous criteria that will be used to determine if the request will be granted. Compiled data is defined as data that is derived from the selection, aggregation or reformulation of specific data elements within the database.”

²¹⁰ PA. STAT. ANN. tit. 65, § 66.8(c)(1) (West 2006).

case preparation purpose.

For requests of non-releasable information, the requestor shall in addition to the request form, submit in writing:

- the purpose/reason for the request;
- identification of the information sought;
- explanation of the steps that the requestor will take to ensure that the information provided will be secure and protected; and
- certification that the information will not be used except for the stated purposes.

This section addresses requests for large volumes of data available from the statewide automation case management systems (PACMS, CPCMS, and MDJS) including incremental data files used to update previously received bulk distributions.²¹¹

²¹¹ After receipt of the initial bulk data transfer, requestors receive additional data sets (increments) periodically that allow them to update their current file.

Section 3.20 REQUESTS FOR ELECTRONIC CASE RECORD INFORMATION FROM ANOTHER COURT OR OFFICE

Any request for electronic case record information from another court should be referred to the proper record custodian in the court or office where the electronic case record information originated. Any request for electronic case record information concerning multiple magisterial district judge courts or judicial districts should be referred to the Administrative Office of the Pennsylvania Courts.

COMMENTARY

The Committee asserts that for electronic case record information “filed” within a specific court or office the requestor should contact the court or office for information. However, requests for information about multiple magisterial district judge courts or judicial districts should be directed to and processed by the AOPC.

In light of the fact that the CPCMS provides the capability for a clerk of courts in one county to produce information about a case in another county, the Committee is concerned that this policy might be used by a requestor to attempt to compel court and office personnel to produce information about a case in another county. The Committee assumes that most personnel would be averse to producing information about a case from another county in that the courts and offices currently have “control” over the release of their own case records. Therefore, it is preferable that situations in which court or office X is releasing court or office Y’s case records be avoided. Therefore this section makes it clear that requests for electronic case record information should be made to the record custodian in the court or office where the electronic case record information originated.

Generally, requests for information regarding a specific court or office should continue to be handled at the local level, but should be consistent with the statewide public access policy, thus ensuring that a requestor will get the same kinds of information from any court or office statewide. If a requestor is unable to obtain the information, the AOPC should work with the record custodian or appropriate administrative authority (e.g., district court administrator) to facilitate the fulfillment of the request consistent with the policy, as currently is done for MDJS requests. As a last resort, the AOPC may handle these requests directly, if possible.

For requests regarding multiple magisterial district judge courts or judicial districts, the Committee recommends that such requests should be referred to the AOPC, which alone should respond to the same. The Committee opines that the AOPC will be in the best position to more efficiently handle these requests, considering the AOPC will be capable of identifying the precise technological queries needed to “run” the request.

Section 4.00 RESPONDING TO A REQUEST FOR ACCESS TO ELECTRONIC CASE RECORDS

- A. Within 10 business days of receipt of a written request for electronic case record access, the respective court or office shall respond in one of the following manners:
1. fulfill the request, or if there are applicable fees and costs that must be paid by the requestor, notify requestor that the information is available upon payment of the same;
 2. notify the requestor in writing that the requestor has not complied with the provisions of this policy;
 3. notify the requestor in writing that the information cannot be provided; or
 4. notify the requestor in writing that the request has been received and the expected date that the information will be available. If the information will not be available within 30 business days, the court or office shall notify the Administrative Office of Pennsylvania Courts and the requestor simultaneously.
- B. If the court or office cannot respond to the request as set forth in subsection A, the court or office shall concurrently give written notice of the same to the requestor and Administrative Office of Pennsylvania Courts.

Commentary

Implementing the provisions of this policy should not unduly burden the courts and offices, nor should implementation impinge upon the judiciary's primary service – the delivery of justice. The question raised by this section is not whether there is to be access, but rather *how and when access should be afforded*.

In drafting this section, the Committee was faced with two competing interests. First, any requirements imposed upon courts and offices regarding how and when they should respond to these requests must not interfere with the courts' and offices' ability to conduct their day-to-day operations, often with limited resources. Second, all requests should be handled by courts and offices in a predictable, consistent, and timely manner statewide. It is the Committee's opinion that the provisions of this section strike the appropriate balance between these two competing interests.

As noted earlier in this Report, FOIA and RTKA are not applicable to the judiciary. However, the Committee when drafting this section of the policy paid particularly close attention as to how both Acts address this issue. In fact, the Committee incorporated elements of those Acts into this section of the policy.²¹²

²¹² 5 U.S.C. § 552(a)(6) (2006) and PA. STAT. ANN. tit. 65, §§ 66.3-3 (West 2006).

Under subsection A(4), the court or office shall specifically state in its written notification to the requestor the expected date that the information will be available. If the information will not be available within 30 business days, the court or office shall provide written notification to the requestor and the Administrative Office of Pennsylvania Courts at the same time. Possible reasons a court or office may need the additional period of time include:

- the request, particularly if for bulk distribution of electronic case records, involves such voluminous amounts of information that the court or office may not be able to fulfill the same within the initial 10 business day period without substantially impeding the orderly conduct of the court or office; or
- the court or office is not able to determine if this policy permits the release of the requested information within the initial 10 business day period. Therefore, the court or office may require an additional period of time to conduct an administrative review of the request to make this determination.

If the court or office believes that the requestor has failed to comply with this policy, written notification to the requestor should set forth the specific areas of non-compliance. For example, a requestor may have failed to pay the appropriate fees associated with the request.

Any written notification to the requestor stating that the information requested cannot be provided shall set forth the reason(s) for this determination.

If the court or office is unable to respond to the request as set forth above, the AOPC should work with the record custodian or appropriate administrative authority (e.g., district court administrator) to facilitate the fulfillment of the request consistent with the policy, as currently is done for MDJS requests. As a last resort, the AOPC may handle these requests directly.

The phrase "in writing" includes but is not limited to electronic communications such as email and fax.

The Committee also discussed when a request is partially fulfilled (e.g., if the requestor asked for a defendant's name, address, and social security number, pursuant to Section 3.00 of this policy a court or office could not release the defendant's social security number or street address) whether the court or office should specifically set forth that it has the restricted information on record although it did not release the same. In the judgment of the Committee it is important that requestors are apprised that all requests for information are fulfilled pursuant to a statewide policy without necessarily pointing out each piece of information that is in the court's or office's possession but not released under the policy. Therefore, when responding to any request, a court or office should provide a general statement to the requestor that "your request for information is being fulfilled consistent with the provisions of the Unified Judicial System Public Access Policy."

The time frames set forth in this section will usually only concern requests for bulk distribution for electronic case records.

Section 5.00 FEES

- A. Reasonable fees may be imposed for providing public access to electronic case records pursuant to this policy.
- B. A fee schedule shall be in writing and publicly posted.
- C. A fee schedule in any judicial district, including any changes thereto, shall not become effective and enforceable until:
 - 1. a copy of the proposed fee schedule is submitted by the president judge to the Administrative Office of Pennsylvania Courts; and
 - 2. the Administrative Office of Pennsylvania Courts has approved the proposed fee schedule.

COMMENTARY

The Committee first considered whether to charge a fee for fulfilling public access requests. It was noted that public access requests are often for information that is not readily available and require staff and equipment time to fulfill the same. The Committee asserts that these costs incurred by courts and offices in fulfilling a request should be passed on to the requestor. Clearly, absent the request, the court or office would not incur these costs.

The Committee noted that the MDJS policy provides that “[c]osts shall be assessed based on the actual costs of the report medium, a pro-rata share of computer and staff time, plus shipping and handling.”²¹³ The RTKA also provides that fees may be charged by agencies in fulfilling RTKA requests.²¹⁴ The Committee reviewed the RTKA fee schedules of the Governor’s Office, Lieutenant Governor’s Office, and the Executive Offices²¹⁵ and the Department of Environmental Protection.²¹⁶ Outside of Pennsylvania, the Committee also noted that several states charge a fee to a requestor when responding to a public access request (which will be discussed in greater detail below). Therefore, the Committee opines that the current practice of charging public access requestors a fee for fulfilling their requests should continue.

The Committee reviewed the costs charged by various state courts in responding to public access requests. In general, it appears that most court systems charge a fee that is intended to recoup from the requestor the costs incurred by the court in responding to the

²¹³ See MDJS Policy, Section II.B.5.

²¹⁴ See PA. STAT. ANN. tit. 65, § 66.7 (West 2006).

²¹⁵ See *Commonwealth of Pennsylvania Governor’s Office, Lieutenant Governor’s Office, and Executive Offices – Right-To-Know Request Policy*.

²¹⁶ See *DEP and the Pennsylvania Right-To-Know Law Schedule of Charges for Public Access*.

request. These court systems include Colorado,²¹⁷ New York,²¹⁸ Vermont,²¹⁹ Maryland,²²⁰ Idaho,²²¹ California,²²² and Florida.²²³ However, some court systems, such as Minnesota,²²⁴ Arizona,²²⁵ and Utah²²⁶ appear to permit a cost/fee that is in excess of the costs incurred in responding to the request. The Committee also noted that the RTKA and FOIA differ on this issue as well. Specifically, the RTKA provides that fees must be reasonable and based on the prevailing fees for comparable services provided by local business entities, except for postage fees which must be the actual cost of postage.²²⁷ However, FOIA provides that only the direct

²¹⁷ Colo. DJD. 05-01 Section 6.00 – Fees for Access – “Clerks of Court and the State Court Administrator’s Office may charge a fee for access to court records pursuant to § 24-72-205(2) and (3) C.R.S. and Chief Justice Directive 96-01. The costs shall include: administrative personnel costs associated with providing the court records; direct personnel costs associated with programming or writing queries to supply data; the personnel costs associated with testing the data for validity and accuracy; maintenance costs associated with hardware and software that are necessary to provide data as expressed in Computer Processing Unit (CPU), network costs, and operating costs of any reproduction medium (i.e. photocopies, zip disks, CD, etc). To the extent that public access to electronic court records is provided exclusively through a vendor, the State Court Administrator’s Office will ensure that any fee imposed by the vendor for the cost of providing access is reasonable. The authorization to charge fees does not imply the service is currently available.”

²¹⁸ *Report to the Chief Judge of the State of New York* by the Commission on Public Access to Court Records (February, 2004), p. 7-8. The Report provides that “records over the Internet [should] be free of charges; if the [court] determines that a charge is advisable we recommend that the charge be nominal and that it in no event should exceed the actual cost to provide such record.”

²¹⁹ 1 VT. STAT. ANN. § 316(b)-(d) and (f) provides that if any cost is assessed it is based upon the actual cost of copying, mailing, transmitting, or providing the document.

²²⁰ Maryland Rule of Procedure 16-1002(d) provides that “Reasonable fees means a fee that bears a reasonable relationship to the actual or estimated costs incurred or likely to be incurred in providing the requested access. Unless otherwise expressly permitted by these Rules, a custodian may not charge a fee for providing access to a court record that can be made available for inspection, in paper form or by electronic access, with the expenditure of less than two hours of effort by the custodian or other judicial employee. A custodian may charge a reasonable fee if two hours or more of effort is required to provide the requested access. The custodian may charge a reasonable fee for making or supervising the making of a copy or printout of a court record.”

²²¹ IDAHO ADMIN. R. 32(1). This Rule provides the clerk should charge \$1.00 a page for making a copy of any record filed in a case (per Idaho Stat. § 31-3201) and for any other record the clerk shall charge the actual cost of copying the record, including personnel costs.

²²² CAL. CT. R. 2076 provides that the court may impose fees for the cost of providing public access to its electronic records as provided by Government Code section 68150(h) (which sets forth that access shall be provided at cost).

²²³ See FLA. J. ADMIN. R. 2.051(e)(3) and FLA. STAT. ANN. § 119.07 which appears to permit the charging for cost of duplication, labor and administrative overhead.

²²⁴ MN ST ACCESS TO REC RULE 8(6) (WEST 2006). “When copies are requested, the custodian may charge the copy fee established by statute but, unless permitted by statute, the custodian shall not require a person to pay a fee to inspect a record. When a request involves any person’s receipt of copies of publicly accessible information that has commercial value and is an entire formula, pattern, compilation, program, device, method, technique, process, data base, or system developed with a significant expenditure of public funds by the judicial branch, the custodian may charge a reasonable fee for the information in addition to costs of making, certifying, and compiling the copies.”

²²⁵ Arizona Rule 123 Public Access to the Judicial Records of the State of Arizona, Subsection (f)(3) provides different levels of fees for requestors for non-commercial purposes and commercial purposes. For non-commercial requestors “[i]f no fee is prescribed by statute, the custodian shall collect a per page fee based upon the reasonable cost of reproduction.” See Rule 123(f)(3)(A). For commercial requestors, “the custodian shall collect a fee for the cost of: (i) obtaining the original or copies of the records and all redaction costs; and (ii) the time, equipment and staff used in producing such reproduction.” See Rule 123(f)(3)(B)(i) and (ii).

²²⁶ UTAH J. ADMIN. R. 4-202.08 establishes a uniform fee schedule for requests for records, information, and services.

²²⁷ See PA. STAT. ANN. tit. 65, § 66.7 (West 2006).

costs incurred by the agency can be charged to the requestor.²²⁸

If fees are based on the prevailing market rate, then fees will not only recoup the actual costs incurred by the particular court of office but also result in a profit. The objective of courts or offices in responding to public access requests is not to make a profit; rather it is to foster the values of open court records without unduly burdening court resources. Put simply, fees should not be financial barriers to accessing case record information. Fees assessed by courts or offices in satisfying public access requests must be reasonable, fair and affordable. To aid in defining the parameters of reasonable, fair and affordable fees, the Committee finds the definition for charges in the Vermont²²⁹ and New York²³⁰ policies instructive. Generally, the public access request fees should not exceed the actual costs associated with producing the requested information for copying, mailing or other methods of transmission, materials used and staff time.

In the judgment of the Committee, it would be beneficial to both the public and AOPC if all courts or offices were required to promulgate their fee schedules. Therefore, the Committee recommends that a court's or office's fee schedule be in writing and publicly posted (preferably so as to permit viewing both in person and remotely via the Internet). This method is similar to the procedures adopted for the promulgation of local rules.²³¹

Subsection C provides that the Administrative Office of Pennsylvania Courts must approve all judicial district fee schedules – to include adoption of any new fees or fee increases -- before the same are effective and enforceable.²³² The purpose of this provision is to further a unified approach to fees associated with case record access in the Pennsylvania Judiciary – with an eye toward avoiding inconsistent and unfair charges amongst the various jurisdictions. This type of approach is not novel, as it is quite similar to the procedure set forth in Rule of Judicial Administration 5000.7(f) pertaining to the approval of court transcripts.

²²⁸ 5 U.S.C. § 552(a)(4)(a)(iv) (2006). In addition, the Committee noted that for certain types of requestors FOIA provides that the first two hours of search time or the first 100 pages of duplication can be provided by the agency without charging a fee. 5 U.S.C. § 552(a)(4)(a)(iv)(II) (2006).

²²⁹ 1 VT. STAT. ANN. § 316(b)-(d) and (f) provides that if any cost is assessed it is based upon the actual cost of copying, mailing, transmitting, or providing the document.

²³⁰ *Report to the Chief Judge of the State of New York* by the Commission on Public Access to Court Records (February, 2004), p. 7-8. The Report provides that “records over the Internet [should] be free of charges; if the [court] determines that a charge is advisable we recommend that the charge be nominal and that it in no event should exceed the actual cost to provide such record.”

²³¹ See PA.R.J.A.103(c), PA. R. CRIM. P. 105(c) and PA. R. C. P. No. 239(c).

²³² See Pa. Const. Art. V, § 10(c); Pa.R.J.A. 501(a), 504(b), 505(11), 506(a); 42 Pa.C.S. § 4301.

SECTION 6.00 CORRECTING DATA ERRORS

- A. A party to a case, or the party's attorney, seeking to correct a data error in an electronic case record shall submit a written request for correction to the court in which the record was filed.
- B. A request to correct an alleged error contained in an electronic case record of the Supreme Court, Superior Court or Commonwealth Court shall be submitted to the prothonotary of the proper appellate court.
- C. A request to correct an alleged error contained in an electronic case record of the Court of Common Pleas, Philadelphia Municipal Court or a Magisterial District Court shall be submitted and processed as set forth below.
 - 1. The request shall be made on a form designed and published by the Administrative Office of Pennsylvania Courts.
 - 2. The request shall be submitted to the clerk of courts if the alleged error appears in an electronic case record of the Court of Common Pleas or Philadelphia Municipal Court. The requestor shall also provide copies of the form to all parties to the case, the District Court Administrator and the Administrative Office of Pennsylvania Courts.
 - 3. The request shall be submitted to the Magisterial District Court if the alleged error appears in an electronic case record of the Magisterial District Court. The requestor shall also provide copies of the form to all parties to the case, the District Court Administrator and the Administrative Office of Pennsylvania Courts.
 - 4. The requestor shall set forth on the request form with specificity the information that is alleged to be in error and shall provide sufficient facts including supporting documentation that corroborates the requestor's contention that the information in question is in error.
 - 5. Within 10 business days of receipt of a request, the clerk of courts or Magisterial District Court shall respond in writing to the requestor, all parties to the case, and the Administrative Office of Pennsylvania Courts, in one of the following manners:
 - a. the request does not contain sufficient information and facts to adequately determine what information is alleged to be error; accordingly, the request form is being returned to the requestor; and no further action will be taken on this matter unless the requestor resubmits the request with additional information and facts.
 - b. the request does not concern an electronic case record that is covered by this policy; accordingly, the request form is being returned to the requestor; no further action will be taken on this matter.

- c. it has been determined that an error does exist in the electronic case record and that the information in question has been corrected.
 - d. it has been determined that an error does not exist in the electronic case record.
 - e. the request has been received and an additional period not exceeding 30 business days is necessary to complete the review of this matter.
6. A requestor has the right to seek review of a final decision under subsection 5(a)-(d) rendered by a clerk of courts or a Magisterial District Court within 10 business days of notification of that decision.
- a. The request for review shall be submitted to the District Court Administrator on a form that is designed and published by the Administrative Office of Pennsylvania Courts.
 - b. If the request for review concerns a Magisterial District Court's decision, it shall be reviewed by the judge assigned by the President Judge.
 - c. If the request for review concerns a clerk of courts' decision, it shall be reviewed by the judge who presided over the case from which the electronic case record alleged to be in error was derived.

COMMENTARY

An important aspect of transparent electronic case records and personal privacy/security is the quality of the information in the court record. The information in UJS electronic case records should be complete and accurate, otherwise incorrect information about a party to a case or court proceeding could be disseminated. The Committee recognizes that electronic case records are as susceptible to errors and omissions as any other public record, particularly when considered in view of the widespread Internet use and access, and agreed procedures for correcting these errors should be incorporated into this policy.

The power of the court to correct errors in its own records is inherent.²³³ "Equity enjoys flexibility to correct court errors that would produce unfair results."²³⁴ Therefore, the Committee opines that the authority for a court to correct errors in its own records is inherent and does not arise from the Criminal History Record Information Act (CHRIA).²³⁵ Although, the Committee does not interpret CHRIA as being applicable to the correction of court records,²³⁶ the

²³³ E.g. Jackson v. Hendrick, 746 A.2d 574 (Pa. 2000).

²³⁴ Id. at 577.

²³⁵ 18 Pa.C.S. § 9101 – 9183.

²³⁶ The Committee notes that it is unclear the extent, if any, to which CHRIA is applicable to court records. Specifically, 18 Pa.C.S. Section 9103 provides that CHRIA is applicable to "person within this Commonwealth and to any agency of the

Committee consulted the correction of error section of CHRIA in drafting this section of the policy,²³⁷ specifically with regard to the safeguards that are found in CHRIA related to the time limitations for action and appeals. CHRIA permits a criminal justice agency 60 days to review a challenge to the accuracy of its record. The Committee believes the time for a decision concerning an alleged error in a court record should be limited in this section of the policy to a maximum of 40 business days. CHRIA also permits the challenger who believes the agency decision is in error to file an appeal. Similarly, in this policy, Subsection 6 permits a requestor who believes the decision is erroneous to seek administrative review as well.

Subsection 6 provides an individual who asserts that an electronic case record is in error an administrative process by which that allegation can be reviewed and resolved. This administrative review process is modeled after the review process set forth in CHRIA and is in addition to any other remedies provided by law. It is important to note the review provided for in Subsection 6 by the Court of Common Pleas is administrative in nature.

The Committee also took note of corrective procedures that other states, including Arizona,²³⁸ Colorado,²³⁹ Kansas,²⁴⁰ Minnesota,²⁴¹ and Wisconsin²⁴² as well as the CCJ/COSCA Guidelines,²⁴³ establish in their policies and/or court rules (enacted or proposed).

In considering the procedures for correcting errors, it is important to emphasize that this section does not provide a party who is dissatisfied with a court's decision, ruling or judgment a new avenue to appeal the same by merely alleging that there is an error in the court's decision, ruling or judgment. Rather, this section permits a party to "fix" information that appears in an

Commonwealth or its political subdivisions which collects, maintains, disseminates or receives criminal history record information." Clearly, the court is not an agency, political subdivision or a person of the Commonwealth. Moreover, Criminal History Record Information is defined in 18 Pa.C.S. Section 9102 as "does not include... information and records specified in section 9104 (relating to scope)." 18 Pa.C.S. Section 9014(a)(2) appears to reference "any documents, records, or indices prepared or maintained by or filed in any court of this Commonwealth, including but not limited to the minor judiciary." Moreover, Section 9104(b) provides that "court dockets... and information contained therein shall... for the purpose of this chapter, be considered public records." If one does contend that the correction procedures set forth in CHRIA are applicable to court records, it is important to note that the procedure provides that a person who wants to appeal a court's decision regarding an alleged error files that appeal with the Attorney General Office. Thus, the Attorney General Office, a part of the Executive Branch of Government, would be reviewing a decision issued by a Court of the Unified Judicial System. Such a procedure appears to raise some constitutional concerns.

²³⁷ See 18 Pa.C.S. § 9152.

²³⁸ *Report and Recommendation of the Ad Hoc Committee to Study Public Access to Electronic Records* dated March 2001 Sections (V)(8) and (VI)(8); ARIZ. SUP. CT. R. 123(g)(6) (this provision, and others related to public access, was adopted by Order of Arizona Supreme Court dated June 6, 2005 to be effective December 1, 2005; effective date postponed by Court's Order dated September 27, 2005 to permit effective and efficient implementation of the provisions).

²³⁹ Colo. CJD. 05-01 Section 9.00 provides for a process to change inaccurate information in a court record.

²⁴⁰ K.S.A. § 60-260 and Kansas Rules Relating to District Courts Rule 196(f).

²⁴¹ MN ST ACCESS TO REC RULE 7(5) (WEST 2006).

²⁴² Wisconsin Circuit Court Access (WCCA) Web site, "The information on a case is incorrect.

Could you correct the information?" at: <http://wcca.wicourts.gov/faqnav.xsl;jsessionid>

=8036D1470A038AB3CBB55B35613773C6.render4#Faql1 and "Who do I contact if I want clarification about information displayed on WCCA?" at: <http://wcca.wicourts.gov/faqnav.xsl;jsessionid>=

8036D1470A038AB3CBB55B35613773C6.render4#Faql18

²⁴³ See CCJ/COSCA *Guidelines*, p. 69.

electronic case record which does not, for one reason or another, correctly set forth the facts contained in the official court record (paper case file).

It is anticipated that those reviewing these alleged errors shall compare the information set forth in the electronic case record against the official court record. If the information in the electronic case record and official court record is consistent, the request to correct the electronic case record should be denied. If the information is not consistent, the reviewer shall determine what, if any, corrections are needed to the electronic case record. Nonetheless, if the requestor believes that the official court record is in error, such an alleged error does not fall within the purview of this section. Rather, the current practices in place in the courts to resolve these errors should continue.

By way of example, the official court records of a case set forth that the defendant's name is "John Smith", however, the electronic case record provides that the defendant's name is "John Smyth". Obviously this was a clerical or data entry error. This type of error falls within the purview of this section. However, if for example, a party claims that he was convicted of the crime of simple assault, but the official court record sets forth that he was convicted of the crime of driving under the influence, this error does not fall within the purview of this section in that the requestor is alleging an error in the official court record.

This section does not preclude a court from accepting and responding to verbal or informal requests to correct a data error in an electronic case record. However, if a requestor wishes to enjoy the benefits of the relief and procedures set forth in this section, he/she must file a formal written request. This procedure is consistent with the RTKA which permits a governmental agency to accept and respond to verbal requests, but provides that "[i]n the event that the requestor wishes to pursue the relief and remedies provided for in this act, the requestor must initiate such relief with a written request."²⁴⁴

In Subsection A, a "party's attorney" means attorney of record.

In Subsection B, the Committee understands that the errors that may appear in appellate court records are different in nature and kind than those that appear at the lower courts. Specifically, most errors will concern the original records from the lower court that the appellate court is reviewing. Therefore, the Committee believes that appellate courts' current practices in resolving these errors should continue.

The term "clerk of courts" includes any office performing the duties of a clerk of courts, regardless of titles (i.e., Clerk of Quarter Sessions, Office of Judicial Support, Office of Judicial Records).

²⁴⁴ 65 P.S. § 66.2(b).

SECTION 7.00 CONTINUOUS AVAILABILITY OF POLICY

A copy of this policy shall be continuously available for public access in every court or office that is using the PACMS, CPCMS, and/or MDJS.

COMMENTARY

The Committee opines that it is essential that the public has access to the provisions of this policy on a continuing basis. In drafting this language, the Committee found that the statewide Rules of Criminal Procedure and Civil Procedure have similar provisions regarding the continuing availability of local rules in each judicial district.²⁴⁵ The Committee used that language as a guide in drafting this provision. The Committee recommends that this policy be publicly posted (preferably so as to permit viewing both in person and remotely via the Internet).

²⁴⁵ PA. R. CRIM. P. 105(c)(5) and PA. R. C. P. No. 239(c)(5) provide that the local rules shall be kept continuously available for public inspection and copying in the office of the prothonotary or clerk of courts. Upon request and payment of reasonable costs of reproduction and mailing, the prothonotary or clerk shall furnish to any person a copy of any local rule.

Additional Recommendations Concerning Paper Case Records

As noted in the Introduction to the Report, the practical difficulties associated with covering paper case records concerning a single case counseled against inclusion in this policy. Even so, the Committee recommends that the UJS take steps in the future to avoid the personal privacy and security issues that may arise with respect to these records.

The Committee proposes the creation of a sensitive information data form. When filing a document with a court or office, litigants and their attorneys would be required to refrain from inserting any sensitive information (such as social security numbers, financial account numbers, etc) in the filed document. Rather, all sensitive information should be inserted on the sensitive information data form, which would not be accessible to the public. Thus, the use of this form should over time help prevent sensitive information from appearing in the paper records that are accessible to the public. The Committee notes that Washington²⁴⁶ and Kansas²⁴⁷ already uses a sensitive information data form, and Arizona²⁴⁸ and Minnesota²⁴⁹ are considering enacting rules/policies to provide for the same. The Committee recommends that this sensitive information data form be available at the courthouse and via the Internet.

²⁴⁶ WASH. CT. GR. 22(c)(2) (2006). Please note that this rule only applies to family law cases.

²⁴⁷ Kansas Rules Relating to District Courts Rule 123 (Rule Requiring Use of Cover Sheets and Privacy Policy Regarding Use of Personal Identifiers in Pleading). The Rule provides that in divorce, child custody, child support or maintenance cases, a party must enter certain information only on the cover sheet which is not accessible to the public. Specifically, a party's or party's child's SSN and date of birth must be entered on the cover sheet only. Moreover, the Rule provides that unless required by law, attorneys and parties shall not include SSNs in pleadings filed with the court (if must be included use last four digits), dates of birth (if must be included use year of birth), and financial account numbers (if must be included use last four digits).

²⁴⁸ See Supreme Court of Arizona's Order of September 27, 2005 vacating amendments to Rule 123 (that were set to become effective on December 1, 2005). The September Order creates a working group of court officials to resolve outstanding issues and issue a report to the Court on or before June 1, 2006.

²⁴⁹ *Recommendations of Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (June 28, 2004), p. 74-75.