THE COURTS

Title 204—JUDICIAL SYSTEM GENERAL PROVISIONS

PART II. GENERAL ADMINISTRATION

[204 PA. CODE CH. 29]

Promulgation of Financial Regulations Pursuant to 42 Pa.C.S. § 3502(a); No. 274 Judicial Administration; Doc. No. 1

Order

Per Curiam:

And now, this 29th day of August, 2005 it is *Ordered* pursuant to Article V, Section 10(c) of the Constitution of Pennsylvania and Section 3502(a) of the Judicial Code, 42 Pa.C.S. § 3502(a), that the Court Administrator of Pennsylvania is authorized to promulgate the following Financial Regulations. The fees outlined in the Financial Regulations are effective as of January 1, 2006.

To the extent that notice of proposed rule-making may be required by Pa.R.J.A. No. 103, the immediate promulgation of the regulations is hereby found to be in the interests of efficient administration.

This Order is to be processed in accordance with Pa.R.J.A. No. 103(b) and is effective immediately.

Annex A

TITLE 204. JUDICIAL SYSTEM GENERAL PROVISIONS

PART II. GENERAL ADMINISTRATION

CHAPTER 29. MISCELLANEOUS PROVISIONS

Subchapter K. COSTS, FINES AND FEES

TITLE 42. JUDICIARY AND JUDICIAL PROCEDURE

PART IV. FINANCIAL MATTERS

CHAPTER 17. GOVERNANCE OF THE SYSTEM

CHAPTER 35. BUDGET AND FINANCE

Subchapter A. GENERAL PROVISIONS

The Pennsylvania Supreme Court, pursuant to Art. V, § 10 of the Pennsylvania Constitution, and 42 Pa.C.S. § 1721, has authorized the Court Administrator of Pennsylvania to promulgate regulations relating to the accounting methods to be utilized in connection with the collection of fees and costs charged and collected by prothonotaries, and clerks of courts of all courts of common pleas, or by any officials designated to perform the functions thereof, as well as by the minor judiciary, including magisterial district judges, Philadelphia Municipal Court and Philadelphia Traffic Court.

Under authority of said Administrative Order and pursuant to the authority vested in the governing authority under Section 3502(a) of the Judicial Code, 42 Pa.C.S. § 3502(a), the following regulations are adopted to implement Act 113 of 2001, 42 Pa.C.S. §§ 1725.1(f) and 3571-(c)(4)(as amended).

42 Pa.C.S. § 1725.1. Costs.

(a) *Civil cases.*—In calendar year 2006, the costs to be charged by magisterial district judges in every civil case, except as otherwise provided in this section, shall be as follows:

(1) Actions involving $500 or less	$41.50
(2) Actions involving more than $500 but not more than $2,000	$55.50
(3) Actions involving more than $2,000 but not more than $4,000	$69.00
(4) Actions involving more than $4,000 but not more than $8,000	$103.50
(5) Landlord-tenant actions involving less than $2,000	$62.50
(6) Landlord-tenant actions involving more than $2,000 but not more than $4,000	$76.00
(7) Landlord-tenant actions involving more than $4,000 but not more than $8,000	$103.50
(8) Order of execution	$31.50
(9) Objection to levy	$14.00
(10) Reinstatement of complaint	$7.00
(11) Entering Transcript on Appeal or Certiorari	$3.50

Said costs shall not include, however, the cost of postage and registered mail which shall be borne by the plaintiff.

(a.1) *Custody cases.*—In calendar year 2006, the cost (in addition to the cost provided by general rule) to be charged by the court of common pleas shall be as follows:

(1) Custody cases, except as provided in section 1725(c)(2)(v)	$6.50

(b) *Criminal cases.*—In calendar year 2006, the costs to be charged by the minor judiciary or by the court of common pleas where appropriate in every criminal case, except as otherwise provided in this section, shall be as follows:

(1) Summary conviction, except motor vehicle cases	$39.50
(2) Summary conviction, motor vehicle cases, other than paragraph (3)	$31.50
(3) Summary conviction, motor vehicle cases, hearing demanded	$37.50
(4) Misdemeanor	$45.00
(5) Felony	$52.00

Such costs shall not include, however, the cost of postage and registered mail which shall be paid by the defendant upon conviction.

(c) *Unclassified costs or charges.*—In calendar year 2006, the costs to be charged by the minor judiciary in the following instances not readily classifiable shall be as follows:

(1) Entering transcript of judgment from another member of the minor judiciary	$7.00
(2) Marrying each couple, making record thereof, and certificate to the parties	$34.50

(3) Granting emergency relief pursuant to 23 Pa.C.S. Ch. 61 (relating to protection from abuse) $14.00

(4) Issuing a search warrant (except as provided in subsection (d)) $14.00

(5) Any other issuance not otherwise provided in this subsection $14.00

42 Pa.C.S. § 3571.

In calendar year 2006, Commonwealth portion of fines, etc.

* * * * *

(2) Amounts payable to the Commonwealth:

(i) Summary conviction, except motor vehicle cases $14.00

(ii) Summary conviction, motor vehicle cases other than subparagraph (iii) $14.00

(iii) Summary conviction, motor vehicle cases, hearing demanded $14.00

(iv) Misdemeanor $18.00

(v) Felony $27.73

(vi) Assumpsit or trespass involving:

(A) $500 or less $17.35

(B) More than $500 but not more than $2,000 ..... $27.60

(C) More than $2,000 but not more than $4,000 ..... $41.40

(D) More than $4,000 but not more than $8,000 ..... $69.00

(vii) Landlord-tenant proceeding involving:

(A) $2,000 or less $27.60

(B) More than $2,000 but not more than $4,000 ..... $34.55

(C) More than $4,000 but not more than $8,000 ..... $48.30

(viii) Objection to levy $7.00

(ix) Order of execution $21.00

(x) Issuing a search warrant (except as provided in section 1725.1(d) (relating to costs)) $9.70

(xi) Order of possession $15.00

(xii) Custody cases (except as provided in section 1725(c)(2)(v)) $5.20

[Pa.B. Doc. No. 05-1703. Filed for public inspection September 16, 2005, 9:00 a.m.]

PART VII. ADMINISTRATIVE OFFICE OF PENNSYLVANIA COURTS

[204 PA. CODE CH. 211]

Promulgation of Consumer Price Index Pursuant to 42 Pa.C.S. §§ 1725.1(f) and 3571(c)(4); No. 275 Judicial Administration; Doc. No. 1

Order

Per Curiam:

And now, this 29th day of August, 2005, it is *Ordered* pursuant to Article V, Section 10(c) of the Constitution of Pennsylvania and Section 3502(a) of the Judicial Code, 42 Pa.C.S. § 3502(a), that the Court Administrator of Pennsylvania is authorized to obtain and publish in the *Pennsylvania Bulletin* the percentage increase in the Consumer Price Index for calendar year 2004 as required by Act 113 of 2001, 42 Pa.C.S. §§ 1725.1(f) and 3571(c)(4) (as amended).

Annex A

TITLE 204. JUDICIAL SYSTEM GENERAL PROVISIONS

PART VII. ADMINISTRATIVE OFFICE OF PENNSYLVANIA COURTS

CHAPTER 211. CONSUMER PRICE INDEX

§ 211.1. Consumer Price Index.

Pursuant to Article V, Section 10 of the Pennsylvania Constitution, and 42 Pa.C.S. § 1721, the Supreme Court has authorized the Court Administrator of Pennsylvania to obtain and publish in the *Pennsylvania Bulletin* on or before November 30 the percentage increase in the Consumer Price Index for calendar year 2004 as required by Act 113 of 2001, 42 Pa.C.S. §§ 1725.1(f) and 3571(c)(4) (as amended). See, No. 275 Judicial Administrative Docket No. 1.

The Court Administrator of Pennsylvania reports that the percentage increase in the Consumer Price Index, All Urban Consumers, U. S. City Average, for calendar year 2004 was 3.3% percent. (See, U. S. Department of Labor, Bureau of Labor Statistics, Series CUUROOOOSAO, February 22, 2005.)

[Pa.B. Doc. No. 05-1704. Filed for public inspection September 16, 2005, 9:00 a.m.]

Title 210—APPELLATE PROCEDURE

PART II. INTERNAL OPERATING PROCEDURES

[210 PA. CODE CH. 63]

Amendments to the Internal Operating Procedures of the Supreme Court; No. 376 Supreme Court Rules; Doc. No. 1

Order

Per Curiam

And Now, this 2nd day of September, 2005, it is ordered that the Internal Operating Procedures of the Supreme Court are amended in Section 3 as set forth as follows.

Annex A

TITLE 210. APPELLATE PROCEDURE

PART II. INTERNAL OPERATING PROCEDURES

CHAPTER 63. INTERNAL OPERATING PROCEDURES OF THE SUPREME COURT

§ 63.3. Decisional Procedures.

A. *Argument Sessions.*

* * * * *

3. *Direct Appeals.*

[a. Because they would, under a differently structured judicial system, have gone to intermedi-

ate appellate courts for evaluation, direct appeals shall be submitted for screening rather than automatically accepted for oral argument. Therefore, as soon as briefs are received, all direct appeals other than death penalty cases will be assigned by the prothonotary to a justice on a rotating basis by seniority for preparation of a Disposition Memorandum, which will contain a short recitation of the facts, a brief discussion of the issues, and a recommendation of whether the case should be resolved by

1) a per curiam order;

(Court Note: A per curiam order may be used when the Court's decision:

1) does not establish a new rule of law;

2) does not alter, modify, criticize or clarify an existing rule of law;

3) does not apply an established rule of law to a novel fact situation;

4) does not constitute the only, or only recent binding precedent on a particular point of law;

5) does not involve a legal issue of continuing public interest; or

6) whenever the Court decides such an order is appropriate.)

2) affirmance on the opinion of the court below, plus, where possible/necessary a brief statement of matters not covered by that opinion;

3) submission on briefs; or

4) should be listed for oral argument.

b. Each Disposition Memorandum shall be circulated to the Court within sixty (60) days of assignment, with contemporaneous notice to the prothonotary of the proposed disposition, and shall set a proposed action date of thirty (30) days from the date of circulation. If, after circulation, a majority of justices join the proposed disposition, the case shall be resolved in accordance with the Disposition Memorandum. If less than a majority of justices agree, the case will be listed for oral argument.]

Because they would, under a differently structured judicial system, have gone to intermediate appellate courts for evaluation, direct appeals shall be submitted for screening rather than automatically accepted for oral argument. Therefore, as soon as briefs are received, all direct appeals other than death penalty cases will be assigned by the prothonotary to a justice on a rotating basis by seniority for preparation of a Disposition Memorandum, which will contain a short recitation of the facts, a brief discussion of the issues, and a recommendation of whether the case should be resolved by 1) a per curiam order; 2) affirmance on the opinion of the court below, plus, where possible/necessary a brief statement of matters not covered by that opinion; 3) submission on briefs; or 4) should be listed for oral argument. Each Disposition Memorandum shall be circulated to the Court within sixty (60) days of assignment, with contemporaneous notice to the prothonotary. It shall then be placed on a supplemental list for consideration and vote at the same time as opinions. (See IV. Opinions. A. Circulation schedule 3. Voting). Disposition Memoranda must be circulated to the Court ten (10) days prior to the list date to be placed on the vote list. The case shall thereafter be disposed of or listed for oral argument in accordance with the vote of the majority. If no clear majority emerges, the case will be listed for oral argument.

* * * * *

B. *Assignments.*

* * * * *

3. *Civil and Criminal Appeals.* **[a.]** Cases shall be assigned by the senior member of the majority in such a manner as to achieve equal distribution of assignments, and to avoid delay in deciding cases. If it appears that due to illness of a justice or for some other reason this purpose is not being served, the Chief Justice may, as a matter of his or her discretion, alter the assignment order.

[b.] In the event a justice to whom a case has been assigned subsequently decides to change his or her vote on the decision of the case and ceases to be among the majority, he or she shall provide a draft opinion along with a cover letter explaining the reason for the change of position.

Where appeals other than direct appeals have been submitted, the prothonotary shall direct the case to the Court for disposition after completion of the briefing schedule. The Chief Justice will assign the case for preparation of a draft opinion to an individual justice in the rotation established by seniority.

4. *Direct Appeals.* **[a.]** An argued direct appeal will be assigned to the justice who prepared the Disposition Memorandum, unless after preliminary vote his or her position is not that of the majority. In such an instance, the assignment shall be made by the senior member of the majority.

[b. Where appeals have been submitted, the prothonotary shall direct the case to the Court for disposition after completion of the briefing schedule. The Chief Justice will assign the case for preparation of a draft opinion to an individual justice in the rotation established by seniority.]

A direct appeal which the Court has determined shall be decided by opinion on the submitted briefs shall be assigned to the justice who prepared the Disposition Memorandum.

5. *Per Curiam Orders*

1) A per curiam order may be used when the Court's decision:

a) does not establish a new rule of law;

b) does not alter, modify, criticize or clarify an existing rule of law;

c) does not apply an established rule of law to a novel fact situation;

d) does not constitute the only, or only recent binding precedent on a particular point of law;

e) does not involve a legal issue of continuing public interest; or

f) whenever the Court decides such an order is appropriate.

2) A per curiam order reversing an order of the lower court, must cite to controlling legal authority or give a full explanation as to the reasons for reversal.

[Pa.B. Doc. No. 05-1705. Filed for public inspection September 16, 2005, 9:00 a.m.]

Title 255—LOCAL COURT RULES

BERKS COUNTY

Rules of Court; No. 98-8009 Prothonotary; No. 1-MD-2000 Clerk of Courts

Order

And Now, this 23rd day of August, 2005, it is hereby *Ordered* and *Decreed* that the following local rule for Papers Presented By Persons Unauthorized By State Rules in the 23rd Judicial District composed of Berks County be, and the same is promulgated herewith, to become effective thirty days after the publication of the rule in the *Pennsylvania Bulletin*:

Rule 401.1 Papers Presented By Persons Unauthorized By State Rules

Any papers or documents that are submitted on behalf of an individual party by someone other than the party's attorney of record as defined by Pa.R.C.P. 76 or by the party pro se shall be accepted by the prothonotary or clerk of courts as a communication only and no further action shall be taken. Such papers will not be forwarded to the assigned judge for further consideration. A copy of the papers accepted will be sent to the party's attorney of record or the party if no attorney has entered an appearance for the party. The following notice shall be attached to the returned copies:

NOTICE

The attached papers were accepted on (date). These papers were not forwarded to the assigned judge due to the failure to comply with B.R.J.A. 401.1.

The Law Librarian of Berks County is *Ordered* and *Directed* to do the following:

1. File ten (10) certified copies of this Order with the Administrative Office of Pennsylvania Courts for distribution in accordance with Pa.R.J.A. 103(c);

2. File two (2) certified copies of this Order with the Legislative Reference Bureau for publication in the *Pennsylvania Bulletin*;

3. File one (1) certified copy of this Order with the Civil Procedural Rules Committee of the Supreme Court of Pennsylvania;

4. File one (1) certified copy of this Order with the Berks County Law Library; and

5. Have other, non-certified copies of this Order continually available for public inspection and copying.

By the Court

ARTHUR E. GRIM,
President Judge

[Pa.B. Doc. No. 05-1706. Filed for public inspection September 16, 2005, 9:00 a.m.]

FAYETTE COUNTY

Local Rule 227.1 Motion for Post-Trial Relief; Civil Division No. 2134 of 2005 GD

Order

And Now, this 25th day of August, 2005, pursuant to Rule 239 of the Pennsylvania Rules of Civil Procedure, it is hereby ordered that Local Rule 227.1 is amended to read as follows.

The Prothonotary is directed as follows:

(1) Seven certified copies of the Local Rule shall be filed with the Administrative Office of Pennsylvania Courts.

(2) Two certified copies and diskette of the Local Rule shall be distributed to the Legislative Reference Bureau for publication in the *Pennsylvania Bulletin*.

(3) One certified copy of the Local Rule shall be sent to the State Civil Procedural Rules Committee.

(4) One certified copy shall be sent to the Fayette County Law Library.

(5) One certified copy shall be sent to the Editor of the *Fayette Legal Journal*.

This Local Rule shall be continuously available for public inspection and copying in the Office of the Prothonotary. Upon request and payment of reasonable costs of reproduction and mailing, the Prothonotary shall furnish to any person a copy of any local rule.

This Local Rule shall be effective 30 days after the date of publication in the *Pennsylvania Bulletin*.

By the Court

CONRAD B. CAPUZZI,
President Judge

Rule 227.1 Motion for Post-Trial Relief

(a) A motion for post-trial relief shall be presented in Motions Court as a Routine Motion within ten (10) days after the date it is filed of record, accompanied by a transcript order or a statement that no transcript is necessary, and together with a proposed order for the Court's use in setting the date and time for argument, or in ordering that the matter be submitted on briefs.

(1) Unless otherwise ordered, the brief of the moving party shall be served on all parties and the assigned Judge within fifteen (15) days from the presentation of the motion pursuant to F.C.R. 208.3(a); and the briefs of all responding parties shall be served on all other parties and the assigned Judge within (15) days after service of the moving party's brief. A certificate of service shall be filed of record, but the brief itself need not be filed.

(2) Failure to comply with the briefing schedule may result in the denial of oral argument, a civil contempt fine of up to $100 per day, deemed waiver of issues not fully developed, and/or such other sanctions as are appropriate. The briefing schedule shall not be stayed pending completion of the transcript unless specially ordered by the Court.

[Pa.B. Doc. No. 05-1707. Filed for public inspection September 16, 2005, 9:00 a.m.]

MONROE COUNTY

Promulgation of Local Rules of Civil Procedure; No. 6513 CV 2005

Order

And Now, this 15th day of August, 2005, Monroe County Rules of Civil Procedure 206.8(a) and 206.8(b) are hereby promulgated effective thirty (30) days after publication in the *Pennsylvania Bulletin*, in accordance with Pa.R.C.P. No. 239. In conformity with Pa.R.C.P. 239, seven (7) certified copies of the within Order and Local Rules shall be filed by the Court Administrator with the Administrative Office of Pennsylvania Courts. Two (2) certified copies and diskette shall be distributed to the Legislative Reference Bureau for publication in the *Pennsylvania Bulletin*. One (1) certified copy shall be filed with the Civil Procedural Rules Committee of the Supreme Court of Pennsylvania. One (1) copy shall be forwarded to the *Monroe County Legal Reporter* for publication. Copies shall be kept continuously available for public inspection in the Office of the Monroe County Prothonotary, the Office of the Court Administrator and the Monroe County Law Library.

By the Court

RONALD E. VICAN,
President Judge

Rule 206.8(a)—Petition for Private Detective and/or Security Guard License

(1) *Definitions:*

(i) "Applicant"—includes any private detective, the business of detective agency, investigator, the business of investigator, security guard, or the business of watch, guard, or patrol agency.

(ii) "Private Detective"—includes any person, partnership, association or corporation, engaged in the private detective business, including individual private detectives, private detective agencies, investigators, or the business of investigator, or businesses providing watch, guard or patrol agency services. (Definition derived from The Private Detective Act of 1953, as amended, 22 P. S. § 12.)

(iii) The term "security guard" includes uniformed or nonuniformed security guards, any patrol agency and/or individuals who are employed full time or part time, on a temporary or permanent basis, to patrol, guard, protect, monitor, regulate, secure or watch over persons and/or property, either real or personal. (Definition derived from The Private Detective Act of 1953, as amended. 22 P. S. § 12(e).)

(2) *Application for Private Detective License:*

(i) An Applicant(s) (or Applicant's counsel, hereafter "Applicant/Attorney"), seeking a private detective or security guard license pursuant to The Private Detective Act of 1953, as amended (hereafter "The Act"), shall file an original and one copy of a Petition for Private Detective or Security Guard License with the Clerk of Courts.

(ii) Applicant must comply with all requirements set forth in the Act and the Petition shall be accompanied by all documentation required under § 14 of The Act.

(iii) The Clerk of Courts shall forward a copy of the Petition to the Court Administrator.

(3) Applicant/Attorney shall serve a copy of the Petition on the District Attorney of Monroe County and shall file a Certificate of Service with the Clerk of Courts evidencing such service.

(4) *Fingerprints of Applicant:*

(i) In accordance with the Act, Applicant/Attorney shall submit, along with the Petition, fingerprint order cards to the Clerk of Courts;

(ii) The Clerk of Courts shall copy or make note of the cards submitted and immediately forward the original fingerprint order cards to the District Attorney of Monroe County for a fingerprint comparison.

(5) The District Attorney shall:

(i) within five (5) days after the filing of Applicant's fingerprints with the Clerk of Courts, submit the fingerprints to the Pennsylvania State Police Central Repository for purposes of conducting a fingerprint comparison with the fingerprints of criminals now or hereafter filed in the Pennsylvania State Police data base.

(ii) review the Applicant's Petition;

(iii) conduct a background check on the Applicant; and

(iv) prepare a report and recommendation to the Court. The report and recommendation must be signed by the District Attorney and shall be filed with the Clerk of Courts.

(6) *Hearing on Petition:*

(i) The District Attorney shall notify Applicant/Attorney when it has completed its investigation, at which time, Applicant/Attorney shall submit to the Court a proposed order for hearing in the form set forth below in subparagraph (9).

(ii) The Court shall schedule a hearing to consider Applicant's Petition, at which time the District Attorney or designee shall appear and report his/her recommendation.

(7) *Notice of Hearing:*

(i) Applicant/Attorney shall ensure that notice of the hearing date is published once a week for two consecutive weeks in the *Monroe Legal Reporter* and in one newspaper of general circulation published in Monroe County, the last advertisement to appear not less than three (3) days prior to the scheduled hearing;

(ii) Applicant/Attorney shall file an Affidavit of Publication, together with proofs of advertising, with the Clerk of Courts.

(8) Failure to comply with any provision of this rule may constitute sufficient grounds for the Court to dismiss the Petition and deny Applicant's request for a private investigator's license.

(9) *Forms:* Order for Hearing

Form—Order for Hearing—Petition for Private Detective and/or Security Guard License

COURT OF COMMON PLEAS OF MONROE COUNTY
FORTY-THIRD JUDICIAL DISTRICT
COMMONWEALTH OF PENNSYLVANIA

IN RE:	:	NO. _____ P.DET. 2 _____
	:	
PETITION OF	:	
	:	

ORDER

AND NOW, this _____ day of _____, 20 _____, upon consideration of the within Petition for [Private Detective or Security Guard] License and upon motion of _____, Attorney for Applicant, a hearing is fixed on the application for the _____ day of _____,

20 _____, at _____ m., in Courtroom No. _____, Monroe County Courthouse, Stroudsburg, Pennsylvania.

Applicant or Applicant's attorney shall publish Notice of the Hearing once a week for two consecutive weeks in the *Monroe Legal Reporter* and in one newspaper of general circulation published in Monroe County, the last advertisement to appear not less than three (3) days prior to the scheduled hearing; and shall file an Affidavit of Publication, together with proofs of advertising, with the Clerk of Courts.

BY THE COURT:

_____
J.

cc: (Applicant/Applicant's Attorney)
District Attorney's Office

Rule 206.8(b)—Petition for Appointment of School Police

(1) *Definitions:*

(i) "Applicant"—means the Board of School Directors of the school district requesting appointment of school police officers.

(ii) "School Police Officers"—includes any person who is hired by the school district for the purpose of enforcing good order in school buildings, on school buses and on school grounds located within the school district; including protecting the students and controlling large crowds at extra curricular student activities and events. (Definition derived from The Public School Code of 1949, as amended, 24 P. S. § 7-778(c).)

(iii) "Solicitor"—legal counsel for the school district.

(iv) "Appointee"—the person or persons to be employed by the Applicant as a school police officer.

(2) *Application for School Police:*

(i) An Applicant or the Solicitor on behalf of Applicant (hereafter "Applicant/Solicitor"), seeking appointment of school police officers pursuant to the Public School Code of 1949, as amended, 24 P. S. § 7-778 (hereafter "The School Code"), shall file an original and one copy of a Petition for Appointment of School Police with the Prothonotary.

(ii) Applicant must comply with all requirements set forth in The School Code and the Petition shall contain the following information:

(a) The name, address, social security number, date of birth, and dates of Act 34 clearance and the FBI investigation clearance for the Appointee(s) to be employed as a school police officer.

(b) The fingerprints of the Appointee(s).

(c) A report issued by the Federal Bureau of Investigation, United States Department of Justice, Investigation Division ("FBI") indicating that the Appointee(s) has no arrest record.

(d) A copy of the Request for Criminal History Record Check issued by the Pennsylvania State Police (PSP) indicating that the Appointee(s) has no arrest record.

(e) A statement by the Applicant representing that Appointee(s) is of good character and repute.

(f) A statement by the Applicant that the Appointee(s) has not resided outside the Commonwealth of Pennsylvania in any other jurisdiction since the FBI and PSP issued the reports verifying that the Appointee(s) does not have a criminal record.

(iii) The Prothonotary shall forward a copy of the Petition to the Court Administrator.

(3) *Hearing on Petition:*

(i) Applicant/Solicitor shall submit to the Court a proposed order for hearing in the form set forth below in subparagraph (F).

(ii) The Court shall schedule a hearing to consider Applicant's Petition, at which time the Solicitor shall appear and report his/her recommendation.

(4) *Notice of Hearing:*

(i) Applicant/Solicitor shall ensure that notice of the hearing date is published once a week for two consecutive weeks in the Monroe Legal Reporter and in one newspaper of general circulation published in Monroe County, the last advertisement to appear not less than three (3) days prior to the scheduled hearing;

(ii) Applicant/Solicitor shall file an Affidavit of Publication, together with proofs of advertising, with the Clerk of Courts.

(5) Failure to comply with any provision of this rule may constitute sufficient grounds for the Court to dismiss the Petition and deny Applicant's request to appoint the Appointee(s) as school police officers.

(6) *Forms:* Order for Hearing

Form—Order for Hearing—Petition for Appointment of School Police Officer

COURT OF COMMON PLEAS OF MONROE COUNTY
FORTY-THIRD JUDICIAL DISTRICT
COMMONWEALTH OF PENNSYLVANIA

IN RE:	: NO. _____ MISC. 2
	:
PETITION FOR APPOINTMENT	:
OF SCHOOL POLICE OFFICER(s)	:
FOR THE {Insert Name of School District}	:

ORDER

AND NOW, this _____ day of _____, 20 _____, upon consideration of the within Petition for Appointment of School Police Officer(s) for the [Name of School District] and upon motion of _____, Solicitor for Applicant, a hearing is fixed on the application for the _____ day of _____, 20 _____, at _____ m., in Courtroom No. _____, Monroe County Courthouse, Stroudsburg, Pennsylvania.

Applicant or Solicitor attorney shall publish Notice of the Hearing once a week for two consecutive weeks in the *Monroe Legal Reporter* and in one newspaper of general circulation published in Monroe County, the last advertisement to appear not less than three (3) days prior to the scheduled hearing; and shall file an Affidavit of Publication, together with proofs of advertising, with the Clerk of Courts.

BY THE COURT:

_____
J.

cc: (Applicant/Solicitor)
District Attorney's Office

By the Court

President Judge

[Pa.B. Doc. No. 05-1708. Filed for public inspection September 16, 2005, 9:00 a.m.]

ADMINISTRATIVE OFFICE OF PENNSYLVANIA COURTS

Notice of Proposed Public Access Policy Concerning Electronic Case Records of the Unified Judicial System

The Administrative Office of Pennsylvania Courts is planning to recommend that the Supreme Court of Pennsylvania adopt this proposed public access policy concerning electronic case records of the Unified Judicial System. At my direction, an ad hoc committee of Administrative of Office of Pennsylvania Courts staff crafted this proposed policy that is being published for public comment.

The proposed policy covers electronic case record information that would be accessible by the public, how public requests for access are to be handled, public access request fees, and other pertinent recommendations. The explanatory Report highlights the Committee's considerations in formulating this proposed policy. I request that interested persons submit suggestions, comments, or objections concerning this proposal to the Committee through

David S. Price
Chair, Public Access Ad Hoc Committee
Administrative Office of Pennsylvania Courts
5035 Ritter Road, Suite 700
Mechanicsburg, PA 17055
Fax: (717) 795-2177
e-mail: publicaccesscomments@pacourts.us

no later than Thursday, November 17th, 2005.

ZYGMONT A. PINES,
Court Administrator of Pennsylvania

Proposed 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. Documents produced from the PACMS, CPCMS, and/or MDJS that concern a single case, except for web docket sheets, do not fall within this definition.

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. "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.

H. "Public Access" means that the public may inspect and obtain electronic case record(s), except as provided by law or as set forth in this policy.

I. "Public Terminal" means a computer terminal that may be located within the courthouse to provide the public with access to electronic case record information.

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 significant subset of electronic case records, as is and without modification or compilation.

K. "Request for Compiled Information From Electronic Case Records" means any request, regardless of the format the information is requested to be received in, for information that is derived from the selection, aggregation, and/or manipulation by the court, office or record custodian of information from more than one individual electronic case record, which is not already available in an existing report.

L. "UJS" means the Unified Judicial System of Pennsylvania.

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

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

1. social security numbers;

2. operator license numbers;

3. victim information;

4. informant information;

5. juror information;

6. a party's street address, except the city, state, and ZIP code may be released;

7. dates of birth, except the year of birth and age may be released;

8. witness information;

9. SID (state identification) numbers;

10. financial institution account numbers and credit card numbers;

11. notes, drafts, and work products related to court administration or any office that is the primary custodian of an electronic case record;

12. arrest and search warrants and supporting affidavits retained by judges, clerks, or other court personnel until execution of the warrant;

13. information sealed or protected pursuant to court order; and

14. information to which access is otherwise restricted by federal law, state law, or state court rule.

B. Notwithstanding subsection A, electronic case records concerning a single case that are accessible at the courthouse via a public terminal may include a party's full date of birth and full address in addition to all other information that is deemed accessible under this policy.

Section 3.10 Requests for Bulk Distribution of Electronic Case Records and Compiled Information from Electronic Case Records

A. A request for bulk distribution of electronic case records and/or compiled information from 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 and/or compiled information from electronic case records not publicly accessible under Section 3.00 of this Policy, may be fulfilled where: the release of the information will not permit the identification of 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) identify what information is sought; and

(c) explain provisions for the secure protection of all data that is considered not accessible to the public.

3. If this type of request is granted, the requestor must sign a declaration that:

(a) the information/data will not be sold or otherwise distributed, directly or indirectly, to third parties except for the stated purposes;

(b) the information/data will not be used, directly or indirectly, to sell a product or service to an individual or the general public, except for the stated purposes; and

(c) no copying or duplication of the information/data provided will occur other than for the stated purposes.

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 multiple 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 ten (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 thirty (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 the Administrative Office of the 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 the Pennsylvania Courts has approved the proposed fee schedule.

Section 6.00 Correcting Data Errors

Any party to a case or his/her attorney seeking to correct a data error or omission in an electronic case record should contact the court or office in which the original record was filed.

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.

EXPLANATORY REPORT

Proposed 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]

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 have caused delays in fulfilling public access requests to case records, resulted in the inadvertent release of non-public information, or impeded 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 York[5] and Vermont[6] 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 Massachusetts[7] and Minnesota[8] 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 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 Proposed 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 "Supervision by Administrative Office—all system and

[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. Except as provided elsewhere in this policy, documents produced from the PACMS, CPCMS, or MDJS concerning a single case, except web docket sheets, are excluded from this definition.

[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] *Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (January 12, 2004).

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 proposed 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]

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 type 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] a transcript of jury voir dire;[27] pleadings and settlement agreements.[28]

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 a significant community therapeutic value as an outlet for community 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

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

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

---

[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).
[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).
[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
[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, 1221 (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.

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 1974[53] 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 Act[55] (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 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, 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 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*.

[52] *United States Department of Justice Freedom of Information Act Reference Guide* (November 2003), available at http://www.usdoj.gov/04foia/referenceguidemay99.htm.
[53] 5 U.S.C. § 552a (2004).
[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 2004).
[56] 56 PA. STAT. ANN. tit. 65, § 66.1 (West 2004).
[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.

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 been 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 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 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

[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.
[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.
[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 28, 2005.
[71] *Id.*
[72] *ID Theft Is No. 1 Fraud Complaint*, CBSNEWS.com, January 22, 2003.

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 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 not released.

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. Documents produced from the PACMS, CPCMS, and/or MDJS that concern a single case, except for web docket sheets, do not fall within this definition.

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. "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.

H. "Public Access" means that the public may inspect and obtain electronic case record(s), except as provided by law or as set forth in this policy.

I. "Public Terminal" means a computer terminal that may be located within the courthouse to provide the public with access to electronic case record information.

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 significant subset of electronic case records, as is and without modification or compilation.

K. "Request for Compiled Information From Electronic Case Records" means any request, regardless of the format the information is requested to be received in, for information that is derived from the selection, aggregation, and/or manipulation by the court, office or record custodian of information from more than one individual electronic case record, which is not already available in an existing report.

L. "UJS" means the Unified Judicial System of Pennsylvania.

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

[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.
[78] ARIZ. SUP. CT. R. 123(b)(6).

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 (PACMS, CPCMS, or MDJS). This definition is derived from Minnesota's definition of "case record."[79] Nonetheless, this definition includes paper documents produced from the UJS' automated case management systems in response to requests for compiled information from electronic case records and requests for bulk distribution of electronic case records.

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, Public, is a variation of a provision in the CCJ/COSCA Guidelines.[80] 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."[81] 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."[82] 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.

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."[83] 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,[84] 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."[85] 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 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.

However, 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

[79] *Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (January 12, 2004), p. 4.

[80] 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.

[81] *Id.*

[82] *Id.*

[83] PA. STAT. ANN. tit. 65, § 66.1 (West 2004).

[84] *Id.*

[85] *CCJ/COSCA Guidelines,* p. 11.

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."[86] 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 H, Public Access, is a Committee created term because the Committee was unable to find an existing definition that was deemed adequate.

Subsection I, Public Terminal, is a Committee-created term.

Subsection J, Request for Bulk Distribution of Electronic Case Records, is derived from the CCJ/COSCA Guidelines.[87] 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.[88]

Subsection K, Request for Compiled Information From Electronic Case Records, is loosely derived from the definition that appears in the CCJ/COSCA Guidelines.[89] In addition to other changes, the Committee replaced the word "reformulation" with "manipulation" which it considers to be more encompassing. This definition includes all requests regardless of the format the requestors want to receive the information in (i.e., paper, electronic, etc.). The Committee notes that this term is used by Indiana.[90]

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.

Section 3.00 Electronic Case Record Information Excluded from Public Access

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

1. social security numbers;

2. operator license numbers;

3. victim information;

4. informant information;

5. juror information;

6. a party's street address, except the city, state, and ZIP code may be released;

7. dates of birth, except the year of birth and age may be released;

8. witness information;

9. SID (state identification) numbers;

10. financial institution account numbers and credit card numbers;

11. notes, drafts, and work products related to court administration or any office that is the primary custodian of an electronic case record;

12. arrest and search warrants and supporting affidavits retained by judges, clerks, or other court personnel until execution of the warrant;

13. information sealed or protected pursuant to court order; and

14. information to which access is otherwise restricted by federal law, state law, or state court rule.

B. Notwithstanding subsection A, electronic case records concerning a single case that are accessible at the courthouse via a public terminal may include a party's full date of birth and full address in addition to all other information that is deemed accessible under this policy.

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]

[86] *CCJ/COSCA Guidelines*, p. 10.
[87] *CCJ/COSCA Guidelines*, p. 29.
[88] For example this term is used by Indiana (Proposed Revision of Ind. Admin. R.9(C)(9)), Minnesota (*Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch*, p. 39), California (Cal. CT. R. 2073(f)), and Colorado (Public Access Committee Cost Recovery Formula Concerning the Release of Electronic Data, Section II.C.1.).
[89] *CCJ/COSCA Guidelines*, p. 34.
[90] Proposed Revision of Ind. Adm. R. 9(C)(10).
[91] *CCJ/COSCA Guidelines*, pp. 24-25.
[92] *See* MDJS policy, Section II.B.2.a.
[93] The Committee notes the introduction of Pennsylvania Senate Bill 703 in the 2003 Legislative Session concerning the confidentiality of social security numbers. This bill is identical to Senate Bill 1407 introduced the previous year which would prohibit the posting or public display of such numbers.
[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).

Second, the Freedom of Information Act (FOIA)[95] and the Privacy Act[96] 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 Vermont[101] and Minnesota[102] appear to have used this statute as a basis for formulating a recommendation on 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 (in criminal cases records),[109] Florida,[110] Vermont,[111] Washington (in family court case records),[112] Minnesota,[113] Massachusetts,[114] and Kentucky.[115]

The CCJ/COSCACCJ/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)[116] or to prohibit access altogether under Section 4.60.[117]

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 year 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.[118] 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.

[95] 5 U.S.C. § 552 (2004).
[96] 5 U.S.C. § 552(a) (2004).
[97] 5 U.S.C. § 551 (2004), *see also*, 5 U.S.C. § 552(f) (2004).
[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. 9.
[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) (2004).
[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] *Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (January 12, 2004), p. 15, n.30 (citing the Social Security Act's provision that provides "[f]ederal law imposes the 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(2) which provides in part that "social security numbers shall be excluded from electronic public access except for judiciary employees, the United States Attorney or their representatives and litigants."
[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 provides that social security numbers should be shortened to their last four digits.
[106] Proposed Revision of IND. ADMIN. R. 9(F)(4)(d) provides that when a request for bulk or compiled information include 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] *Recommendations to the Court of Appeals Court Committee Designated to Develop Rules Regarding Public Access to Court Records*, p. 44 which 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 2073.5(c) which provides that "[t]he court should, to the extent feasible, redact the following information from records to which it allows remote access [to]: . . . social security numbers." Please note that this subsection of the rule provides in part that it "does not apply to any document in the original court file, it applies only to documents that are available by remote electronic access." *See also* CAL. CT. R 2077(c)(1).
[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."
[112] WASH. CT. R. 22. In this Rule, a social security number is considered to be a "restricted personal identifier" under section (b)(5). Furthermore, under section (g), restricted personal identifiers are generally not accessible to the public.
[113] *Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (January 12, 2004), pp. 14, 36, and 48. Specifically, proposed 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] *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."
[116] *CCJ/COSCA Guidelines*, p. 40.
[117] *CCJ/COSCA Guidelines*, p. 45.
[118] *See* MDJS policy, Section II.B.2.a.

First, the Driver's Privacy Protection Act[119] (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 obtained by the department in connection with a motor vehicle record.[120] The DPPA defines personal information as "information that identifies an individual, including an individual's photograph, social security number, driver identification number. . . ."[121] 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."[122] 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]."[123] 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 (in criminal case records),[124] Florida,[125] and Washington (in family law case records),[126] 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 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.[127]

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 year 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.[128] 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 . . ."[129]

Additionally, the Committee notes that several states, such as California (in criminal case records),[130] Florida,[131] Indiana,[132] Minnesota,[133] and Massachusetts[134] 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 may result in intimidation or harassment of those individuals who are victims of a

[119] 18 U.S.C. §§ 2721—2725 (2004).
[120] 18 U.S.C. § 2721(a)(1) (2004).
[121] 18 U.S.C. § 2725(3) (2004).
[122] 75 PA. CONS. STAT. § 6114(a)(1) (2004).
[123] 75 PA. CONS. STAT. § 6114(a)(2) (2004).
[124] CAL. CT. R 2073.5(c) which provides "[t]he court should, to the extent feasible, redact the following information from records to which it allows remote access [to]: . . . driver license numbers." Please note that this subsection of the rule provides in part that it "does not apply to any document in the original court file, it applies only to documents that are available by remote electronic access."
[125] 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.
[126] WASH. CT. R. 22. In this Rule, a driver license number is considered to be a "restricted personal identifier" under section (b)(5). Furthermore, under section (g), restricted personal identifiers are generally not accessible to the public.
[127] Robert C. Lind, Natalie B. Eckart, *The Constitutionality of the Driver's Privacy Protection Act*, 17 Communication Lawyer 18 (1999).
[128] *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."
[129] *See CCJ/COSCA Guidelines*, p. 48.
[130] CAL. CT. R. 2073.5(c). The Rule specifically provides that remote electronic access will not be allowed to addresses and phone numbers of victims. Please note that this subsection of the rule provides in part that it "does not apply to any document in the original court file, it applies only to documents that are available by remote electronic access."
[131] 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.
[132] Proposed Revision of IND. ADMIN. R. 9(G)(4)(e). Specifically, the Rule provides that case records excluded from public access include addresses, phone numbers, dates of birth and other information which tends to explicitly identify victims.
[133] *Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (January 12, 2004), p. 36. 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.
[134] *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.

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,[135] Indiana,[136] Minnesota,[137] and Massachusetts[138] 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."[139]

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. In addition, the Committee maintains that releasing information about an informant 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. Thus, 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.

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."[140] In addition, the Committee notes 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."[141]

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 . . . ."[142] Rule 632 also sets forth that "the original and any copies of the juror information questionnaire shall not constitute a public record."[143] 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."[144] 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."[145]

In addition, in the case of *Commonwealth v. Karl Long*,[146] 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)."[147]

Moreover, the Committee notes that several states, such as Vermont,[148] Idaho,[149] Maryland,[150] Arizona,[151] Minnesota,[152] and Utah[153] 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

[135] 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.

[136] Proposed Revision of IND. ADMIN. R 9(F)(4)(e). Specifically, the Rule provides that case records excluded from public access include addresses, phone numbers, dates of birth and other information which tends to explicitly identify a witness.

[137] *Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (January 12, 2004), p. 36. 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.

[138] *Policy Statement by the Justices of the Supreme Judicial Court Concerning Publications of Court Case Information on the Web*, (May 2003), p. 32. The policy provides that the trial court web site should not list any information that is likely to identify witnesses (except for expert witnesses).

[139] *CCJ/COSCA Guidelines*, p. 48.

[140] *Id.*

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

[142] PA.R.CRIM.P. 632(B).

[143] PA.R.CRIM.P. 632(C).

[144] PA.R.CRIM.P. 632(F).

[145] PA.R.CRIM.P. 632(G).

[146] —A2d—, 2005 WL 729656 (March 31, 2005).

[147] *Id.* At p. 7.

[148] 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."

[149] 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."

[150] *Recommendations to the Court of Appeals Court Committee Designated to Develop Rules Regarding Public Access to Court Records*, p. 18. Rule 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."

[151] 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."

[152] *Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (January 12, 2004), p. 36. 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.

[153] UTAH J. ADMIN. R. 4-202.02(4)(d) which provides that the following records are private "records containing the name, address or telephone number of a juror or prospective juror or other information from which a juror or prospective juror could be identified or located."

principles.[154] 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.[155]

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.

Party's Address

The Committee notes that the MDJS policy provides that AOPC will not release the addresses of parties.[156] 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 . . . ."[157]

In addition, several states and the federal courts[158] 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: California (in criminal case records),[159] Indiana,[160] Minnesota,[161] Massachusetts,[162] and Kentucky.[163] In addition, some federal courts have begun releasing only a partial address as well.[164] Furthermore, the Committee notes that in *Sapp Roofing Co. v. Sheet Metal Workers' Int'l*[165] and *Bargeron v. Dep't of Labor and Indus.*,[166] 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 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. However, at the public terminals located at the courthouse, full addresses for parties will be accessible (see Section 3.00(B)). Thus, the Committee recommends the same.

Dates of Birth

The Committee notes that the MDJS policy provides that "the following information will not be released . . . identifiers which would present a risk to personal security or privacy."[167] AOPC considers date of birth an identifier that, if released, would present a risk to an individual's personal security or privacy. Therefore, current practice has been not to release any dates of birth. Upon request, the AOPC has released the age of an individual.

Further, the Committee notes that in *Moak v. Phila. Newspaper, Inc.*,[168] the court held that date of birth information could be released under the RTKA. However, it is unclear based on more recent cases such as *Tribune-Review Publ'g Co. v. Allegheny County Hous. Auth.*[169] and *Times Publ'g Co., Inc. v. Michel*,[170] if the same result would be reached today. In *Moak*, the court analyzed whether date of birth information falls under the personal security exception of the RTKA. The Court held that in order for this information to fall under the personal security exception it must be intrinsically harmful and not merely capable of being used for a harmful purpose.[171] However, in the *Tribune-Review* and *Times* cases, the courts held that the appropriate test is weighing privacy interests of the individual and the extent to which those interests may be invaded *against* the public benefit that would result from disclosure.[172] Therefore, being that the courts in more recent cases are using a different analysis than the *Moak* court, it is unclear as to how much guidance the *Moak* decision provides.

In addition, a review of how other states address this issue reveals that a variety of approaches have been taken. Some states such as New York[173] and Indiana,[174]

[154] http://abanet.org/juryprojectstandards/principles.pdf.
[155] 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.'").
[156] *See* MDJS policy, Section II.B.2.a.
[157] *See CCJ/COSCA Guidelines*, p. 49.
[158] *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.
[159] CAL. CT. R. 2073.5(c). The Rule specifically provides that remote electronic access will not be allowed to addresses of parties. Note that this subsection of the rule provides in part that it "does not apply to any document in the original court file, it applies only to documents that are available by remote electronic access."
[160] Proposed Revision of 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 . . . "
[161] *Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (January 12, 2004), p. 36. Remote access in electronic records to a party's street address will not be allowed.
[162] *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.
[163] *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."
[164] *See also* Local Rules of Practice for the Southern District of California Order 514(1)(e) and (3)(B)(3) 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 redact from all documents filed with the court home addresses. ("If a home address must be included, only the city and state should be listed").
[165] 713 A.2d 627, 630 (Pa. 1998).
[166] 720 A.2d 500, 502 (Pa. Commw. Ct. 1998).
[167] *See* MDJS Policy, Section II.B.2.a.
[168] 336 A.2d 920, 924 (Pa. Commw. Ct. 1975).
[169] 662 A.2d 677 (Pa. Commw. Ct. 1995), *appeal denied*, 686 A.2d 1315 (Pa. 1996).
[170] 633 A.2d 1233 (Pa. Commw. Ct. 1993) *appeal denied*, 645 A.2d 1321 (Pa. 1994).
[171] *Moak*, 336 A.2d at 924.
[172] *Tribune-Review*, 662 A.2d at 682-84; *Times*, 633 A.2d at 1239.
[173] *Report to the Chief Judge of the State of New York* by the Commission on Public Access to Court Records (February, 2004), p. 8.
[174] Proposed Revision of 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 dates of birth will be compiled with by only providing the year of birth. However, Rule 9(G)(1)(e) provides that "[t]he following information in case records is excluded from public access and is confidential . . . dates of birth . . . [of] witnesses or victims in criminal, domestic violence, stalking, sexual assault, juvenile, or civil protection order proceedings . . ."

as well as the Federal Courts,[175] will only release the year of birth rather than an entire date of birth. Other states release the entire date of birth such as Arizona,[176] Florida,[177] and Missouri.[178] However, in California (in criminal case records),[179] Massachusetts,[180] and Kentucky[181] court case information available on the Web does not have any date of birth information.

The Committee was faced with three choices: to release a full date of birth, to release a partial date of birth, or to restrict access to dates of birth. The Committee opines there is a legitimate public interest in releasing a party's date of birth, specifically ensuring that the "right" party is matched with the "right" case information. However, the Committee is concerned that releasing the entire date of birth would cause an unjustified invasion of personal privacy as well as present a risk to personal security.

Therefore, the Committee opines that the release of a partial date of birth (year of birth 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. However, at the public terminals located at the courthouse, full dates of birth will be accessible (see Section 3.00(B)). 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.[182] 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.[183] 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,[184] Florida,[185] Indiana,[186] Minnesota,[187] and Massachusetts.[188]

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 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.

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).[189] Moreover, the MDJS policy provides in part that "[t]he following information will not be released: . . .state fingerprint identification number (SID)."[190]

It appears that California has a similar prohibition. Specifically, California (in criminal cases) will not allow remote electronic access to "National Crime Information numbers" which the Committee suspects are a national counterpart to the SIDs.[191]

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 and Credit Card Numbers

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 infor-

[175] Only year of birth accessible in electronic case records, whether civil and criminal. *See Report of the Judicial Conference Committee on Court Administration and Case Management on Privacy and Public Access to Electronic Case Files*, p. 3 which provides for civil cases "if an individual's date of birth is necessary, only the year should be used . . ." and *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. 28 which provides in criminal cases "date of birth to the year only" shall be redacted. *See also* Local Rules of Practice for the Southern District of California Order 514(1)(c) and Eastern District of Pennsylvania promulgated Local Rule 5.1.3.

[176] *See Report and Recommendations of the Ad Hoc Committee to Study Public Access to Electronic Court Records*, (March 2001) p. 9 which provides that "personal addresses, phones numbers and dates of birth will still be available to distinguish one John Smith from another . . ."

[177] Order of Supreme Court of Florida, No. AOSO04-4 (February 12, 2004), p. 8. Specifically, the Order lists information that shall be accessible to the public. A party's date of birth is listed in the Order; therefore, this information is accessible.

[178] MO. COURT OPERATING RULE 2.04 which provides that "[e]lectronic records that are public and from which a person can be identified will include only the following data elements, if not confidential by statute or rule: Civil cases . . .(f) date of birth . . . Criminal cases . . . (j) date of birth . . . "

[179] CAL. CT. R. 2073.5(c) which provides that there will be no remote electronic access in individual criminal cases to any part of the date of birth. Please note that this subsection of the rule provides in part that it "does not apply to any document in the original court file, it applies only to documents that are available by remote electronic access." In addition, CAL. CT. R. 2077(c)(12) which provides that "the following information must be excluded from a court's electronic calendar, index, and register of actions: . . . date of birth."

[180] *Policy Statement by the Justices of the Supreme Judicial Court Concerning Publications of Court Case Information on the Web*, (May 2003), Subsection (a)(6) p. 3. The policy provides that the trial court web site should not list an individual's date of birth.

[181] *Kentucky Court of Justice Access to Electronic Court Records* (December 2003) provides in part that "we decided to remove the individual's . . . date of birth . . . from public remote access."

[182] *See* MDJS policy, Section II.B.2.a.

[183] *See CCJ/COSCA Guidelines*, p. 48.

[184] CAL. CT. R. 2073.5(c). The Rule specifically provides that remote electronic access will not be allowed to addresses and phone numbers of witnesses. Note that this subsection of the rule provides in part that it "does not apply to any document in the original court file, it applies only to documents that are available by remote electronic access."

[185] 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.

[186] Proposed Revision of IND. ADMIN. R. 9(G)(1)(e). Specifically, the Rule provides that case records excluded from public access include addresses, phone numbers, dates of birth and other information which tends to explicitly identify witnesses.

[187] *Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (January 12, 2004), p. 36. 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.

[188] *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.

[189] 18 PA. CONS. STAT. § 9101 et. seq.

[190] *See* MDJS Policy, Section II.B.2.a.

[191] CAL. CT. R. 2073.5(c) which provides that there will be no remote electronic access in individual criminal cases to any part of the criminal identification and information and National Crime Information numbers. Note that this subsection of the rule provides in part that it "does not apply to any document in the original court file, it applies only to documents that are available by remote electronic access."

mation (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."[192] In addition, the Committee notes that the federal courts[193] and several states, such as Arizona,[194] California,[195] Colorado,[196] Florida,[197] Indiana,[198] Minnesota,[199] New York,[200] and Vermont[201] 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 and credit card information. 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,[202] Idaho,[203] Indiana,[204] Minnesota,[205] Vermont,[206] and Utah[207] 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."[208]

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.[209]

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."[210] 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.[211]

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

[192] *See CCJ/COSCA Guidelines*, p. 48.

[193] *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(1)(e) and (3)(B)(3) and Eastern District of Pennsylvania Local Rule of Civil Procedure 5.1.3.

[194] 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).

[195] CAL. CT. R. 2073.5(c). The Rule specifically provides that remote electronic access will not include financial information and account numbers. Note that this subsection of the rule provides in part that it "does not apply to any document in the original court file, it applies only to documents that are available by remote electronic access." In addition, 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: . . . any financial information."

[196] Colorado excludes from release to the public electronic data concerning financial files, except for the financial summary screen. As part of its case management system for criminal, traffic, and civil cases, Colorado includes a financial summary screen which displays a summary of assessed and paid fines, costs, filing fees, etc. . . . *See* COLO. CJD 98-05 III.B. In addition, Colorado permits a court by blanket order to exclude from public view financial affidavits of parties. *See* COLO. CJD 98-05 I.A.2.

[197] 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.

[198] Proposed Revision of 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.

[199] *Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (January 12, 2004), p. 12, 36, & 48. Remote access in electronic records to financial account numbers will not be allowed.

[200] *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.

[201] 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).

[202] PUBLIC ACCESS TO THE JUDICIAL RECORDS OF THE STATE OF ARIZONA, Rule (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."

[203] 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.

[204] Proposed Revision of 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.

[205] *Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (January 12, 2004), Rule 4(1)(c). Case records that are not accessible by the public include "all notes, 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 . . . "

[206] 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.

[207] UTAH J. ADMIN. R. 4-202.02(8)(a)-(c) which provides that "[t]he following judicial records are protected: (A) personal notes or memoranda prepared by a judge or any person charged by law with performing a judicial function and used in the decision-making process; (B) drafts of opinions or orders; (C) memoranda prepared by staff for a member of any body charged by law with performing a judicial function and used in the decision-making process."

[208] *See CCJ/COSCA Guidelines*, p. 48-49.

[209] *See CCJ/COSCA Guidelines*, p. 50.

[210] *See CCJ/COSCA Guidelines*, p. 50.

[211] *See CCJ/COSCA Guidelines*, p. 51. *See also* ARIZ. SUP. CT. R. 123(e) (restricting access to *inter alia* judicial case assignments, pre-decisional documents, and library records); CAL. CT. R. 2072(a) (excluding personal notes or preliminary memoranda of court personnel from definition of court record); FLA. J. ADMIN. R. 2.051(c) (keeping confidential *inter alia* materials prepared as part of the court's judicial decision-making process utilized in disposing of case and controversies unless filed as a part of the court record); *Report to the Chief Judge of the State of New York* by the Commission on Public Access to Court Records (February 2004), p. 1, ftnt. 1 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; 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.").

interest in releasing this type of information. Therefore, the Committee asserts that the same should not be released.

Arrest and Search Warrants and Supporting Affidavits Retained by Judges, Clerks, or other Court Personnel Until Execution of the Warrant

The Committee notes that the federal courts[212] and several states including: California,[213] Florida,[214] Idaho,[215] Indiana,[216] Maryland,[217] and Vermont[218] have a similar provision regarding arrest and search warrants and supporting affidavits retained by judges, clerks, or other court personnel until the execution of the warrant.

The Committee recognizes that there may be a legitimate public interest in releasing this information, specifically for the community to know who is subject to arrest by law enforcement. Nonetheless, the Committee is convinced that to permit the release of search or arrest warrant information prior to the same being executed by law enforcement officers could impede the execution of these warrants as well as endanger law enforcement personnel in performing their duties, thus causing an unjustified invasion of personal privacy as well as presenting a risk to personal security. Therefore, the Committee opines that this information should not be released until the warrant is executed.

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 the proposed policies of New York[219] and Maryland[220] have a similar prohibition.

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.[221]

Access to Electronic Case Records at a Public Terminal

The Committee asserts that those individuals who travel to the courthouse to review electronic case records on a public terminal should be permitted to see additional information that is not available remotely. This additional information consists of a party's full date of birth and full address. Being that these two pieces of information are accessible in the paper case records to which access is unrestricted under this policy, the Committee is satisfied that providing this additional information to the public terminal users will not greatly increase the risk of harm to individuals. Specifically, these two pieces of information will still be afforded some of the protection afforded by the notion of "practical obscurity" by requiring a requestor to travel to the courthouse to view case records individually. In addition, AOPC has learned through the implementation of the CPCMS in the initial twenty counties that providing this information to public terminal users would greatly assist public access requestors in distinguishing one John Doe from another. In addition, if public access requestors are able to gain all the information they need via the public terminal, there should be less requests made to court staff to review the paper files, thus presumably conserving scarce court resources.

Section 3.10 Requests for Bulk Distribution of Electronic Case Records and Compiled

Information from Electronic Case Records

A. A request for bulk distribution of electronic case records and/or compiled information from electronic case records shall be permitted for data that is not excluded from access as set forth in this Policy.

B. A request for bulk distribution of electronic case records and/or compiled information from electronic case records not publicly accessible under Section 3.00 of this Policy, may be fulfilled where: the release of the information will not permit the identification of 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) identify what information is sought; and

(c) explain provisions for the secure protection of all data that is considered not accessible to the public.

3. If this type of request is granted, the requestor must sign a declaration that:

(a) the information/data will not be sold or otherwise distributed, directly or indirectly, to third parties except for the stated purposes;

(b) the information/data will not be used, directly or indirectly, to sell a product or service to an individual or the general public, except for the stated purposes; and

---

[212] *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. 28. The pilot program in the eleven federal courts to provide public access to criminal case files electronically requires that courts should not provide remote public access to unexecuted warrants of any kind (e.g., search warrants, arrest warrants).

[213] CAL. CT. R. 2077(c)(2) and (3) which provides that "the following information must be excluded from a court's electronic calendar, index, and register of actions: . . . arrest warrant information [and] search warrant information."

[214] FLA. J. ADMIN. R. 2.051(c)(6). This Rule provides that "copies of arrest and search warrants and supporting affidavits retained by judges, clerks or other court personnel until execution of said warrant or until a determination is made by law enforcement authorities that execution cannot be made" shall not be released.

[215] IDAHO ADMIN. R. 32(d)(3) & (4). This Rule provides that "unreturned search warrants, arrest warrants or summonses in a criminal case" and "affidavits or sworn testimony and records of proceedings in support of the issuance of search or arrest warrant pending the return of the warrant" are not releasable to the public.

[216] Proposed Revision of IND. ADMIN. R. 9(G)(1)(b)(x). Specifically, the Rule provides that case records excluded from public access include those arrest warrants and search warrants ordered confidential by the judge, prior to the return of duly executed service.

[217] *Recommendations to the Court of Appeals Court Committee Designated to Develop Rules Regarding Public Access to Court Records* Rule 16-1006(5)(b) and (C). This rule provides that access shall be denied to the following case records: "court records pertaining to search warrants: the warrant, application, and supporting affidavit, prior to execution of the warrant and the filing of the records with the clerk [and] executed search warrants and all papers attached thereto filed pursuant to MD. R. 4-601." Moreover, "the following court records pertaining to an arrest warrant: a court record pertaining to an arrest warrant issued under MD. R. 4-212(d) and the charging document upon which the warrant was issued until the conditions set forth in MD. R. 4-212(d)(3) are satisfied [and except as otherwise provided by law] a court record pertaining to an arrest warrant issued pursuant to a grand jury indictment or conspiracy investigation and the charging document upon which the arrest warrant was issued."

[218] VERMONT RULES FOR PUBLIC ACCESS TO COURT RECORDS RULE 6(b)(15) & (16). These Rules provide "the public shall not have access to the following judicial branch records: . . . (15) Records of the issuance of a search warrant, until the date of the return of the warrant, unless sealed by order of the court; (16) Records of the denial of a search warrant by a judicial officer, unless opened by order of the court."

[219] *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."

[220] *Recommendations to the Court of Appeals Court Committee Designated to Develop Rules Regarding Public Access to Court Records*, p. 41-42, Rule 16-1006(1)(10) which provides that "the custodian shall deny inspection of . . . a case record that: a court has ordered sealed or not subject to inspection. . . . "

[221] *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).

(c) no copying or duplication of the information/data provided will occur other than for the stated purposes.

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 and compiled information from 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 and compiled information from court records.[222] In addition, the Committee notes that several states, including California,[223] Colorado,[224] Indiana,[225] and Minnesota[226] permit the release of bulk and/or compiled 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."[227] Therefore, the Committee recommends that requests for bulk distribution of electronic case records and compiled information from electronic case records continue to be fulfilled.

With regard to both types of requests, the Court's automated systems (PACMS, CPCMS, and MDJS) provide system users with various "canned" reports which a user can produce for requestors in response to a request. However, if a request cannot be fulfilled with one of these "canned" reports, the requestor should be referred to AOPC.

Upon referral to the AOPC, it will be determined whether the request involves a bulk distribution of electronic case records or compiled information from electronic case records.

Bulk Distribution of Electronic Case Records

A request for bulk distribution of electronic case records is defined as a request for all, or a significant subset, of electronic case records, as is and without modification or compilation. Bulk distribution of electronic case record information shall be permitted for data that are publicly accessible as specified in the policy (e.g., year 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 release of the information will not permit the identification of 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, date of birth, 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 provided would not enable the requestor to establish the identity of 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 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;

—identify what information is sought; and

—explain provisions for the secure protection of any data that is considered not accessible to the public.

Further, if the request for non-releasable information is granted, the requestor must sign a declaration that:

—the information/data will not be sold or otherwise distributed, directly or indirectly, to third parties except for the stated purposes;

—the information/data will not be used, directly or indirectly, to sell a product or service to an individual or the general public, except for the stated purposes; and

—no copying or duplication of the information or data provided will occur other than 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.[228] Information distributed may include data that, when coupled with other data, could specifically identify an individual. Requests for data that could be used for this purpose may be denied.

Compiled Information from Electronic Case Records

A request for compiled information from electronic case records is defined as a request for information that is derived from the selection, aggregation, and/or manipulation by the court, office or record custodian of information from more than one individual case record and such information is not already available in an existing report. Generally speaking, compiled information is a set of data that have undergone a specific transformation, using programming or querying techniques, to make it separate and distinct from that of a bulk distribution. Examples of compiled information would include limiting the entire database to a specific charge or section, specific geographic area, and/or specific age or race to limit record selection. Compiled data would also include the compilation of statistics based on case information. Therefore, requests for compiled information from electronic case records should be permitted so long as the information has been previously set forth in this Policy as releasable.

In addition, a request for compiled distribution of information/data not publicly accessible may be permitted where the release of the information will not permit the identification of specific individuals or 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. For further

[222] *See* CCJ/COSCA *Guidelines*, pp. 34, 35, and 39.

[223] *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."

[224] *See* Chief Justice Directive, Order 98-05 Subsection (II)(c)(1), p. 3, which permits the release of bulk data. the court's electronic records."

[225] Proposed Revision of IND. ADMIN. R. 9(F) permits the release of bulk or compiled data.

[226] *Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (January 12, 2004), p. 10 & 36 which provides that "a court administration office shall provide bulk distribution of only its electronic case records that are remotely accessible to the public pursuant [to this policy]. "Bulk distribution" means distribution of all, or a significant subset, of the court's electronic case records."

[227] PA. STAT. ANN. tit. 65, § 66.8(c)(1) (West 2004).

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

explanation of this type of request, please refer to the bulk distribution of electronic case records information section.

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

—the purpose/reason for the request;

—identify what information is sought; and

—explain provisions for the secure protection of any data that is considered not accessible to the public.

Further, if the request for non-releasable information is granted, the requestor must sign a declaration that:

—the information/data will not be sold or otherwise distributed, directly or indirectly, to third parties except for the stated purposes;

—the information/data will not be used, directly or indirectly, to sell a product or service to an individual or the general public, except for the stated purposes; and

—no copying or duplication of the information or data provided will occur other than for the stated purposes.

Requests for compiled information may be denied if the data could be used to identify individuals.

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 multiple 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 multiple judicial districts should be directed to and processed by 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 consistent with a 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.

With regard to the issue of the request for information regarding multiple magisterial district judge courts or multiple 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 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 ten (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 thirty (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 the Administrative Office of the 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.[229]

Under subsection A(4), the court or office shall specifically state in its written notification to the requestor the

[229] 5 U.S.C. § 552(a)(6) (2004) and PA. STAT. ANN. tit. 65, §§ 66.3-3 (West 2004).

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 and/or compiled information from 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 ten (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 ten (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. However, upon the expiration of the additional thirty (30) business day period, the court or office must either fulfill the request or notify the requestor that the request cannot be fulfilled. The court or office may not use the entire thirty day period to merely determine that the information is releasable and then require the requestor to wait an additional period of time to receive the information.

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."

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 the 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."[230] The RTKA also provides that fees may be charged by agencies in fulfilling RTKA requests.[231] The Committee reviewed the RTKA fee schedules of the Governor's Office, Lieutenant Governor's Office, and the Executive Offices[232] and the Department of Environmental Protection.[233] 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 request. These court systems include New York,[234] Vermont,[235] Maryland,[236] Idaho,[237] California,[238] Colorado,[239] and Florida.[240] However, some court systems, such as Minne-

[230] *See* MDJS Policy, Section II.B.5.

[231] *See* PA. STAT. ANN. tit. 65, § 66.7 (West 2004).

[232] *See Commonwealth of Pennsylvania Governor's Office, Lieutenant Governor's Office, and Executive Offices—Right-To-Know Request Policy.*

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

[234] *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."

[235] 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.

[236] *Recommendations to the Court of Appeals Court Committee Designated to Develop Rules Regarding Public Access to Court Records*, p. 11 which provides the following. "(1) 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. (2) A custodian may charge a reasonable fee if two hours or more of effort is required to provide the requested access. (3) The custodian may charge a reasonable fee for making or supervising the making of a copy or printout of a court record." The Report further provides on p. 15 that "*. . .* a court may charge a reasonable fee for access to the record in *order to recover its costs*." [emphasis added].

[237] IDAHO ADMIN. R. 32(m). 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.

[238] 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).

[239] *Public Access Committee Cost Recovery Formula Concerning the Release of Electronic Data*. In reviewing this documentation, the Committee is of the opinion that Colorado is merely attempting to recover its costs in providing the information.

[240] *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.

sota,[241] Arizona,[242] and Utah[243] 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.[244] However, FOIA provides that only the direct costs incurred by the agency can be charged to the requestor. [245]

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 Vermont[246] and New York[247] 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.[248]

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.[249] 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 the avoidance of 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.

Section 6.00 Correcting Data Errors

Any party to a case or his/her attorney seeking to correct a data error or omission in an electronic case record should contact the court or office in which the original record was filed.

Commentary

Electronic case records are as susceptible to errors and omissions as any other public record. If a party to a case or his/her attorney believes that an electronic case record contains information that is inaccurate, he/she should contact the court or office in which the record originated to amend the same. For example, if the electronic case record originated in the court of common pleas, the court of common pleas should be contacted. The Committee notes that other states, including Arizona[250] and Minnesota[251] cover this subject matter in their policies and/or court rules (enacted or proposed).

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.[252] 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).

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, dates of birth, 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 Wash-

[241] *Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (January 12, 2004), p. 36. "When copies are requested, the custodian may charge the copy fee established pursuant to 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."

[242] 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).

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

[244] *See* PA. STAT. ANN. tit. 65, § 66.7 (West 2004).

[245] 5 U.S.C. § 552(a)(4)(a)(iv) (2004). In addition, the Committee noted that 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) (2004).

[246] 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.

[247] *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."

[248] *See* PA.R.J.A.103(c), PA. R. CRIM. P. 105(c) and PA. R. C. P. No. 239(c).

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

[250] *Report and Recommendation of the Ad Hoc Committee to Study Public Access to Electronic Records* dated March 2001 Sections (V)(8) and (VI)(8).

[251] *Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (January 12, 2004), p. 11 & 33.

[252] 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.

ington[253] already uses a sensitive information data form, and Arizona[254] and Minnesota[255] 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.

[Pa.B. Doc. No. 05-1709. Filed for public inspection September 16, 2005, 9:00 a.m.]

[253] RULES OF GENERAL APPLICATION 22(c)(2). Please note that this rule only applies to family law cases.

[254] Proposed Amendment to ARIZ. SUP. CT. R. 123 Relating to the use of a sensitive data form.

[255] *Preliminary Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (January 12, 2004), p. 48.