THE COURTS

Title 204—JUDICIAL SYSTEM GENERAL PROVISIONS

PART V. PROFESSIONAL ETHICS AND CONDUCT

[204 PA. CODE CH. 81]

Amendment of Rules 1.1 and 1.6 of the Pennsylvania Rules of Professional Conduct; No. 157 Disciplinary Rules Doc.

Order

Per Curiam

And Now, this 23rd day of April, 2018, upon the recommendation of the Disciplinary Board of the Supreme Court of Pennsylvania; the proposal having been published for public comment in the *Pennsylvania Bulletin*, 47 Pa.B. 5926 (September 23, 2017):

It Is Ordered pursuant to Article V, Section 10 of the Constitution of Pennsylvania that Rules 1.1 and 1.6 of the Pennsylvania Rules of Professional Conduct are amended as set forth in Annex A.

This *Order* shall be processed in accordance with Pa.R.J.A. No. 103(b), and shall be effective July 1, 2018.

Annex A

TITLE 204. JUDICIAL SYSTEM GENERAL PROVISIONS

PART V. PROFESSIONAL ETHICS AND CONDUCT

Subpart A. PROFESSIONAL RESPONSIBILITY

CHAPTER 81. RULES OF PROFESSIONAL CONDUCT

Subchapter A. RULES OF PROFESSIONAL CONDUCT

§ 81.4. Rules of Professional Conduct.

The following are the Rules of Professional Conduct:

CLIENT-LAWYER RELATIONSHIP

Rule 1.1. Competence.

* * * * *

Comment:

* * * * *

Maintaining Competence

(8) To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. **To provide competent representation, a lawyer should be familiar with policies of the courts in which the lawyer practices, which include the Case Records Public Access Policy of the Unified Judicial System of Pennsylvania.**

Rule 1.6. Confidentiality of Information.

* * * * *

Comment:

* * * * *

Acting Competently to Preserve Confidentiality

(25) **Pursuant to paragraph (d), a lawyer should act in accordance with court policies governing disclosure of sensitive or confidential information, including the Case Records Public Access Policy of the Unified Judicial System of Pennsylvania.** Paragraph (d) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (d) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments (3)-(4).

* * * * *

[Pa.B. Doc. No. 18-673. Filed for public inspection May 4, 2018, 9:00 a.m.]

Title 204—JUDICIAL SYSTEM GENERAL PROVISIONS

PART VII. ADMINISTRATIVE OFFICE OF PENNSYLVANIA COURTS

[204 PA. CODE CH. 213]

Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania

In accordance with the Judicial Code, 42 Pa.C.S. § 4301(b), the following amendment to the Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania has been approved by the Supreme Court. The amendment shall be effective immediately in the interest of justice. The changes to the policy are shown in bold and underline; deletions are shown in bold and brackets.

The entire policy, including this amendment and other related information, can be found on the Unified Judicial System's public records webpage located at http://www.pacourts.us.

Filed in the Administrative Office of Pennsylvania Courts on April 19, 2018.

THOMAS B. DARR,
Court Administrator of Pennsylvania

Annex A

TITLE 204. JUDICIAL SYSTEM GENERAL PROVISIONS

PART VII. ADMINISTRATIVE OFFICE OF PENNSYLVANIA COURTS

CHAPTER 213. COURT RECORDS POLICIES

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

§ 213.73. Electronic Case Record Information Excluded from Public Access.

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

* * * * *

(12) information to which access is otherwise restricted by federal law, state law, or state court rule; **[and]**

(13) information presenting a risk to personal security, personal privacy, or the fair, impartial and orderly administration of justice, as determined by the Court Administrator of Pennsylvania with the approval of the Chief Justice**[.]; and**

(14) information regarding arrest warrants and supporting affidavits until execution.

EXPLANATORY REPORT

Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania

Introduction

With the statewide implementation of the Common Pleas Criminal Court Case Management System (CPCMS) in process, the Administrative Office of the Pennsylvania Courts (AOPC) faced the complicated task of developing a uniform public access policy to criminal case records for Pennsylvania's Unified Judicial System (UJS). Public access to case records is a subject well known to the AOPC. Specifically, the AOPC has been providing information to the public from the judiciary's Magisterial District Judge Automated System (MDJS) pursuant to a public access policy covering MDJS records since 1994.[1] For over a decade now, the AOPC has endeavored to provide accurate and timely MDJS information to requestors without fail.

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

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

Administrative Scope of the Public Access Policy Governing Case Records

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

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

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

At the heart of this issue is the question of whether access to paper records and electronic records should be the same. The Committee researched how other state court systems are addressing this issue. It appears that two distinct schools of thought have emerged. One school (represented by the New 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 Massa-

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

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

[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).

chusetts[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 Public Access Policy Governing Electronic Case Records

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

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

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

Common Law Right to Access

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

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

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

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

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

[7] *Policy Statement by the Justices of the Supreme Judicial Court Concerning Publications of Court Case Information on the Web* (May 2003).
[8] MN ST ACCESS TO REC RULE 1-11 (WEST 2006).

[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).

Federal Constitutional Right to Access

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

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

(1) promotion of informed discussion of governmental affairs by providing the public with a more complete understanding of the judicial system;

(2) promotion of the public perception of fairness which can be achieved only by permitting full public view of the proceedings;

(3) providing significant therapeutic value to a community as an outlet for concern, hostility, and emotion;

(4) serving as a check on corrupt practices by exposing the judicial process to public scrutiny;

(5) enhancement of the performance of all involved; and

(6) discouragement of perjury.[32]

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

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

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

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

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

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

[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 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).

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."

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*

[45] *Commonwealth v. Harris*, 703 A.2d 441, 445 (Pa. 1997), *citing Commonwealth v. Berrigan*, 501 A.2d 226 (Pa. 1985).
[46] *Commonwealth v. Conde*, 822 A.2d 45, 49 (Pa. Super. Ct. 2003), *citing Commonwealth v. Knight*, 364 A.2d 902, 906-07 (Pa. 1976).
[47] *Id.*, *citing Knight*, 364 A.2d at 906-07.
[48] *Commonwealth v. French*, 611 A.2d 175, 180 n.12 (Pa. 1992).
[49] *R.W. v. Hampe*, 626 A.2d 1218, 1220 (Pa. Super. Ct. 1993), *citing Hutchinson v. Luddy*, 581 A.2d 578, 582 (Pa. Super. Ct. 1990) (citing *Publicker Industries, Inc. v. Cohen*, 733 F.2d 1059, 1070 (3d Cir. 1983)).
[50] *Commonwealth v. Murray*, 502 A.2d 624, 629 (Pa.Super. Ct. 1985) *appeal denied*, 523 A.2d 1131 (Pa. 1987).
[51] *French*, 611 A.2d at 180 n.12.
[52] *United States Department of Justice Freedom of Information Act Reference Guide* (May 2006), available at http://www.usdoj.gov/04foia/referenceguidemay99.htm.
[53] 5 U.S.C. § 552a (2006).
[54] United States House of Representatives *A Citizen's Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records* (First Report 2003).
[55] PA. STAT. ANN. tit. 65, §§ 66.1—66.9 (West 2006).
[56] PA. STAT. ANN. tit. 65, § 66.1 (West 2006).
[57] *Id.*

Federal Courts), the U.S. District Court for the Eastern District of Pennsylvania and the Southern District of California, Alaska, Arizona, California, Colorado, Florida, Georgia, Indiana, Idaho, Kansas, Kentucky, Maryland, Massachusetts, Minnesota, Missouri, New York, North Carolina, Washington, Utah, and Vermont.

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

As it wrestled with and attempted to appropriately balance the thorny issues and significant challenges associated with the development and implementation of a statewide access policy, the Committee was grateful for the insight and thought-provoking discussions these policies engendered.

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

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

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

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

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

The Values of Transparency

The values of transparency can 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

[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.

[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).

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 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 prohibited from release.

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

Section 1.00 Definitions

A. "CPCMS" means the Common Pleas Criminal Court Case Management System.

B. "Custodian" is the person, or designee, responsible for the safekeeping of electronic case records held by any court or office and for processing public requests for access to case records.

C. "Electronic Case Record" means information or data created, collected, received, produced or maintained by a court or office in connection with a particular case that exists in the PACMS, CPCMS, or MDJS and that appears on web docket sheets or is provided in response to bulk distribution requests, regardless of format. This definition does not include images of documents filed with, received, produced or maintained by a court or office which are stored in PACMS, CPCMS or MDJS and any other automated system maintained by the Administrative Office of Pennsylvania Courts.

D. "MDJS" means the Magisterial District Judge Automated System.

E. "Office" is any entity that is using one of the following automated systems: Pennsylvania Appellate Court Case Management System (PACMS); Common Pleas Criminal Court Case Management System (CPCMS); or Magisterial District Judge Automated System (MDJS)."

F. "PACMS" means the Pennsylvania Appellate Court Case Management System.

G. "Party" means one by or against whom a civil or criminal action is brought.

H. "Public" includes any person, business, non-profit entity, organization or association.

"Public" does not include:

1. Unified Judicial System officials or employees, including employees of the office of the clerk of courts, prothonotary, and any other office performing similar functions;

[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 26, 2005.
[71] *Id.*
[72] *ID Theft Is No. 1 Fraud Complaint*, CBSNEWS.com, January 22, 2003.
[73] Jim Smith, *Regional Task Force to Tackle ID-Theft Crimes*, phillynews.com, November 13, 2002.
[74] John Waggoner, *Id theft scam spreads across USA,* USATODAY.com, February 22, 2005; *LexisNexis Id theft much worse than thought,* MSNBC.com, April 12, 2005.
[75] *Thief steals UC-Berkeley laptop,* CNN.com, March 31, 2005.
[76] Hiawatha Bray, *BC warns its alumni of possible Id theft after computer is hacked,* Boston Globe, March 17, 2005.
[77] Jonathon Krim, *States Scramble to Protect Data,* Washington Post, April 9, 2005.

2. people or entities, private or governmental, who assist the Unified Judicial System or related offices in providing court services; and

3. any federal, state, or local governmental agency or an employee or official of such an agency when acting in his/her official capacity.

I. "Public Access" means that the public may inspect and obtain electronic case records, except as provided by law or as set forth in this policy.

J. "Request for Bulk Distribution of Electronic Case Records" means any request, regardless of the format the information is requested to be received in, for all or a subset of electronic case records.

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

L. "Web Docket Sheets" are internet available representations of data that have been entered into a Unified Judicial System supported case management system for the purpose of recording filings, subsequent actions and events on a court case, and miscellaneous docketed items.

2013 Commentary

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

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

2007 Commentary

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

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

Subsection C, Electronic Case Record, the Committee opines it is necessary to set forth a term for those records that exist within one of the UJS' automated case management systems (PACMS, CPCMS, or MDJS). This definition is derived from Minnesota's definition of "case record."[79] Nonetheless, this definition includes responses to requests for bulk distribution of electronic case records as well as web docket sheets as defined in this policy. However, paper documents concerning a single case produced from the PACMS, CPCMS, or MDJS are not included in this definition except as otherwise provided for in this definition.

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

Subsection G, Party, is a Committee-created term. The Committee wanted to clarify who a party to an action is. This definition is a combination of the definition for party set forth in 42 Pa.C.S. § 102[80] and Seventh Edition of Black's Law Dictionary.[81]

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

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

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

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

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

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

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

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

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

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

[83] *Id.*

[84] *Id.*

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

that the intent of the RTKA is for it to be only applicable to public (non-governmental) requestors.

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

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

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

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

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

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

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

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

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

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

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

A. social security numbers;

B. operator license numbers;

C. victim information including name, address and other contact information;

D. informant information including name, address and other contact information;

E. juror information including name, address and other contact information;

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

G. witness information including name, address and other contact information;

[86] *Id.*
[87] *CCJ/COSCA Guidelines*, p. 11.
[88] *CCJ/COSCA Guidelines*, p. 10.
[89] *CCJ/COSCA Guidelines*, p. 29.
[90] For example this term is used by Indiana (Ind. Admin. R.9(C)(9)), Minnesota *(Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (June 28, 2004), p. 15; MN ST ACCESS TO REC RULE 8(3) (WEST 2006).), and California (Cal. CT. R. 2073(f)).
[91] *CCJ/COSCA Guidelines*, pp. 24-25.

H. SID (state identification) numbers;

I. financial institution account numbers, credit card numbers, PINS or passwords used to secure accounts;

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

K. information sealed or protected pursuant to court order;

L. information to which access is otherwise restricted by federal law, state law, or state court rule; **[and]**

M. information presenting a risk to personal security, personal privacy, or the fair, impartial and orderly administration of justice, as determined by the Court Administrator of Pennsylvania with the approval of the Chief Justice**[.]; and**

N. information regarding arrest warrants and supporting affidavits until execution.

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

2018 Commentary

Information Regarding Arrest Warrants and Supporting Affidavits Until Execution

The federal courts[92] and several states, including California,[93] Florida,[94] Idaho,[95] Indiana,[96] and Maryland,[97] have a similar provision restricting public access to arrest warrants and supporting affidavits until execution.

While 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, advance warning to defendants about the impending service of an arrest warrant puts the safety of law enforcement personnel at risk, jeopardizes the judicial process, and likely increases the risk of flight by defendants. Therefore, this information shall not be released until the warrant is executed.

2007 Commentary

Social Security Numbers

At the outset, the Committee noted that the MDJS Policy provides that the AOPC will not release social security numbers.[98] 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.[99] 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.[100]

Second, the Freedom of Information Act (FOIA)[101] and the Privacy Act[102] apply only to records of "each authority of the Government of the United States,"[103] and they do not apply to state case records.[104] 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,[105] 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."[106] Although, it is unclear as to whether this law is applicable to state courts, some courts such as Vermont[107] and Minnesota[108] 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.[109] 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,

[92] The Judicial Conference of the United States approved the Judicial Conference Policy on Privacy and Public Access to Electronic Case Files (March 2008) that provides unexecuted summons or warrants of any kind (e.g. arrest warrants) shall not be included in the public case file, or be made available to the public at the courthouse or via remote electronic access.

[93] Cal. Rules of Court, Rule 2.507(c)(3). This Rule provides that "[t]he following information must be excluded from a court's electronic calendar, index, and register of actions:. . .[a]rrest warrant information."

[94] Fla. R. Jud. Admin. 2.420(c)(6). This Rule provides that "[c]opies of arrest. . .warrants and supporting affidavits retained by judges, clerks or other court personnel [shall be confidential] until execution of said warrants or until a determination is made by law enforcement authorities that execution cannot be made."

[95] IDAHO ADMIN. R. 32(g)(3) & (5). This Rule exempts from disclosure "[a]ffidavits or sworn testimony and records of proceedings in support of the issuance of. . .arrest warrant pending the return of the warrant" as well as "[u]nreturned arrest warrants, except bench warrants, or summonses in a criminal case, provided that the arrest warrants or summonses may be disclosed by law enforcement agencies at their discretion."

[96] IND. ADMIN. R. 9(G)(2)(j)(i) and (ii). Specifically, the Rule provides that case records excluded from public access include those arrest warrants ordered confidential by the judge, prior to the arrest of the defendant.

[97] MD R. CTS. J. and ATTYS Rule 16-907(g)(3)(A) and (B) This rule provides that access shall be denied to: "[t]he following case records. . . : A case record pertaining to an arrest warrant [that initiates a case as well as]. . .a case record pertaining to an arrest warrant issued pursuant to a grand jury indictment or conspiracy investigation. . . ."

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

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

[100] *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).

[101] 5 U.S.C. § 552 (2006).

[102] 5 U.S.C. § 552(a) (2006).

[103] 5 U.S.C. § 551 (2006), *see also*, 5 U.S.C. § 552(f) (2006).

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

[105] *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).

[106] 42 U.S.C. § 405(c)(2)(C)(viii) (2006).

[107] *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.

[108] *Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch* (June 28, 2004), p. 37, n.76 (citing the Social Security Act's provision that provides "[f]ederal law imposes the confidentiality of SSN whenever submission of the SSN is 'required' by state or federal law enacted on or after October 1, 1990.")

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

the Judicial Conference set forth that the courts shall only release the last four digits of any social security number.[110]

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,[111] Indiana,[112] and Maryland.[113] 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,[114] California,[115] Florida,[116] Vermont,[117] Washington,[118] Minnesota,[119] Massachusetts,[120] Kansas,[121] and Kentucky.[122]

The CCJ/COSCA Guidelines suggest that the release of social security numbers should be considered on a case by case basis to determine if access should be allowed only at the court facility (whether in electronic or paper form) under Section 4.50(a)[123] or to prohibit access altogether under Section 4.60.[124]

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

Operator License Numbers

The Committee notes that the MDJS policy provides that the AOPC will not release operator license numbers.[125] The Committee found no controlling legal authority that would prohibit a court and/or office from redacting operator license numbers from an electronic case record prior to its release to the public. However, several statutes were of interest to the Committee in analyzing this issue.

First, the Driver's Privacy Protection Act[126] (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.[127] The DPPA defines personal information as "information that identifies an individual, including an individual's photograph, social security number, driver identification number. . . ."[128] 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."[129] 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]."[130] 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,[131] Florida,[132] Vermont,[133] and Washington[134] do not permit the release of operator license numbers.

[110] *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.

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

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

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

[114] 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).

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

[116] 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.

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

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

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

[120] *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.

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

[122] *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."

[123] *CCJ/COSCA Guidelines*, p. 40.

[124] *CCJ/COSCA Guidelines*, p. 45.

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

[126] 18 U.S.C. §§ 2721—2725 (2006).

[127] 18 U.S.C. § 2721(a)(1) (2006).

[128] 18 U.S.C. § 2725(3) (2006).

[129] 75 PA. CONS. STAT. § 6114(a)(1) (2006).

[130] 75 PA. CONS. STAT. § 6114(a)(2) (2006).

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

[132] 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.

[133] VERMONT RULES GOVERNING DISSEMINATION OF ELECTRONIC CASE RECORDS RULE § 3(b).

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

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.[135]

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

Victim Information

The Committee notes that the MDJS policy provides that "names of juvenile victims of abuse" shall not be released.[136] 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. . ."[137]

Additionally, the Committee notes that several states, such as California,[138] Florida,[139] Indiana,[140] Minnesota,[141] Massachusetts,[142] as well as the federal government[143] (concerning victims in protection from abuse cases) have enacted or proposed public access policies or court rules that would prohibit the release of victim information.

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

Informant Information

The Committee asserts that information about an informant should not be released in that doing so could put the informant and/or law enforcement personnel who may be working with an informant at risk of harm, as well as possibly impede ongoing criminal investigations. Although the Committee could not find any court policies or rules that would specifically prohibit the release of informant information, the Committee notes that several states, such as Florida,[144] Minnesota,[145] and Massachusetts[146] 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."[147]

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

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

---

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

[136] *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."

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

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

[139] 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.

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

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

[142] *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.

[143] Title 18 U.S.C.A. § 2265(d)(3) provides that "[a] State. . .shall not make available publicly on the Internet any information regarding the registration or filing of a protection order, restraining order, or injunction in either the issuing or enforcing State. . .if such publication would be likely to publicly reveal the identity or location of the party protected under such order. A State. . .may share court-generated and law enforcement-generated information contained in secure, government registries for protection order enforcement purposes."

[144] 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.

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

[146] *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).

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

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."[148] In addition, the Committee notes that Rule 630 of the Pennsylvania Rules of Criminal Procedure sets forth that "[t]he information provided on the juror qualification form shall be confidential" and further provides that "[t]he original and any copies of the juror qualification form shall not constitute a public record."[149]

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. . . ."[150] Rule 632 also sets forth that "the original and any copies of the juror information questionnaire shall not constitute a public record."[151] 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."[152] 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."[153]

In addition, in the case of *Commonwealth v. Karl Long*,[154] 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)."[155]

Moreover, the Committee notes that several states, such as Vermont,[156] Idaho,[157] Maryland,[158] Arizona,[159] Minnesota,[160] and Utah[161] have enacted or proposed public access policies or court rules that would prohibit the release of some or all juror information.

In February 2005, the American Bar Association's House of Delegates approved a series of model jury principles.[162] 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.[163]

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.[164] 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. . . ."[165]

In addition, several states and the federal courts[166] have enacted or proposed public access policies or court rules that would prohibit the release of a party address or permit the release of only a partial address. Those states include: Indiana,[167] Minnesota,[168] Massachusetts,[169] Kansas[170], Kentucky[171] and Vermont.[172] In addition,

[148] *Id.*
[149] PA.R.CRIM.P. 630(A)(2), (3).
[150] PA.R.CRIM.P. 632(B).
[151] PA.R.CRIM.P. 632(C).
[152] PA.R.CRIM.P. 632(F).
[153] PA.R.CRIM.P. 632(G).
[154] Please note that the Supreme Court has granted a petition for allowance of appeal in this matter. For more information, please see 884 A.2d 248-9 and 39-40 WAP 2005. See also *Jury Service Resource Center v. De Muniz,* —P.3d—, 2006 WL 1101064 (April 27, 2006) (Oregon Supreme Court held that the First Amendment did not require state and county officials to give full access to jury pool records).
[155] *Id.* At p. 7.
[156] 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."
[157] 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."
[158] Maryland Rule of Procedure 16-1004(B)(2) provides that ". . .a custodian shall deny inspection of a court record used by the jury commissioner or clerk in connection with the jury selection process. Except as otherwise provided by court order, a custodian may not deny inspection of a jury list sent to the court pursuant to Maryland Rules 2-512 or 4-312 after the jury has been empanelled and sworn."
[159] 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."
[160] MN ST ACCESS TO REC RULE 8(2)(b) (WEST 2006). Remote access in electronic records to a juror's social security number, street address, telephone number, financial account numbers or information that specifically identifies the individual or from which the identity of the individual could be ascertained will not be allowed.
[161] UTAH J. ADMIN. R. 4-202.02(2)(k) provides that "public court records include but are not limited to: name of a person other than a party, but the name of a juror or prospective juror is private unless released by a judge." Moreover, subsection (4)(i) of the same Rule provides that "the following court records are private; the following personal identifying information about a person other than a party; address, email address, telephone number, date of birth, driver's license number, social security number, account description and number, password, identification number, maiden name and mother's maiden name." Rule 4-202-03 provides who has access to private records which in general appears not to be the public.
[162] http://abanet.org/juryprojectstandards/principles.pdf.
[163] 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.'").
[164] *See* MDJS policy, Section II.B.2.a.
[165] *See CCJ/COSCA Guidelines*, p. 49.
[166] *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.
[167] 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. . . ."
[168] MN ST ACCESS TO REC RULE 8(2)(b)(2) (WEST 2006). Remote access in electronic records to a party's street address will not be allowed.
[169] *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.
[170] Kansas Rules Relating to District Courts Rule 196(d)(3) "[d]ue to privacy concerns, some otherwise public information, as determined by the Supreme Court,

some federal courts have begun releasing only a partial address as well.[173] Furthermore, the Committee notes that in *Sapp Roofing Co. v. Sheet Metal Workers' Int'l*[174] and *Bargeron v. Dep't of Labor and Indus.*,[175] 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. 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.[176] 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.[177] 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,[178] Florida,[179] Indiana,[180] Minnesota,[181] and Massachusetts.[182]

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

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).[183] Moreover, the MDJS policy provides in part that "[t]he following information will not be released:. . .state fingerprint identification number (SID)."[184]

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

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

The Committee maintains when an individual provides the court or office with a financial institution account number (e.g., banking account number) and/or a credit card number that they should not be released to the public because of the financial harm that can result. The CCJ/COSCA Guidelines provide in part that examples of "documents, parts of the court record, or pieces of information (as opposed to the whole case file) for which there may be a sufficient interest to prohibit public access [include f]inancial information that provide identifying account numbers on specific assets, liabilities, accounts, credit cards, or personal identification numbers (PINs) of individuals or business entities."[185] In addition, the Committee notes that the federal courts[186] and several states, such as Arizona,[187] California,[188] Colorado,[189] Florida,[190]

may not be available through electronic access. A nonexhaustive list of information generally not available electronically includes street addresses. . ."

[171] *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."

[172] VERMONT RULES GOVERNING DISSEMINATION OF ELECTRONIC CASE RECORDS RULE § 3(b).

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

[174] 713 A.2d 627, 630 (Pa. 1998).

[175] 720 A.2d 500, 502 (Pa.Commw. Ct. 1998).

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

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

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

[179] 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.

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

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

[182] *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.

[183] 18 PA. CONS. STAT. § 9101 et. seq.

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

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

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

[187] 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).

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

Indiana,[191] Minnesota,[192] New York,[193] and Vermont[194] either prohibit the release of this information entirely or only permit the partial release of this information (i.e., the last four digits).

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

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

The Committee notes that several states including: Arizona,[195] Idaho,[196] Indiana,[197] Minnesota,[198] Vermont,[199] and Utah[200] 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."[201]

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.[202]

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."[203] 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.[204]

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

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

Information Sealed or Protected Pursuant to Court Order

If there is a court order that seals a case record or information contained within that case record, the same shall not be released to the public. The Committee notes that New York[205] has proposed and Maryland[206] has adopted 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.[207]

---

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

[190] 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.

[191] 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.

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

[193] *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.

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

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

[196] 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.

[197] 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.

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

[199] 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.

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

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

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

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

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

[205] *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."

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

[207] *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).

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

The MDJS policy provides that "the following information will not be released:. . .other identifiers which would present a risk to personal security or privacy."[208] Moreover, the RTKA provides that the definition of "public records" does not include "any record. . .which would operate to the prejudice or impairment of a person's reputation or personal security. . . ."[209]

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

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

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

The Committee is cognizant that providing a "catchall" provision such as this could lead to a perception of overreaching, and due consideration was given before offering this recommendation. Notwithstanding, it is believed that such a provision used in judicious fashion is absolutely necessary to the successful implementation of this policy, as has been the case with the MDJS.

Section 3.10 Requests for Bulk Distribution of Electronic Case Records

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

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

1. Requests of this type will be reviewed on a case-by-case basis.

2. In addition to the request form, the requestor shall submit in writing:

(a) the purpose/reason for the request;

(b) identification of the information sought;

(c) explanation of the steps that the requestor will take to ensure that the information provided will be secure and protected;

(d) certification that the information will not be used except for the stated purposes; and

(e) whether IRB approval has been received, if applicable.

2013 Commentary

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

2007 Commentary

In the judgment of the Committee, the number of electronic case records that may be requested by the public should not be limited. AOPC's practice has been to fulfill requests for bulk distribution of electronic MDJS case records regardless of the number of records involved. In addition, the Committee's recommendation and analysis on this issue closely mirrors the CCJ/COSCA Guidelines, which permit the release of bulk distribution of court records.[210] In addition, the Committee notes that several states, including California,[211] Indiana,[212] and Minnesota[213] permit the release of bulk data. Some states such as Kansas[214] and Colorado[215] (in part) do not permit the release of bulk data. Moreover, the RTKA provides that "[a] policy or regulation may not include any of the following: a limitation on the number of public records which may be requested or made available for inspection or duplication."[216] Therefore, the Committee recommends that requests for bulk distribution of electronic case records continue to be fulfilled.

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

A request for bulk distribution of electronic case records is defined as a request for all, or a subset, of electronic case records. Bulk distribution of electronic case record information shall be permitted for data that are publicly

[208] *See* MDJS Policy, Section II.B.2.a.
[209] PA. STAT. ANN. tit. 65, § 66.1 (West 2006).

[210] *See* CCJ/COSCA *Guidelines*, pp. 34, 35, and 39.
[211] *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."
[212] IND. ADMIN. R. 9(F) permits the release of bulk or compiled data.
[213] MN ST ACCESS TO REC RULE 8(3) (WEST 2006).
[214] Kansas Rules Relating to District Courts Rule 196(e) "Bulk and Compiled Information Distribution—Information in bulk or compiled format will not be available."
[215] Colo. CJD. 05-01 provides in Section 4.30 that bulk data will not be released to individuals, government agencies or private entities. Bulk data being the entire database or that subset of the entire database that remains after the extraction of all data that is confidential under law. However, Section 4.40 provides that requests for compiled data for non-confidential data will be entertained. There are numerous criteria that will be used to determine if the request will be granted. Compiled data is defined as data that is derived from the selection, aggregation or reformulation of specific data elements within the database."
[216] PA. STAT. ANN. tit. 65, § 66.8(c)(1) (West 2006).

accessible as specified in the policy (e.g., date of birth, a party's address limited to city, state and ZIP code).

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

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

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

—the purpose/reason for the request;

—identification of the information sought;

—explanation of the steps that the requestor will take to ensure that the information provided will be secure and protected; and

—certification that the information will not be used except for the stated purposes.

This section addresses requests for large volumes of data available from the statewide automation case management systems (PACMS, CPCMS, and MDJS) including incremental data files used to update previously received bulk distributions.[217]

Section 3.20 Requests for Electronic Case Record Information from Another Court or Office

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

Commentary

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

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

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

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

Section 4.00 Responding to a Request for Access to Electronic Case Records

A. Within 10 business days of receipt of a written request for electronic case record access, the respective court or office shall respond in one of the following manners:

1. fulfill the request, or if there are applicable fees and costs that must be paid by the requestor, notify requestor that the information is available upon payment of the same;

2. notify the requestor in writing that the requestor has not complied with the provisions of this policy;

3. notify the requestor in writing that the information cannot be provided; or

4. notify the requestor in writing that the request has been received and the expected date that the information will be available. If the information will not be available within 30 business days, the court or office shall notify the Administrative Office of Pennsylvania Courts and the requestor simultaneously.

B. If the court or office cannot respond to the request as set forth in subsection A, the court or office shall concurrently give written notice of the same to the requestor and Administrative Office of Pennsylvania Courts.

Commentary

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

In drafting this section, the Committee was faced with two competing interests. First, any requirements imposed upon courts and offices regarding how and when they

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

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.[218]

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

—the request, particularly if for bulk distribution of electronic case records, involves such voluminous amounts of information that the court or office may not be able to fulfill the same within the initial 10 business day period without substantially impeding the orderly conduct of the court or office; or

—the court or office is not able to determine if this policy permits the release of the requested information within the initial 10 business day period. Therefore, the court or office may require an additional period of time to conduct an administrative review of the request to make this determination.

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

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

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

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

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

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

Section 5.00 Fees

A. Reasonable fees may be imposed for providing public access to electronic case records pursuant to this policy.

B. A fee schedule shall be in writing and publicly posted.

C. A fee schedule in any judicial district, including any changes thereto, shall not become effective and enforceable until:

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

2. the Administrative Office of Pennsylvania Courts has approved the proposed fee schedule.

Commentary

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

The Committee noted that the MDJS policy provides that "[c]osts shall be assessed based on the actual costs of the report medium, a pro-rata share of computer and staff time, plus shipping and handling."[219] The RTKA also provides that fees may be charged by agencies in fulfilling RTKA requests.[220] The Committee reviewed the RTKA fee schedules of the Governor's Office, Lieutenant Governor's Office, and the Executive Offices[221] and the Department of Environmental Protection.[222] 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 Colorado,[223] New York,[224] Ver-

[218] 5 U.S.C. § 552(a)(6) (2006) and PA. STAT. ANN. tit. 65, §§ 66.3-3 (West 2006).

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

[220] *See* PA. STAT. ANN. tit. 65, § 66.7 (West 2006).

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

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

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

[224] *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

mont,[225] Maryland,[226] Idaho,[227] California,[228] and Florida.[229] However, some court systems, such as Minnesota,[230] Arizona,[231] and Utah[232] 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.[233] However, FOIA provides that only the direct costs incurred by the agency can be charged to the requestor.[234]

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[235] and New York[236] 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.[237]

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.[238] The purpose of this provision is to further a unified approach to fees associated with case record access in the Pennsylvania Judiciary—with an eye toward avoiding inconsistent and unfair charges amongst the various jurisdictions. This type of approach is not novel, as it is quite similar to the procedure set forth in Rule of Judicial Administration 5000.7(f) pertaining to the approval of court transcripts.

Section 6.00 Correcting Data Errors

A. A party to a case, or the party's attorney, seeking to correct a data error in an electronic case record shall submit a written request for correction to the court in which the record was filed.

B. A request to correct an alleged error contained in an electronic case record of the Supreme Court, Superior Court or Commonwealth Court shall be submitted to the prothonotary of the proper appellate court.

C. A request to correct an alleged error contained in an electronic case record of the Court of Common Pleas, Philadelphia Municipal Court or a Magisterial District Court shall be submitted and processed as set forth below.

1. The request shall be made on a form designed and published by the Administrative Office of Pennsylvania Courts.

2. The request shall be submitted to the clerk of courts if the alleged error appears in an electronic case record of the Court of Common Pleas or Philadelphia Municipal Court. The requestor shall also provide copies of the form to all parties to the case, the District Court Administrator and the Administrative Office of Pennsylvania Courts.

3. The request shall be submitted to the Magisterial District Court if the alleged error appears in an electronic case record of the Magisterial District Court. The requestor shall also provide copies of the form to all parties to the case, the District Court Administrator and the Administrative Office of Pennsylvania Courts.

4. The requestor shall set forth on the request form with specificity the information that is alleged to be in error and shall provide sufficient facts including supporting documentation that corroborates the requestor's contention that the information in question is in error.

5. Within 10 business days of receipt of a request, the clerk of courts or Magisterial District Court shall respond in writing to the requestor, all parties to the case, and the Administrative Office of Pennsylvania Courts, in one of the following manners:

a. the request does not contain sufficient information and facts to adequately determine what information is alleged to be error; accordingly, the request form is being returned to the requestor; and no further action will be

advisable we recommend that the charge be nominal and that it in no event should exceed the actual cost to provide such record."

[225] 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.

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

[227] IDAHO ADMIN. R. 32(l). 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.

[228] 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).

[229] *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.

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

[231] 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).

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

[233] *See* PA. STAT. ANN. tit. 65, § 66.7 (West 2006).

[234] 5 U.S.C. § 552(a)(4)(a)(iv) (2006). In addition, the Committee noted that for certain types of requestors FOIA provides that the first two hours of search time or the first 100 pages of duplication can be provided by the agency without charging a fee. 5 U.S.C. § 552(a)(4)(a)(iv)(II) (2006).

[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] *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."

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

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

taken on this matter unless the requestor resubmits the request with additional information and facts.

b. the request does not concern an electronic case record that is covered by this policy; accordingly, the request form is being returned to the requestor; no further action will be taken on this matter.

c. it has been determined that an error does exist in the electronic case record and that the information in question has been corrected.

d. it has been determined that an error does not exist in the electronic case record.

e. the request has been received and an additional period not exceeding 30 business days is necessary to complete the review of this matter.

6. A requestor has the right to seek review of a final decision under subsection 5(a)—(d) rendered by a clerk of courts or a Magisterial District Court within 10 business days of notification of that decision.

a. The request for review shall be submitted to the District Court Administrator on a form that is designed and published by the Administrative Office of Pennsylvania Courts.

b. If the request for review concerns a Magisterial District Court's decision, it shall be reviewed by the judge assigned by the President Judge.

c. If the request for review concerns a clerk of courts' decision, it shall be reviewed by the judge who presided over the case from which the electronic case record alleged to be in error was derived.

Commentary

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

The power of the court to correct errors in its own records is inherent.[239] "Equity enjoys flexibility to correct court errors that would produce unfair results."[240] Therefore, the Committee opines that the authority for a court to correct errors in its own records is inherent and does not arise from the Criminal History Record Information Act (CHRIA).[241] Although, the Committee does not interpret CHRIA as being applicable to the correction of court records,[242] the Committee consulted the correction of error section of CHRIA in drafting this section of the policy,[243] specifically with regard to the safeguards that are found in CHRIA related to the time limitations for action and appeals. CHRIA permits a criminal justice agency 60 days to review a challenge to the accuracy of its record. The Committee believes the time for a decision concerning an alleged error in a court record should be limited in this section of the policy to a maximum of 40 business days. CHRIA also permits the challenger who believes the agency decision is in error to file an appeal. Similarly, in this policy, Subsection 6 permits a requestor who believes the decision is erroneous to seek administrative review as well.

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

The Committee also took note of corrective procedures that other states, including Arizona,[244] Colorado,[245] Kansas,[246] Minnesota,[247] and Wisconsin[248] as well as the CCJ/COSCA Guidelines,[249] establish in their policies and/or court rules (enacted or proposed).

In considering the procedures for correcting errors, it is important to emphasize that this section does not provide a party who is dissatisfied with a court's decision, ruling or judgment a new avenue to appeal the same by merely alleging that there is an error in the court's decision, ruling or judgment. Rather, this section permits a party to "fix" information that appears in an electronic case record which does not, for one reason or another, correctly set forth the facts contained in the official court record (paper case file).

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

By way of example, the official court records of a case set forth that the defendant's name is "John Smith", however, the electronic case record provides that the defendant's name is "John Smyth". Obviously this was a

[239] E.g. *Jackson v. Hendrick*, 746 A.2d 574 (Pa. 2000).
[240] Id. at 577.
[241] 18 Pa.C.S. § 9101—9183.
[242] The Committee notes that it is unclear the extent, if any, to which CHRIA is applicable to court records. Specifically, 18 Pa.C.S. Section 9103 provides that CHRIA is applicable to "person within this Commonwealth and to any agency of the Commonwealth or its political subdivisions which collects, maintains, disseminates or receives criminal history record information." Clearly, the court is not an agency, political subdivision or a person of the Commonwealth. Moreover, Criminal History Record Information is defined in 18 Pa.C.S. Section 9102 as "does not include. . .information and records specified in section 9104 (relating to scope)." 18 Pa.C.S. Section 9014(a)(2) appears to reference "any documents, records, or indices prepared or maintained by or filed in any court of this Commonwealth, including but not limited to the minor judiciary." Moreover, Section 9104(b) provides that "court dockets. . .and information contained therein shall. . .for the purpose of this chapter, be considered public records." If one does contend that the correction procedures set forth in CHRIA are applicable to court records, it is important to note that the procedure provides that a person who wants to appeal a court's decision regarding an alleged error files that appeal with the Attorney General Office. Thus, the Attorney General Office, a part of the Executive Branch of Government, would be reviewing a decision issued by a Court of the Unified Judicial System. Such a procedure appears to raise some constitutional concerns.
[243] See 18 Pa.C.S. § 9152.
[244] *Report and Recommendation of the Ad Hoc Committee to Study Public Access to Electronic Records* dated March 2001 Sections (V)(8) and (VI)(8); ARIZ. SUP. CT. R. 123(g)(6) (this provision, and others related to public access, was adopted by Order of Arizona Supreme Court dated June 6, 2005 to be effective December 1, 2005; effective date postponed by Court's Order dated September 27, 2005 to permit effective and efficient implementation of the provisions).
[245] Colo. CJD. 05-01 Section 9.00 provides for a process to change inaccurate information in a court record.
[246] K.S.A. § 60-260 and Kansas Rules Relating to District Courts Rule 196(f).
[247] MN ST ACCESS TO REC RULE 7(5) (WEST 2006).
[248] Wisconsin Circuit Court Access (WCCA) Web site, "The information on a case is incorrect. Could you correct the information?" at: http://wcca.wicourts.gov/faqnonav.xsl;jsessionid=8036D1470A038AB3CBB55B35613773C6.render4#Faq11 and "Who do I contact if I want clarification about information displayed on WCCA?" at: http://wcca.wicourts.gov/
faqnonav.xsl;jsessionid=8036D1470A038AB3CBB55B35613773C6.render4#Faq18
[249] *See* CCJ/COSCA *Guidelines*, p. 69.

clerical or data entry error. This type of error falls within the purview of this section. However, if for example, a party claims that he was convicted of the crime of simple assault, but the official court record sets forth that he was convicted of the crime of driving under the influence, this error does not fall within the purview of this section in that the requestor is alleging an error in the official court record.

This section does not preclude a court from accepting and responding to verbal or informal requests to correct a data error in an electronic case record. However, if a requestor wishes to enjoy the benefits of the relief and procedures set forth in this section, he/she must file a formal written request. This procedure is consistent with the RTKA which permits a governmental agency to accept and respond to verbal requests, but provides that "[i]n the event that the requestor wishes to pursue the relief and remedies provided for in this act, the requestor must initiate such relief with a written request."[250]

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

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

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

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.[251] 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, financial account numbers, etc) in the filed document. Rather, all sensitive information should be inserted on the sensitive information data form, which would not be accessible to the public. Thus, the use of this form should over time help prevent sensitive information from appearing in the paper records that are accessible to the public. The Committee notes that Washington[252] and Kansas[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. 18-674. Filed for public inspection May 4, 2018, 9:00 a.m.]

[250] 65 P.S. § 66.2(b).

[251] 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.

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

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

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

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

Title 204—JUDICIAL SYSTEM GENERAL PROVISIONS

PART VII. ADMINISTRATIVE OFFICE OF PENNSYLVANIA COURTS

[204 PA. CODE CH. 213]

Order Amending Public Access Policy of the Unified Judicial System of Pennsylvania: Case Records of the Appellate and Trial Courts; No. 496 Judicial Administration Doc.

Amended Order

Per Curiam

And Now, this 28th day of March, 2018, upon the recommendation of the Administrative Office of Pennsylvania Courts to amend the *Public Access Policy of the Unified Judicial System of Pennsylvania: Case Records of the Appellate and Trial Courts* to include all minor courts within the scope of the Policy and achieve one statewide policy for case records in every court:

It Is Ordered that:

1) The Policy is amended to read as follows.

2) The name of the Policy is amended as follows *Case Records Public Access Policy of the Unified Judicial System of Pennsylvania*.

3) The Administrative Office of Pennsylvania Courts shall publish the amended Policy and accompanying Explanatory Report on the Unified Judicial System's website.

4) Every court and custodian's office, as defined by the Policy, shall continuously make available for public in-

spection a copy of the amended Policy in appropriate physical locations as well as on their website.

5) The *Public Access Policy of the Unified Judicial System of Pennsylvania: Official Case Records of the Magisterial District Courts* is hereby rescinded as of July 1, 2018.

6) Whereas prior distribution and publication of this rule would otherwise be required, it has been determined that immediate promulgation is required in the interest of justice and efficient administration. Pa.R.J.A. No. 103(a)(3).

This *Order* shall be processed in accordance with Pa.R.J.A. No. 103(b), and shall be effective July 1, 2018.

Annex A

TITLE 204. JUDICIAL SYSTEM GENERAL PROVISIONS

PART VII. ADMINISTRATIVE OFFICE OF PENNSYLVANIA COURTS

CHAPTER 213. COURT RECORDS POLICIES

Subchapter D. **CASE RECORDS** PUBLIC ACCESS POLICY OF THE UNIFIED JUDICIAL SYSTEM OF PENNSYLVANIA**[: CASE RECORDS OF THE APPELLATE AND TRIAL COURTS]**

§ 213.81. **Case Records** Public Access Policy of the Unified Judicial System of Pennsylvania**[: Case Records of the Appellate and Trial Courts]**.

Section 1.0. Definitions.

A. "Abuse Victim" is a person for whom a protection order has been granted by a court pursuant to Pa.R.C.P. No. 1901 et seq. and 23 Pa.C.S. § 6101 et seq. or Pa.R.C.P. No. 1951 et seq. and 42 Pa.C.S § 62A01 et seq. **as well as Pa.R.C.P.M.D.J. No. 1201 et seq.**

B. "Case Records" are (1) documents for any case filed with, accepted and maintained by a court or custodian; (2) dockets, indices, and documents (such as orders, opinions, judgments, decrees) for any case created and maintained by a court or custodian. This term does not include notes, memoranda, correspondence, drafts**, worksheets,** and work product of judges and court personnel. Unless otherwise provided in this policy, this definition applies equally to case records maintained in paper and electronic formats.

C. "Clerical errors" are errors or omissions appearing in a case record that are patently evident, as a result of court personnel's action or inaction.

D. "Court" includes the Supreme Court, Superior Court, Commonwealth Court, Courts of Common Pleas, **[and]** Philadelphia Municipal Court, **[excluding the Traffic Division of Philadelphia Municipal Court] and Magisterial District Courts**.

E. "Court of Record" includes the Supreme Court, Superior Court, Commonwealth Court, Courts of Common Pleas, and Philadelphia Municipal Court.

[E.] F. "Court Facility" is the location or locations where case records are filed or maintained.

[F.] G. "Custodian" is any person responsible for maintaining case records or for processing public requests for access to case records.

[G.] H. "Docket" is a chronological index of filings, actions, and events in a particular case, which may include identifying information of the parties and counsel, a brief description or summary of the filings, actions, and events, and other case information.

[H.] I. "Financial Account Numbers" include financial institution account numbers, debit and credit card numbers, and methods of authentication used to secure accounts such as personal identification numbers, user names and passwords.

[I.] J. "Financial Source Documents" are:

1. Tax returns and schedules;

2. W-2 forms and schedules including 1099 forms or similar documents;

3. Wage stubs, earning statements, or other similar documents;

4. Credit card statements;

5. Financial institution statements;

6. Check registers;

7. Checks or equivalent; and

8. Loan application documents.

[J.] K. "Medical/psychological records" are records relating to the past, present, or future physical or mental health or condition of an individual.

[K.] L. "Minor" is a person under the age of eighteen.

[L.] M. "Party" is one who commences an action or against whom relief is sought in a matter.

[M.] N. "Public" is any person, member of the media, business, non-profit entity, organization or association. The term does not include a party to a case; the attorney(s) of record in a case; Unified Judicial System officials or employees if acting in their official capacities; or any federal, state, or local government entity, and employees or officials of such an entity if acting in their official capacities.

[N.] O. "Remote Access" is the ability to electronically search, inspect, print or copy information in a case record without visiting the court facility where the case record is maintained or available, or requesting the case record from the court or custodian pursuant to Section 4.0.

Commentary

Regarding Subsection B, "documents for any case filed with, accepted and maintained by a court or custodian" are those not created by a court or custodian, such as pleadings and motions. Indices are tools for identifying specific cases.

Regarding Subsection C, examples of clerical errors are the docket entry links to the wrong document or court personnel misspells a name in the caption.

Regarding Subsection **[F] G**, the definition of "custodian" **includes clerks of court, prothonotaries, clerks of orphans' court and magisterial district judges, for example. The definition** does not include those entities listed in Pa.R.A.P. 3191 who receive copies of briefs filed in an appellate court **or a register of wills**.

Regarding Subsection **[J] K**, this definition is derived from the definition of "health information" provided in 45 C.F.R. § 160.103 (HIPAA). Examples of case records that would fall within this exclusion are: drug and alcohol treatment records, psychological reports in custody matters, and DNA reports.

Regarding Subsection **[L]** **M**, *amici curiae* are not parties. *See* Pa.R.A.P. 531.

Regarding Subsection **[M]** **N**, Unified Judicial System officials or employees include: judicial officers and their personal staff, administrative staff and other central staff, prothonotaries, clerks of the courts, clerks of the orphans' court division, sheriffs, prison and correctional officials, and personnel of all the above.

Section 2.0. Statement of General Policy.

A. This policy shall govern access by the public to case records.

B. Security, possession, custody, and control of case records shall generally be the responsibility of the applicable custodian and designated staff.

C. Facilitating access by the public shall not substantially impede the orderly conduct of court business.

D. A court or custodian may not adopt more restrictive or expansive access protocols than provided for in this policy. Nothing in this policy requires a court or custodian to provide remote access to case records. However, if a court or custodian chooses to provide remote access to any of its case records, access shall be provided in accordance with Section 10.0.

Commentary

[The Supreme Court of Pennsylvania has adopted other policies governing public access to Unified Judicial System case records: the] **The** *Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania* **[that]** provides for access to the statewide case management systems' web docket sheets and requests for bulk data **[and the *Public Access Policy of the Unified Judicial System of Pennsylvania: Official Case Records of the Magisterial District Courts* that provides for access to case records of the magisterial district courts maintained in a paper format]**.

Section 3.0. Access to Case Records.

All case records shall be open to the public in accordance with this policy.

Section 4.0. Requesting Access to Case Records.

A. When desiring to inspect or copy case records, a member of the public shall make an oral **[or written]** request to the applicable custodian, unless otherwise provided by **[court order or rule]** **a local rule or an order issued by a court of record**. **[If the request is oral, the custodian may require a written request.]**

B. When the information that is the subject of the request is complex or voluminous, the custodian may require a written request. If the requestor does not submit a written request when required, access may be delayed until the written request is submitted or a time when an individual designated by the custodian is available to monitor such access to ensure the integrity of the case records is maintained.

[B.] **C.** Requests shall identify or describe the records sought with specificity to enable the custodian to ascertain which records are being requested.

Commentary

Public access requests to the courts and custodians are routinely straightforward and often involve a limited number of records. Therefore, artificial administrative barriers should not be erected so as to inhibit making these requests in an efficient manner.

This policy provides the courts and custodians latitude to establish appropriate administrative protocols for viewing/obtaining case records remotely. However, the definition of "remote access" in Section 1.0 clarifies that a request under this section is neither necessary nor expected under this policy.

Nonetheless, Subsection **[A]** **B** provides a custodian with the flexibility to require that a more complex request be submitted in writing to avoid misunderstandings and errors that can often result in more time being expended to provide the requested information than is necessary. This approach is not novel; submission of a written request form has been a longstanding practice under the Unified Judicial System's *Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania* **[and *Public Access Policy of the Unified Judicial System of Pennsylvania: Official Case Records of the Magisterial District Courts*]**.

Subsection **[B]** **C** does not require a requestor to identify a case by party or case number in order to have access to the files, but the request shall clearly identify or describe the records requested so that court personnel can fulfill the request.

Written requests should be substantially in the format designed and published by the Administrative Office of Pennsylvania Courts.

Section 5.0. Responding to Requests for Access to Case Records.

A. A custodian shall fulfill a request for access to case records as promptly as possible under the circumstances existing at the time of the request.

B. If a custodian cannot fulfill the request promptly or at all, the custodian shall inform the requestor of the specific reason(s) why access to the information is being delayed or denied.

C. If a custodian denies a written request for access, the denial shall be in writing.

D. **[Relief]** **Except as provided in Subsection E, relief** from a custodian's written denial may be sought by filing a motion or application with the court for which the custodian maintains the records.

E. Relief from a magisterial district court may be sought by filing an appeal with the president judge of the judicial district or the president judge's designee. Relief from a written denial by the Philadelphia Municipal Court may be sought by filing a motion with the president judge of Philadelphia Municipal Court or the president judge's designee.

Commentary

Given that most public access requests for case records are straightforward and usually involve a particular case or matter, custodians should process the same in an expeditious fashion.

There are a number of factors that can affect how quickly a custodian may respond to a request. For example, the custodian's response may be slowed if the request is vague, involves retrieval of a large number of case records, or involves information that is stored offsite. Ultimately, the goal is to respond timely to requests for case records.

In those unusual instances in which access to the case records cannot be granted in an expeditious fashion, the custodian shall inform the requestor of the specific reason(s) why access to the information is being delayed or denied, which may include:

• the request involves such voluminous amounts of information that the custodian is unable to fulfill the same without substantially impeding the orderly conduct of the court or custodian's office;

• records in closed cases are located at an off-site facility;

• a particular file is in use by a judge or court staff. If a judge or court staff needs the file for an extended period of time, special procedures should be considered, such as making a duplicate file that is always available for public inspection;

• the requestor failed to pay the appropriate fees, as established pursuant to Section 6.0 of this policy, associated with the request;

• the requested information is restricted from access pursuant to applicable authority, or any combination of factors listed above.

[An] **With respect to Subsection D, an** aggrieved party may seek relief from a denial of a written request for access consistent with applicable authority (for example, in an appellate court, Pa.R.A.P. 123 sets forth procedures for applications for relief under certain circumstances, or pertinent motion practice at the trial court level).

Section 6.0. Fees.

A. Unless otherwise provided by applicable authority, fees for duplication by photocopying or printing from electronic media or microfilm shall not exceed $0.25 per page.

B. **[A]** **Except as provided in Subsection C, a** custodian shall establish a fee schedule that is (1) posted in the court facility in an area accessible to the public, and (2) posted on the custodian's website.

C. Any fee schedule for a magisterial district court shall be established by the president judge of the judicial district by local rule pursuant to Pa.R.J.A. No. 103(c). The fee schedule shall be publicly posted in an area accessible to the public.

Commentary

Reasonable fees may be imposed for providing public access to case records pursuant to this policy and in accordance with applicable authority. This section does not authorize fees for viewing records that are stored at the court facility.

To the extent that the custodian is not the court, approval of the fee schedule by the court may be necessary.

An example of applicable authority setting forth photocopying fees is 42 Pa.C.S. § 1725(c)(1)(ii) that provides the Clerk of Orphans' Court of the First Judicial District shall charge $3 per page for a copy of any record. *See also* 42 P.S. § 21032.1 (providing authority for the establishment of fees in orphans' court in certain judicial districts). In addition, the copying fees for appellate court records are provided for in 204 Pa. Code § 155.1. However, copies of most appellate court opinions and orders are available for free on the Unified Judicial System's website, www.pacourts.us.

Section 7.0. Confidential Information.

A. Unless required by applicable authority or as provided in Subsection C, the following information is confidential and shall be not included in any document filed with a court or custodian, except on a Confidential Information Form filed contemporaneously with the document:

1. Social Security Numbers;

2. Financial Account Numbers, except an active financial account number may be identified by the last four digits when the financial account is the subject of the case and cannot otherwise be identified;

3. Driver License Numbers;

4. State Identification (SID) Numbers;

5. Minors' names and dates of birth except when a minor is charged as a defendant in a criminal matter (see 42 Pa.C.S. § 6355); and

6. Abuse victim's address and other contact information, including employer's name, address and work schedule, in family court actions as defined by Pa.R.C.P. No. 1931(a), except for victim's name.

This section is not applicable to cases that are sealed or exempted from public access pursuant to applicable authority.

B. The Administrative Office of Pennsylvania Courts shall design and publish the Confidential Information Form.

C. Instead of using the Confidential Information Form, a court **of record** may adopt a rule or order permitting the filing of any document in two versions, a "Redacted Version" and "Unredacted Version." The "Redacted Version" shall not include any information set forth in Subsection A, while the "Unredacted Version" shall include the information. Redactions must be made in a manner that is visibly evident to the reader. **This Subsection is not applicable to filings in a magisterial district court.**

D. Parties and their attorneys shall be solely responsible for complying with the provisions of this section and shall certify their compliance to the court. The certification that shall accompany each filing shall be substantially in the following form: "I certify that this filing complies with the provisions of the ***Case Records*** *Public Access Policy of the Unified Judicial System of Pennsylvania* **[** ***: Case Records of the Appellate and Trial Courts*** **]** that require filing confidential information and documents differently than non-confidential information and documents."

E. A court or custodian is not required to review or redact any filed document for compliance with this section. A party's or attorney's failure to comply with this section shall not affect access to case records that are otherwise accessible.

F. If a filed document fails to comply with the requirements of this section, a court **of record** may, upon motion or its own initiative, with or without a hearing order the filed document sealed, redacted, amended or any combination thereof. A court **of record** may impose sanctions, including costs necessary to prepare a compliant document for filing in accordance with applicable authority.

G. If a filed document fails to comply with the requirements of this section, a magisterial district court may, upon request or its own initiative, with

or without a hearing order the filed document redacted, amended or both.

[G.] H. This section shall apply to all documents for any case filed with a court or custodian on or after the effective date of this policy.

Commentary

There is authority requiring information listed in Subsection A to appear on certain documents. For example, Pa.R.C.P. No. 1910.27 provides for inclusion of the plaintiff's and defendant's social security number on a complaint for support.

This section is not applicable to cases that are sealed or exempted from public access pursuant to applicable authority, for example, cases filed under the Juvenile Act that are already protected by 42 Pa.C.S. § 6307, and Pa.Rs.J.C.P. 160 and 1160.

While Pa.R.C.P. No. 1931 is suspended in most judicial districts, the reference to the rule is merely for definitional purposes.

Unless constrained by applicable authority, court personnel and jurists are advised to refrain from inserting confidential information in court-generated case records (e.g., orders, notices) when inclusion of such information is not essential to the resolution of litigation, appropriate to further the establishment of precedent or the development of law, or necessary for administrative purposes. For example, if a court's opinion contains confidential information and, therefore, must be sealed or heavily redacted to avoid release of such information, this could impede the public's access to court records and ability to understand the court's decision.

Whether using a Confidential Information Form or filing a redacted and unredacted version of a document **in a court of record**, the drafter shall indicate where in the document confidential information has been omitted. For example, the drafter could insert minors' initials in the document, while listing full names on the Confidential Information Form. If more than one child has the same initials, a different moniker should be used (e.g., child one, child two, etc.).

[While Pa.R.C.P. No. 1931 is suspended in most judicial districts, the reference to the rule is merely for definitional purposes.]

The option to file a redacted and unredacted version of a document does not apply to filings in a magisterial district court. Most filings in magisterial district courts are completed on statewide forms designed by the Administrative Office of Pennsylvania Courts. Safeguarding the information set forth in this Section for magisterial district courts is achieved through the use of a Confidential Information Form (see Subsection A) in tandem with other administrative protocols (e.g., instituting a public access copy page to the citation form set).

With regard to Subsection D, the certification of compliance is required whether documents are filed in paper form or via an e-filing system. **Moreover, the certification is required on every document filed with a court or custodian regardless of whether the filing contains "confidential information" requiring safeguarding under this policy.**

With regard to Subsection E, a court or custodian is not required to review or redact documents filed by a party or attorney for compliance with this section. However, such activities are not prohibited.

[Any] With regard to Subsection F any party may make a motion to the court **of record** to cure any defect(s) in any filed document that does not comport with this section.

With regard to Subsection G, any party may file a request form designed and published by the Administrative Office of Pennsylvania Courts with a magisterial district court when there is an allegation that a filing was made with that court that does not comply with this policy.

Section 8.0. Confidential Documents.

A. Unless required by applicable authority, the following documents are confidential and shall be filed with a court or custodian under a cover sheet designated "Confidential Document Form":

1. Financial Source Documents;

2. Minors' educational records;

3. Medical/Psychological records;

4. Children and Youth Services' records;

5. Marital Property Inventory and Pre-Trial Statement as provided in Pa.R.C.P. No. 1920.33;

6. Income and Expense Statement as provided in Pa.R.C.P. No. 1910.27(c); and

7. Agreements between the parties as used in 23 Pa.C.S. § 3105.

This section is not applicable to cases that are sealed or exempted from public access pursuant to applicable authority.

B. The Administrative Office of Pennsylvania Courts shall design and publish the Confidential Document Form.

C. Confidential documents submitted with the Confidential Document Form shall not be accessible to the public, except as ordered by a court. However, the Confidential Document Form or a copy of it shall be accessible to the public.

D. Parties and their attorneys shall be solely responsible for complying with the provisions of this section and shall certify their compliance to the court. The certification that shall accompany each filing shall be substantially in the following form "I certify that this filing complies with the provisions of the ***Case Records*** *Public Access Policy of the Unified Judicial System of Pennsylvania* ***[: Case Records of the Appellate and Trial Courts]*** that require filing confidential information and documents differently than non-confidential information and documents."

E. A court or custodian is not required to review any filed document for compliance with this section. A party's or attorney's failure to comply with this section shall not affect access to case records that are otherwise accessible.

F. If confidential documents are not submitted with the Confidential Document Form, a court **of record** may, upon motion or its own initiative, with or without a hearing, order that any such documents be sealed. A court **of record** may also impose appropriate sanctions for failing to comply with this section.

G. If a filed document fails to comply with the requirements of this section, a magisterial district court may, upon request or its own initiative, with or without a hearing order that any such documents be sealed.

[G.] **H.** This section shall apply to all documents for any case filed with a court or custodian on or after the effective date of this policy.

Commentary

This section is not applicable to cases that are sealed or exempted from public access pursuant to applicable authority, such as Juvenile Act cases pursuant to 42 Pa.C.S. § 6307, and Pa.Rs.J.C.P. 160 and 1160.

Unless constrained by applicable authority, court personnel and jurists are advised to refrain from attaching confidential documents to court-generated case records (e.g., orders, notices) when inclusion of such information is not essential to the resolution of litigation, appropriate to further the establishment of precedent or the development of law, or necessary for administrative purposes. For example, if a court's opinion contains confidential information and, therefore, must be sealed or heavily redacted to avoid release of such information, this could impede the public's access to court records and ability to understand the court's decision.

Examples of "agreements between the parties" as used in Subsection (A)(7) include marital settlement agreements, post-nuptial, pre-nuptial, ante-nuptial, marital settlement, and property settlement. See 23 Pa.C.S. § 3105 for more information about agreements between parties.

With regard to Subsection D, the certification of compliance is required whether documents are filed in paper form or via an e-filing system. **Moreover, the certification is required on every document filed with a court or custodian regardless of whether the filing contains a "confidential document" requiring safeguarding under this policy.**

With regard to Subsection E, if the party or party's attorney fails to use a cover sheet designated "Confidential Document Form" when filing a document deemed confidential pursuant to this section, the document may be released to the public.

[Any] **With regard to Subsection F any** party may make a motion to the court **of record** to cure any defect(s) in any filed document that does not comport with this section.

With regard to Subsection G, any party may file a request form designed and published by the Administrative Office of Pennsylvania Courts with a magisterial district court when there is an allegation that a filing was made with that court that does not comply with this policy.

Section 9.0. Limits on Public Access to Case Records at a Court Facility.

The following information shall not be accessible by the public at a court facility:

A. Case records in proceedings under 20 Pa.C.S. § 711(9), including but not limited to case records with regard to issues concerning recordation of birth and birth records, the alteration, amendment, or modification of such birth records, and the right to obtain a certified copy of the same, except for the docket and any court order or opinion;

B. Case records concerning incapacity proceedings filed pursuant to 20 Pa.C.S. §§ 5501—5555, except for the docket and any final decree adjudicating a person as incapacitated;

C. Any Confidential Information Form or any Unredacted Version of any document as set forth in Section 7.0;

D. Any document filed with a Confidential Document Form as set forth in Section 8.0;

E. Information sealed or protected pursuant to court order;

F. Information to which access is otherwise restricted by federal law, state law, or state court rule; and

G. Information presenting a risk to personal security, personal privacy, or the fair, impartial and orderly administration of justice, as determined by the Court Administrator of Pennsylvania with the approval of the Chief Justice. The Court Administrator shall publish notification of such determinations in the *Pennsylvania Bulletin* and on the Unified Judicial System's website.

Commentary

Unless constrained by applicable authority, court personnel and jurists are advised to refrain from inserting confidential information in or attaching confidential documents to court-generated case records (e.g., orders, notices) when inclusion of such information is not essential to the resolution of litigation, appropriate to further the establishment of precedent or the development of law, or necessary for administrative purposes. For example, if a court's opinion contains confidential information and, therefore, must be sealed or heavily redacted to avoid release of such information, this could impede the public's access to court records and ability to understand the court's decision.

With respect to Subsection F, Pennsylvania Rule of Appellate Procedure 104(a), Pa.R.A.P. 104(a), provides that the appellate courts may make and amend rules of court governing their practice. The Administrative Office of Pennsylvania Courts shall from time to time publish a list of applicable authorities that restrict public access to court records or information. This list shall be published on the Unified Judicial System's website and in the *Pennsylvania Bulletin*. In addition, all custodians shall post this list in their respective court facilities in areas accessible to the public and on the custodians' websites.

With respect to Subsection G, the Administrative Office of Pennsylvania Courts shall include any such determinations in the list of applicable authorities referenced above. The same provision appears in **[existing statewide public access policies adopted by the Supreme Court:]** **the** *Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania* **[and *Public Access Policy of the Unified Judicial System of Pennsylvania: Official Case Records of the Magisterial District Courts*]**. The provision is intended to be a safety valve to address a future, extraordinary, unknown issue of statewide importance that might escape timely redress otherwise. It cannot be used by parties or courts in an individual case.

Section 10.0. Limits on Remote Access to Case Records.

A. The following information shall not be remotely accessible by the public:

1. The information set forth in Section 9.0;

2. In criminal cases, information that either specifically identifies or from which the identity of jurors, witnesses (other than expert witnesses), or victims could be ascertained, including names, addresses and phone numbers;

3. Transcripts lodged of record, excepting portions of transcripts when attached to a document filed with the court;

4. *In Forma Pauperis* petitions;

5. Case records in family court actions as defined in Pa.R.C.P. No. 1931(a), except for dockets, court orders and opinions;

6. Case records in actions governed by the Decedents, Estates and Fiduciaries Code, Adult Protective Services Act and the Older Adult Protective Services Act, except for dockets, court orders and opinions; and

7. Original and reproduced records filed in the Supreme Court, Superior Court or Commonwealth Court as set forth in Pa.R.A.P. 1921, 1951, 2151, 2152, and 2156.

B. With respect to Subsections A(5) and A(6), unless otherwise restricted pursuant to applicable authority, dockets available remotely shall contain only the following information:

1. A party's name;

2. The city, state, and ZIP code of a party's address;

3. Counsel of record's name and address;

4. Docket number;

5. Docket entries indicating generally what actions have been taken or are scheduled in a case;

6. Court orders and opinions;

7. Filing date of the case; and

8. Case type.

C. Case records remotely accessible by the public prior to the effective date of this policy shall be exempt from this section.

Commentary

Remote access to the electronic case record information residing in the Pennsylvania Appellate Court Case Management System (PACMS), the Common Pleas Case Management System (CPCMS) and the Magisterial District Judges System (MDJS) is provided via web dockets, available on https://ujsportal.pacourts.us/, and is governed by the *Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania*.

Depending upon individual court resources, some courts have posted online docket information concerning civil matters. If a court elects to post online docket information concerning family court actions and actions governed by the Decedents, Estates and Fiduciaries Code, Adult Protective Services Act and the Older Adult Protective Services Act, the docket may only include the information set forth in Subsection B. This information will provide the public with an overview of the case, its proceedings and other pertinent details, including the court's decision. Release of such information will enhance the public's trust and confidence in the courts by increasing awareness of the procedures utilized to adjudicate the claims before the courts as well as the material relied upon in reaching determinations. This provision does not impact what information is maintained on the docket available at the court facility.

Access to portions of transcripts when attached to a document filed with the court in family court actions is governed by Subsection A(5). While Pa.R.C.P. No. 1931 is suspended in most judicial districts, the reference to the rule is merely for definitional purposes.

Section 11.0. Correcting Clerical Errors in Case Records.

A. A party, or the party's attorney, seeking to correct a clerical error in a case record may submit a written request for correction.

1. A request to correct a clerical error in a case record of the Supreme Court, Superior Court or Commonwealth Court shall be submitted to the prothonotary of the proper appellate court.

2. A request to correct a clerical error in a case record of a court of common pleas **[or], the** Philadelphia Municipal Court**, or a magisterial district court** shall be submitted to the applicable custodian.

B. The request shall be made on a form designed and published by the Administrative Office of Pennsylvania Courts.

C. The requestor shall specifically set forth on the request form the information that is alleged to be a clerical error and shall provide sufficient facts, including supporting documentation, that corroborate the requestor's allegation that the information in question is in error.

D. The requestor shall provide copies of the request to all parties to the case.

E. Within 10 business days of receipt of a request, the custodian shall respond in writing to the requestor and all parties to the case in one of the following manners:

1. The request does not contain sufficient information and facts to determine what information is alleged to be in error, and no further action will be taken on the request.

2. The request does not concern a case record that is covered by this policy, and no further action will be taken on the request.

3. A clerical error does exist in the case record and the information in question has been corrected.

4. A clerical error does not exist in the case record.

5. The request has been received and an additional period not exceeding 30 business days is necessary to complete a review of the request.

F. A requestor may seek review of the custodian's response under Subsections E(1)—(4) within 10 business days of the mailing date of the response.

1. The request for review shall be submitted on a form that is designed and published by the Administrative Office of Pennsylvania Courts.

2. The request shall be reviewed by the judge(s) who presided over the case. **However, if the request for review concerns a magisterial district court's decision, it shall be reviewed by the president judge or his/her designee.**

Commentary

Case records are as susceptible to clerical errors and omissions as any other public record. The power of the court to correct errors in its own records is inherent. *E.g., Jackson v. Hendrick,* 746 A.2d 574 (Pa. 2000). It is important to emphasize that this section does not provide a party who is dissatisfied with a court's decision, ruling or judgment a new avenue to appeal the same by merely alleging there is an error in the court's decision, ruling or judgment. Rather, this section permits a party to "fix" information that appears in a case record which is not, for one reason or another, correct.

Particularly in the context of Internet publication of court records, a streamlined process is appropriate for addressing clerical errors to allow for prompt resolution of oversights and omissions. For example, to the extent that a docket in a court's case management system incorrectly reflects a court's order, or a scanning error occurred with regard to an uploaded document, such clerical inaccuracies may be promptly corrected by the appropriate court staff, upon notification, without a court order. Since 2007, the *Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania* has provided a similar procedure for any errors maintained on the web docket sheets of the PACMS, CPCMS and MDJS. The procedure has successfully addressed clerical errors on docket entries in a timely and administratively simple manner.

A party or party's attorney is not required to utilize the procedures set forth in this section before making a formal motion for correction of a case record in the first instance. Alleged inaccuracies in orders and judgments themselves must be brought to the attention of the court in accordance with existing procedures.

This section is not intended to provide relief for a party's or attorney's failure to comply with Sections 7.0 and 8.0 of this policy. Sections 7.0 and 8.0 already provide for remedial action in the event that non-compliance occurs.

With respect to this section, a custodian includes, but is not limited to, the county prothonotaries, clerks of orphans' court, **[and]** clerks of the court**, and magisterial district judges**.

A log of all corrections made pursuant to this section may be maintained by the custodian, so that there is a record if an objection is made in the future. Such a log should remain confidential. It is suggested that custodians include a registry entry on the case docket when a request is received and a response is issued.

Section 12.0. Continuous Availability of Policy.

A copy of this policy shall be continuously available for public inspection in every court and custodian's office and posted on the Unified Judicial System's website.

EXPLANATORY REPORT

Case Records Public Access Policy of the Unified Judicial System of Pennsylvania**[: Case Records of the Appellate and Trial Courts]**

General Introduction

Recognizing the importance of the public's access to the courts and with the Supreme Court's approval, the Administrative Office of Pennsylvania Courts (AOPC) has developed statewide policies governing access to court records. Protocols have been implemented for access to electronic case records in the Judiciary's statewide case management systems, magisterial district court case records, and financial records of the Unified Judicial System (UJS). In 2013, the AOPC embarked on the next phase of policy development designed to address access to case records of the trial and appellate courts.

This latest effort is necessitated by the confluence of several factors. The proliferation of e-filing systems and related decisions to post (or not post) case records online (as part of document imaging or e-filing systems) on a county-by-county basis has resulted in disjointed accessibility to the UJS's trial court case records. A county may post all divorce and custody records online for viewing, perhaps for free, and a neighboring county may not. Online posting of sensitive information contained in case records, such as social security numbers, currently depends upon geography. Surveys conducted by the AOPC also revealed the treatment of sensitive information contained in paper case records maintained by the filing offices varies widely. For example, whether a social security number is available to a member of the public who wishes to view the records of a particular case in a filing office depends upon local practices.

The implementation of e-filing in Pennsylvania's appellate courts and future initiatives at other court levels is also a catalyst for policy development. While appellate court opinions, orders and dockets have been online via the UJS's website for over a decade, the e-filing of appellate briefs and related legal papers raises basic questions that should be considered when a court undertakes such a project, for instance: What sensitive information must be redacted? Who is responsible for ensuring the appropriate information is redacted?

At the state and local level, the Judiciary is moving forward into the digital age, and it clearly needs to give thoughtful consideration to its systems and procedures to ensure equal access to the UJS's trial and appellate case records. Disparate filing and access protocols certainly impede the statewide practice of law in the Commonwealth. Litigants and third parties, some of whom are unrepresented or are not voluntary participants in the judicial process, may be left in the dark as to whether their private, personal identifiers and intimate details of their lives will be released (online) for public viewing.

Government and the private sector collect extensive amounts of personal data concerning individuals' finances, unique identifiers, medical history and so on. Many of these types of data are relevant to the cases that are before the courts for decision, and some data is provided in court filings even though irrelevant to the matter before the court. Therefore, like other branches of government and the private sector, the courts are constantly considering issues regarding the need for openness and transparency and the concern for personal privacy and security.

With regard to the courts, however, the constitutional and common law presumption of openness has to be carefully weighed against relevant practical, administrative considerations when crafting solutions to avert breaches of privacy and security. Striking the right balance is not an easy task.

The public's right to access court proceedings and records is grounded in the First and Sixth Amendments of the U.S. Constitution, Article I §§ 7, 9, and 11 of the Pennsylvania Constitution, and the common law. While there is overlap between the common law and constitutional analyses, there is a distinction between the two. Specifically, the constitutional provisions provide a greater right of access than the common law.[1] However, these constitutional and common law rights are not absolute and may be qualified by overriding interests. A more extensive discussion of the right to access is contained in the Explanatory Report of the *Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania*.[2]

Therefore, with the approval of the Supreme Court, the Court Administrator of Pennsylvania convened a working group to study and develop a proposed policy for public

[1] See *Commonwealth v. Long*, 922 A.2d 892 (Pa. 2007).

[2] Explanatory Report is found at: http://www.pacourts.us/assets/files/page-381/file-833.pdf?cb=1413983484884.

comment. Under the experienced and dedicated leadership of Commonwealth Court Judge Reneé]Cohn Jubelirer and Montgomery County Court of Common Pleas Judge Lois E. Murphy, the working group undertook its charge with an open mind and an aim to appropriately balance the competing interests at hand. The group consisted of judges, appellate court filing office personnel, local court personnel, two Prothonotaries/ Clerks of Courts, one Register of Wills/Clerk of Orphans' Court, and representatives from the Pennsylvania Bar Association and the rules committees of the Supreme Court, as well as AOPC staff.

Before developing a proposed policy, the working group studied and discussed the different types of records pertaining to criminal, domestic relations, civil, juvenile, orphans' court and appellate matters filed in the courts. Tackling each case type individually, the working group considered existing legal restrictions and other jurisdictions' access policies on the release of data and documents. In formulating whether information and documents should be considered confidential, the group also determined how access would be limited. There are categories of information that are completely restricted, such as social security numbers, and categories that are restricted from online viewing by the public but remain available for public inspection at a court facility, such as original and reproduced records filed in the appellate courts.

The working group published its proposal for a 60-day public comment period[3] and received thirty-two submissions. The comments reflected diverse, and sometimes conflicting, viewpoints, which helped the working group define the issues and find solutions. In doing so, the working group endeavored to find as much "common ground" as it could in reviewing and addressing the various comments.

In crafting its proposal, the group was guided at all times by the long-standing tradition of access to court records and the important interests it serves, as follows:

> to assure the public that justice is done evenhandedly 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. *Commonwealth v. Fenstermaker*, 530 A.2d 414, 417 (Pa. 1987) (citing *Commonwealth v. Contankos*, 453 A.2d 578, 579-80 (Pa. 1982)).

However, the group also recognized that transparency of judicial records and proceedings must be balanced with other considerations in this Internet age. The group attempted to strike the appropriate balance between access and interests involving the administration of justice, personal privacy and security—particularly with regard to online records. Also essential to the group's evaluation were practical considerations, such as the methods of redaction to be implemented and identification of various "best practices" that should be instituted statewide.

[3] http://www.pabulletin.com/secure/data/vol45/45-6/222.html.

The working group provides the following relevant commentary for the sections of the policy.

Section 1

The definitions incorporate elements of those found in existing UJS public access policies and other authorities.

This policy governs access to (1) official paper case records of appellate courts, courts of common pleas, **[and]** Philadelphia Municipal Court**, and magisterial district courts**, (2) images of scanned or e-filed documents residing in the three statewide case management systems, (3) images of scanned or e-filed documents residing in the case management systems of the judicial districts, and (4) case record information posted online by judicial districts via their own "local" case management systems. This approach ensures a more equitable and systematic approach to the case records filed in and maintained for the trial and appellate courts.

It is important to note how this policy intersects with **[existing UJS policies, namely]** the *Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania* (hereinafter referred to as "*Electronic Policy*") **[and *MDC Paper Policy*] as well as the recently rescinded *Public Access Policy of the Unified Judicial System of Pennsylvania: Official Case Records of the Magisterial District Courts* (hereinafter referred to as "MDC Paper Policy")**. The *Electronic Policy* governs access to the electronic case record information, excluding images of scanned documents, residing in the three statewide case management systems: Pennsylvania Appellate Courts Case Management System, Common Pleas Case Management System and the Magisterial District Judge System. Put simply, the *Electronic Policy* governs what information resides on the public web docket sheets accessible via the UJS web portal or is released to a member of the public requesting electronic case record information from one of the systems.

[The *MDC Paper Policy* governs access to the paper case records on file in a magisterial district courts.]

The *MDC Paper Policy* had governed access to the paper case records on file in a magisterial district court, but was rescinded when this Policy was amended in 2018 to govern public access to those records.

The definition of "financial source document" is derived from the definition of "sealed financial source documents" used in Minnesota (Minn.G.R.Prac. Rule 11.01) and Washington (WA.R.Gen. Rule 22(b)).

Section 2

This section's provisions are similar to those contained in the **rescinded** *MDC Paper Policy,* which **[have] had** been successfully implemented.

Section 4

Requestors may be unable to complete a written request, if required by a court. In such circumstances, access should not be denied but may be delayed until the custodian or designated staff is available to assist the requestor. If the request is granted, it may be necessary for the custodian or designated staff to sit with the requestor and monitor the use of the file to ensure its integrity. This is consistent with the responsibility placed upon the custodian and designated staff for the security, possession, custody and control of case records in Section

2.0(B). Such a practice is also consistent with the requirement that addressing requests for access cannot impede the administration of justice or the orderly operation of a court, pursuant to Section 2.0(C).

This section's provisions are similar to those contained in the **rescinded** *MDC Paper Policy*.

Section 5

While implementing the provisions of this policy should not unduly burden the courts and custodians or impinge upon the delivery of justice, it is reasonable for the public to expect that courts and custodians shall respond to requests for access in a consistent fashion. This section brings uniformity, in general, as to when and how courts and custodians must respond to requests. **[Similar sections are found in the *Electronic Policy* and *MDC Paper Policy*.] Both the *Electronic Policy* and the rescinded *MDC Paper Policy* contained similar sections.**

Section 6

Judicial districts have adopted different approaches to imposition of fees, especially with regard to remote access to court records. Some impose a fee for providing remote access because the costs associated with building and maintaining such systems are often substantial. Given that remote access is a value-added service, not a requirement, it is thought that those who avail themselves of this service should be charged for the convenience of maintaining these systems.

Others do not impose fees for remote access because providing this service reduces the "foot traffic" in the filing offices for public access requests. This, in turn, frees staff to attend to other business matters, resulting in a financial benefit by reducing costs associated with dealing with the requests over the counter. The AOPC has provided "free" online access to public web docket sheets for cases filed in the appellate courts, criminal divisions of the courts of common pleas and Philadelphia Municipal Court, as well as the magisterial district courts for years. In 2014, 59 million of those web dockets sheets were accessed online.

It is interesting to note that the two largest judicial districts in the Commonwealth are at opposite ends of the spectrum (i.e., one has posted virtually all dockets and documents for free, and the other posts some dockets for free but not documents). While the working group recognizes that other factors play into these determinations (such as, technological capabilities, statutorily mandated fees), judicial districts should ensure that fees do not become a barrier to public access. Completion of statewide case management systems in all levels of court will likely bring about standardization in remote access to case records.

The working group notes that this section's provisions are similar to those contained in the **rescinded** *MDC Paper Policy.*

Section 7

The concept of restricting access to particular, sensitive identifiers is not novel. The *Electronic Policy* and **the rescinded** *MDC Paper Policy* restrict access to social security numbers and financial account numbers, for example. The federal courts, and many state court systems, have restricted access to the types of identifiers that are listed in Section 7.0.

The *Electronic Policy* and **the rescinded** *MDC Paper Policy* provide that access to social security numbers is shielded from release. Moreover, there are scores of authorities at both the federal and state level that protect the release of this information. While some of these authorities are not applicable to court records, they require access to this information in government records be limited or wholly restricted. For example: 65 P.S. § 67.708(b)(6)(i)(A), 74 P.S. § 201, 42 U.S.C.A. § 405(c)(2)(C)(viii), F.R.Civ.P.5.2(a)(1), F.R.Crim.P. 49.1(a)(1), Alaska (AK R Admin Rule 37.8(a)(3)), Arizona (AZ ST S CT Rule 123(c)(3)), Arkansas (Sup. Ct. Admin. Order 19(VII)(a)(4)), Florida (FL ST J ADMIN Rule 2.420(d)(1)(B)(iii)), Idaho (ID R Admin Rule 32(e)(2)), Indiana (Ind. St. Admin. Rule 9(G)(1)(d)), Maryland (MD. Rules 16-1007), Michigan (Administrative Order 2006-2), Minnesota (Minn.Gen.R.Prac. Rule 11.01(a)), Mississippi (Administrative Order dated August 27, 2008 paragraph 8), Nebraska (Neb Ct R § 1-808(a) and Neb. Rev. Stat § 84-712.05(17)), New Jersey (NJ R GEN APPLICATION Rule 1:38-7(a)), North Dakota (N.D.R.Ct. Rule 3.4(a)(1) and A.R. 41(5)(B)(10)(a)), Ohio (OH ST Sup Rules 44(h) and 45(d)), South Dakota (SDCL § 15-15A-8), Texas (TX ST J ADMIN Rule 12.5(d)), Utah (UT R J ADMIN Rules 4-202.02(4)(i) and 4-202-03(3)), Vermont (VT R PUB ACC CT REC § 6(b)(29)), Washington (WA.R.Gen. Rule 31(3)(1)(a)) and West Virginia (WV R RAP Rule 40(e)(3)).

With regard to financial account numbers, the *Electronic Policy* and **the rescinded** *MDC Paper Policy* provide that this information is not accessible. Many other jurisdictions have taken a similar approach. For example: F.R.Civ.P. 5.2(a)(1), F.R.Crim.P. 49.1(a)(1), Alaska (AK R Admin Rule 37.8(a)(5)), Arizona (AZ ST S CT Rule 123(c)(3)), Arkansas (Sup. Ct. Admin. Order 19(VII)(a)(4)), Florida (FL ST J ADMIN Rule 2.420(d)(1)(B)(iii)), Idaho (ID R Admin Rule 32(e)(2)), Indiana (Ind. St. Admin. Rule 9(G)(1)(f)), Minnesota (Minn.Gen.R.Prac. Rule 11.01(a)), Nebraska (Neb Ct R § 1-808(a) and Neb. Rev. Stat § 84-712.05(17)), New Jersey (NJ R GEN APPLICATION Rule 1:38-7(a)), North Dakota (N.D.R.Ct. Rule 3.4(a)(1) and A.R. 41(5)(B)(10)(a)), Ohio (OH ST Sup Rules 44(h) and 45(d)), South Dakota (SDCL § 15-15A-8), Vermont (VT R PUB ACC CT REC § 6(b)(29)), Washington (WA.R.Gen. Rule 31(3)(1)(b)) and West Virginia (WV R RAP Rule 40(e)(4)).

Concerning driver license numbers, the *Electronic Policy* provides that driver license numbers should be protected. Moreover, there are many authorities at both the federal and state level that protect the release of this information. While some of these authorities are not applicable to court records, they require access to this information in government records be limited or wholly restricted. For example: 65 P.S. § 67.708(b)(6)(i)(A), 75 Pa.C.S. § 6114, 18 U.S.C. §§ 2721—2725, Alaska (AK R Admin Rule 37.8(a)(4)), Idaho (ID R Admin Rule 32(e)(2)), New Jersey (NJ R GEN APPLICATION Rule 1:38-7(a)), Utah (UT R J ADMIN Rules 4-202.02(4)(i) and 4-202-03(3)), Vermont (VT R PUB ACC CT REC § 6(b)(29)) and Washington (WA.R.Gen. Rule 31(3)(1)(c)).

State Identification Numbers ("SID") have been defined as "[a] unique number assigned to each individual whose fingerprints are placed into the Central Repository of the State Police. The SID is used to track individuals for crimes which they commit, no matter how many subsequent fingerprint cards are submitted." *See* 37 Pa. Code § 58.1. The *Electronic Policy* prohibits the release of SID. Furthermore, in *Warrington Crew v. Pa. Dept. of Corrections*, (Pa. Cmwlth., No. 1006 C.D. 2010, filed Nov. 19,

2010)[4], the Commonwealth Court upheld a ruling by the Office of Open Records that a SID number is exempt from disclosure through a right-to-know request because such numbers qualify as a confidential personal identification number.

Other jurisdictions provide similar protections to minors' names, dates of births, or both. For example: F.R.Civ.P. 5.2(a)(1), F.R.Crim.P. 49.1(a)(1), Alaska (AK R Admin Rule 37.8(a)(6)), North Dakota (N.D.R.Ct. Rule 3.4(a)(3) and A.R.41(5)(B)(10)(c)), Utah (UT R J ADMIN Rules 4-202.02(4)(l) and 4-202-03(3)) and West Virginia (WV R RAP Rule 40(e)(1)).

With regard to abuse victims' address and other contact information, Pennsylvania through the enactment of various statutes has recognized the privacy and security needs of victims of abuse. For example, Pennsylvania's Domestic and Sexual Violence Victim Address Confidentiality Act (23 Pa.C.S. §§ 6701—6713) provides a mechanism whereby victims of domestic and sexual violence can shield their physical address (even in court documents) and hence protect their ability to remain free from abuse. The Pennsylvania Right To Know Law (65 P.S. §§ 67.101—67.1304) recognizes the potential risk of harm which can be caused by the disclosure by the government of certain personal information. For example, 65 P.S. § 67.708(b)(1)(ii) prohibits the disclosure that "would be reasonably likely to result in a substantial and demonstrable risk of physical harm to or the personal security of an individual." Moreover, 23 Pa.C.S. § 5336(b) prohibits the disclosure of the address of a victim of abuse in a custody matter to the other parent or party. 23 Pa.C.S. § 4305(a)(10)(ii) and (iii) provides that the domestic relations section shall have the power and duty to:

> "implement safeguards applicable to all confidential information received by the domestic relations section in order to protect the privacy rights of the parties, including: prohibitions against the release of information on the whereabouts of one party or the child to another party against whom a protective order with respect to the former party or the child has been entered; and prohibitions against the release of information on the whereabouts of one party or the child to another person if the domestic relations section has reason to believe that the release of the information may result in the physical or emotional harm to the party or the child."

In addition, other jurisdictions have taken a measure to protect similarly situated individuals, such as: Alaska (AK R Admin Rule 37.8(a)(2)), Florida (FL ST J ADMIN Rule 2.420(d)(1)(B)(iii)), Indiana (Ind. St. Admin. Rule 9(G)(1)(e)(i)), New Jersey (NJ R GEN APPLICATION Rule 1:38-3(c)(12)), and Utah (UT R J ADMIN Rules 4-202.02(8)(E)(i) and 4-202-03(7)).

To maintain the confidentiality of the information listed in subsection (A), parties and their attorneys can set forth the listed information on a Confidential Information Form, designed and published by the AOPC. This is akin to the procedure set forth in the **rescinded** *MDC Paper Policy***[; the Confidential Information Form used by that policy is posted on the UJS's website at www.pacourts.us]**.

Alternatively, parties and their attorneys can file two versions of each document with the court/custodian—one with sensitive information redacted ("redacted copy') and the other with no information redacted ("unredacted copy"). The redacted copy shall omit any information not accessible under this policy in a visibly evident manner, and be available for public inspection. The unredacted copy shall not be accessible by the public. At least one other jurisdiction has implemented a similar approach. *See* WA.R.Gen. R. 22(e)(2) (Washington). Some contend that a redacted copy of a document will be more readable than an unredacted copy containing monikers as placeholders for sensitive information not included in the document. This approach was also identified as a more amenable solution given the current design of the statewide e-filing initiative.

This option is not applicable to filings in a magisterial district court, rather filers must use the Confidential Information Form as provided in subsection (A). However, most of the forms that are found within the case files of a magisterial district court are statewide forms that are generated from the Magisterial District Judge System (a statewide case management system for these courts). The protection of confidential information captured on current MDJS forms requires a multi-faceted approach that takes into account how each form that contains such information is used. For example, AOPC has removed or suppressed social security numbers and operator license numbers from various forms when such information is extraneous to the court's adjudication of the case or the collection of the information is not otherwise required. In some instances, the filer will be responsible for placing the confidential information on the Confidential Information Form.

While a court or custodian is not required to review any pleading, document, or other legal paper for compliance with this section, such activity is not prohibited. If a court or custodian wishes to accept the burden of reviewing such documents and redacting the same, such a process must be applied uniformly across all documents or cases. This provision, however, does not alter or expand upon existing legal authority limiting a custodian's authority to reject a document for filing. *See Nagy v. Best Home Services, Inc.,* 829 A.2d 1166 (Pa. Super. 2003).

Courts that permit e-filing should consider the development of a compliance "checkbox" whereby e-filers could indicate their compliance with this policy.

This section only applies to documents filed with a court or custodian on or after the effective date of this policy. There will be a period of transition prior to full implementation of this policy; that is, some documents filed with a court or custodian prior to the effective date of this policy will contain information that the policy restricts from public access. To expect full and complete implementation of this policy by applying it retroactively to those documents filed prior to the effective day of this policy is impractical and burdensome.

However, it is important to remember with regard to pre-policy records, a party or attorney always has the option to file a motion with **[the court] a court of record** to seal, in whole or part, a document or file. This includes the ability to request sealing and/or redaction of only some information that resides on a document in the court file (e.g., a social security number on a document).

Section 8

The protocol of submitting to a court or custodian certain documents under a cover sheet so that the documents are not accessible to the public has been

[4] Pursuant to Section 414(a) of the Commonwealth Court's Internal Operating Procedures, an unreported panel decision issued by the Court after January 15, 2008 may be cited "for its persuasive value, but not as binding precedent." 210 Pa. Code § 69.414(a).

instituted in other jurisdictions, such as Minnesota (Minn.G.R.Prac. Rule 11.03), South Dakota (SDCL § 15-15A-8), and Washington (WA.R.Gen. Rule 22(b)(8) and (g)). One manner in which to implement this protocol (e.g., the need to separate a confidential document within a file accessible to the public) is to maintain a confidential electronic folder or confidential documents file within the case file, thus ensuring that the file folder with the non-public information can be easily separated from the public case file, when access is requested.

Concerning financial source documents, other jurisdictions have similar provisions regarding such documents including Minnesota (Minn.G.R.Prac. Rule 11.03), South Dakota (SDCL § 15-15A-8), and Washington (WA.R.Gen. Rule 22(b)(8) and (g)).

Similar protocols with regard to minors' education records are found in other jurisdictions, such as Nebraska (Neb Ct R § 1-808(a) and Neb. Rev. Stat § 84-712.05(1)) and Wyoming (WY R Gov Access Ct Rule 6(a) and WY ST § 16-4-203(d)(viii)).

With regard to medical records, other jurisdictions have similar provisions including Indiana (Ind. St. Admin. Rule 9(G)(1)(b)(xi)), Maryland (MD. Rules 16-1006(i)), Nebraska (Neb Ct R § 1-808(a) and Neb. Rev. Stat § 84-712.05(2)), Utah (UT R J ADMIN Rules 4-202.02(4)(k) and 4-202-03(3)), Vermont (VT R PUB ACC CT REC § 6(b)(17)), West Virginia (WV R RAP Rule 40(e)(1)) and Wyoming (WY R Gov Access Ct Rule 6(t)).

Section 7111 of the Mental Health Procedures Act, 50 P.S. § 7111, provides that all documentation concerning an individual's mental health treatment is to be kept confidential and may not be released or disclosed to anyone, absent the patient's written consent, with certain exceptions including a court's review in the course of legal proceedings authorized under the Mental Health Procedures Act (50 P.S. § 7101). While it is unclear if this provision is applicable to the public accessing an individual's mental health treatment records in the court's possession, the working group believes this provision provides guidance on the subject. Thus, such records should not be available to the public except pursuant to a court order. *See Zane v. Friends Hospital,* 575 Pa. 236, 836 A.2d 25 (2003). Other jurisdictions have similar protocols, such as Maryland (MD. Rules 16-1006(i)), New Mexico (NMRA Rule 1-079(c)(5)), Utah (UT R J ADMIN Rules 4-202.02(4)(k) and 4-202-03(3)), Vermont (VT R PUB ACC CT REC § 6(b)(17)) and Wyoming (WY R Gov Access Ct Rule 6(p)).

Children and Youth Services' records introduced in juvenile dependency or delinquency matters are not open to public inspection. *See* 42 Pa.C.S. § 6307 as well as Pa.Rs.J.C.P. 160 and 1160. Introduction of such records in a different proceeding (e.g., a custody matter) should not change the confidentiality of these records; thus, the records should be treated similarly. These records are treated similarly by other jurisdictions, such as Florida (FL ST J ADMIN Rule 2.420(d)(1)(B)(i)), Indiana (Ind. St. Admin. Rule 9(G)(1)(b)(iii)) and New Jersey (NJ R GEN APPLICATION Rule 1:38-3(d)(12) and (15)).

The extent of financially sensitive information required by Pa.R.C.P. No. 1910.27(c) and 1920.33 that must be listed on income and expense statements, marital property inventories and pre-trial statements rivals information contained in a financial source document. Therefore, these documents should also be treated as confidential. Vermont has a similar protocol (VT R PUB ACC CT REC § 6(b)(33) and 15 V.S.A. § 662).

Courts that permit e-filing should consider the development of a compliance "checkbox" whereby e-filers could indicate their compliance with this policy.

This section only applies to documents filed with a court or custodian on or after the effective date of this policy. There will be a period of transition prior to full implementation of this policy; that is, some documents filed with a court or custodian prior to the effective date of this policy will contain information that the policy restricts from public access. To expect full and complete implementation of this policy by applying it retroactively to those documents filed prior to the effective day of this policy is impractical and burdensome.

However, it is important to remember with regard to pre-policy records, a party or attorney always has the option to file a motion with **[the court]** **a court of record** to seal, in whole or part, a document or file. This includes the ability to request sealing and/or redaction of only some information that resides on a document in the court file (e.g., a social security number on a document).

Section 9

This section safeguards certain sensitive information that is already protected by existing authority or was deemed to require protection by the working group from access at the court facility. The latter category included two specific types of records: birth records and incapacity proceeding records.

Access to a birth certificate from the Department of Health, particularly an amended birth certificate, such as in an adoption case, is limited pursuant to various statutes. 35 P.S. §§ 450.603, 2915 and 2931. Unrestricted access to records filed in proceedings about birth records could have the unintended effect of circumventing the purposes of the confidentiality provisions of the above statutory framework. Moreover, at least one jurisdiction, Florida (FL ST J ADMIN Rule 2.420(d)(1)(B)(vi)), provides similar protections to these records. However, concerned that the lack of transparency may erode the public's trust and confidence, dockets and any court order, decree or judgment in these cases are exempted by the policy. Releasing the dockets as well as any order, decree or judgment disposing of the case is believed to strike the appropriate balance between access to the court's decision, and hence the public's understanding of the judicial function, and personal privacy.

Given the extent of financial and sensitive information that is provided in order that a court may determine whether a person is incapacitated and, if so, that must subsequently be reported in a guardian's report, these records are not be accessible. Similar provisions are found in many other jurisdictions including: California (Cal. Rules of Court, Rule 2.503(c)(3)), Florida (F.S.A. §§ 744.1076 and 744.3701), Georgia (Ga. Code Ann. § 29-9-18), Idaho (ID. R. Admin. Rule 32), Maryland (MD. Rules 16-1006), New Jersey (NJ R GEN APPLICATION Rule 1:38-3(e)), New Mexico (NMRA Rule 1-079(c)(7)), South Dakota (SDCL § 15-15A-7(3)(m)), Utah (UT R J Admin. Rule 4-202.02(4)(L)(ii)), Washington (WA.R.Gen. Rule 22(e)) and Wyoming (WY R Gov Access Ct Rule 6(g)). For the reasons of transparency, the case docket and any court order, decree or judgment for these cases is exempted pursuant to this policy.

The provisions of Subsection G are consistent with those contained in the *Electronic Policy*, **the rescinded** *MDC Paper Policy* and Rule of Judicial Administration 509. The Judiciary's commitment to the principle of open

and accessible case records is reflected in the inclusion of a publication requirement.

Section 10

Any information to which access is limited pursuant to Sections 7, 8 or 9 is also not accessible remotely pursuant to Subsection A(1). As to Subsections A(2) through (A)(7), it is important to note that this information will remain available at the courthouse or court facility where access has been traditionally afforded. There is a difference between maintaining "public" records for viewing/copying at the courthouse and "publishing" records on the Internet. Thus, there is certain information for which at the present time courthouse access remains the appropriate forum.

Concerning Subsection A(2)'s restriction on remote access to information that identifies jurors, witnesses, and victims in criminal cases, similar provision exist in the *Electronic Policy* and have been implemented by other jurisdictions, including Alaska (AK R ADMIN Rule 37.8(a)(1) and (2)), Indiana (Ind. St. Admin. Rule 9(G)(1)(e)), Mississippi (Administrative Order dated August 27, 2008 paragraph 8), Nebraska (NE R CT § 1-808(b)(3)), Texas (TX ST J ADMIN Rule 12.5(d)) and Utah (UT R J ADMIN Rules 4-202.02(8)(e) and 4-202-03(7)).

As pertains to Subsection A(5), in considering family court records (i.e., divorce, custody, and support), individual courts have implemented protocols to shield some of these records from access. Sensitive to these concerns, prohibiting online posting of any family court records (save for a docket, court orders and opinions), along with the requirements that certain information and documents filed with the court or custodian be restricted from access via the use of a Confidential Information Form, redacted filings or a Confidential Document Form, removes a significant amount of the personal, sensitive information from access, while allowing public access to ensure accountability and transparency of the judicial system.

With regard to Subsection A(6), New Mexico has a similar protocol protecting Older Adult Protective Services Act matters (NMRA Rule 1-079(c)(4)). For the reasons expressed above, remote access should be afforded to dockets, court orders and opinions in these cases, to the extent that the judicial districts have developed systems and procedures that facilitate such access.

While case records remotely accessible to the public prior to the effective date of this policy may remain online in unredacted form, judicial districts are not prohibited from taking steps to safeguard sensitive case records designated by this section. To expect full and complete implementation of the policy by applying it retroactively to records remotely accessible prior to the effective date of this policy is impractical and burdensome.

However, it is important to remember with regard to pre-policy records, a party or attorney always has the option to file a motion with the court to seal, in whole or part, a document or file. This includes the ability to request sealing and/or redaction of only some information that resides on a document in the court file (e.g., a social security number on a document).

It is essential that courts and custodians in designing systems, such as those for document imaging, e-filing, or both consider the requirements of this policy and ensure such systems are in compliance. This is imperative as the Judiciary moves toward statewide e-filing for all levels of courts.

As for systems currently in existence, the policy may require changes to current protocols and processes.

Section 11

A similar provision is included in the *Electronic Policy*. This policy delineates a procedure by which an individual may correct a clerical error that appears in a case record accessible remotely. As noted in the Explanatory Report to the *Electronic Policy*, these provisions borrow heavily from the correction provisions in the Criminal History Record Information Act. For the same reasons outlined in the Explanatory Report, a similar protocol was included in this policy.

Best Practices

The following are various "best practices" that should be considered by the courts, parties and their attorneys to promote the successful implementation of this policy.

1. The Judiciary should remain cognizant of this policy in the development of e-filing and case management systems, procedures and forms. The following "best practices" should be considered as courts develop systems for e-filing:

a. Access to the courts should be promoted by the e-filing processes;

b. Court control over its own records should be preserved;

c. Systems should have consistent functionality, compatible protocols and rules to facilitate statewide practice;

d. Processes for *pro se* litigants should be defined to provide equal and secure access to the system;

e. Issues involving public access to e-documents, and the sensitive data that may be contained therein, should be fully studied before the e-filing system is developed (e.g., separate e-filing of exhibits from other documents);

f. Payment of any required filing fees should be accomplished via electronic methods;

g. Bi-directional exchange of data should be facilitated between e-filing and case management systems; and

h. Maximum flexibility in the design of a system should be sought to accommodate future evolutions of technology.

2. Compliance with this policy and the Judiciary's commitment to open records may be assisted by various technological and administrative solutions, such as:

a. Implementation of redaction and "optical character recognition" software may assist parties and their attorneys in complying with the policy. Some judicial districts also employ redaction software to protect sensitive data as a "best practice."

b. Due consideration and routine review by custodians should be given to the standards for record retention as applied to those records in paper form and electronic form.

[Pa.B. Doc. No. 18-675. Filed for public inspection May 4, 2018, 9:00 a.m.]

Title 237—JUVENILE RULES

PART I. RULES

[237 PA. CODE CH. 4]

Order Amending Rule 409 of the Rules of Juvenile Court Procedure; No. 763 Supreme Court Rules Doc.

Order

Per Curiam

And Now, this 23rd day of April, 2018, upon the recommendation of the Juvenile Court Procedural Rules Committee, the proposal having been published for public comment at 47 Pa.B. 7304 (December 2, 2017):

It is Ordered pursuant to Article V, Section 10 of the Constitution of Pennsylvania that Rule 409 of the Pennsylvania Rules of Juvenile Court Procedure is amended in the following form.

This Order shall be processed in accordance with Pa.R.J.A. No. 103(b), and shall be effective on July 1, 2018.

Annex A

TITLE 237. JUVENILE RULES

PART I. RULES

Subpart A. DELINQUENCY MATTERS

CHAPTER 4. ADJUDICATORY HEARING

Rule 409. Adjudication of Delinquency.

A. *Adjudicating the* **[** ***juvenile delinquent*** **]** ***Juvenile Delinquent***. Once the court has ruled on the offenses as provided in Rule 408, the court shall conduct a hearing to determine if the juvenile is in need of treatment, supervision, or rehabilitation.

1) *Not in* **[** ***need*** **]** ***Need***. If the court determines that the juvenile is not in need of treatment, supervision, or rehabilitation, the court shall enter an order providing that:

a) **[jurisdiction shall be terminated] the petition shall be dismissed** and the juvenile shall be released, if detained, unless there are other reasons for the juvenile's detention; and

b) any records, fingerprints, and photographs taken shall be expunged or destroyed.

2) *In* **[** ***need*** **]** ***Need***.

* * * * *

Comment

Under paragraph (A), absent evidence to the contrary, evidence of the commission of acts that constitute a felony is sufficient to sustain a finding that the juvenile is in need of treatment, supervision, or rehabilitation. *See* 42 Pa.C.S. § 6341(b).

If the court determines that the juvenile is not in need of treatment, supervision, or rehabilitation and the court enters an order **[terminating jurisdiction] dismissing the petition**, the victim, if not present, shall be notified of the final outcome of the proceeding. *See* Victim's Bill of Rights, 18 P.S. § 11.201 *et seq.*

This rule addresses adjudicating the juvenile delinquent or **[releasing the juvenile from the court's jurisdiction] dismissing the petition**. This determination is different from finding the juvenile committed a delinquent act under Rule 408.

* * * * *

***Official Note*:** Rule 409 adopted April 1, 2005, effective October 1, 2005. Amended December 24, 2009, effective immediately. Amended May 26, 2011, effective July 1, 2011. Amended July 28, 2014, effective September 29, 2014. **Amended April 23, 2018, effective July 1, 2018.**

Committee Explanatory Reports:

Final Report explaining the provisions of Rule 409 published with the Court's Order at 35 Pa.B. 2214 (April 16, 2005).

Final Report explaining the amendments to Rule 409 published with the Court's Order at 40 Pa.B. 222 (January 9, 2010).

Final Report explaining the amendments to Rule 409 published with the Court's Order at 41 Pa.B. 3180 (June 25, 2011).

Final Report explaining the amendments to Rule 409 published with **the** Court's Order at 44 Pa.B. 5447 (August 16, 2014).

Final Report explaining the amendments to Rule 409 published with the Court's Order at 48 Pa.B. 2615 (May 5, 2018).

FINAL REPORT[1]

Amendment of Pa.R.J.C.P. 409

On April 23, 2018, the Supreme Court amended Rule of Juvenile Court Procedure 409 to change the outcome from "termination of jurisdiction" to "dismissal of petition" when the court finds the juvenile is "not in need."

The amendment is not intended to have a substantive impact on current procedure. Rather, it represents a change in terminology to more precisely identify the procedural outcome, to avoid conflation of "jurisdiction" with its use in other Rules of Juvenile Court Procedure, see e.g., Pa.R.J.C.P. 630, and to enhance correlation with Rule 170(A)(2).

The amendment will become effective July 1, 2018.

[Pa.B. Doc. No. 18-676. Filed for public inspection May 4, 2018, 9:00 a.m.]

Title 237—JUVENILE RULES

PART I. RULES

[237 PA. CODE CH. 11]

Order Amending Rule 1140 of the Rules of Juvenile Court Procedure; No. 764 Supreme Court Rules Doc.

Order

Per Curiam

And Now, this 23rd day of April, 2018, upon the recommendation of the Juvenile Court Procedural Rules Committee, the proposal having been published for public comment at 47 Pa.B. 7016 (November 18, 2017):

[1] The Committee's Final Report should not be confused with the official Committee Comments to the rules. Also note that the Supreme Court does not adopt the Committee's Comments or the contents of the Committee's explanatory Final Reports.

It is Ordered pursuant to Article V, Section 10 of the Constitution of Pennsylvania that Rule 1140 of the Pennsylvania Rules of Juvenile Court Procedure is amended in the following form.

This Order shall be processed in accordance with Pa.R.J.A. No. 103(b), and shall be effective on July 1, 2018.

Annex A

TITLE 237. JUVENILE RULES

PART I. RULES

Subpart B. DEPENDENCY MATTERS

CHAPTER 11. GENERAL PROVISIONS

PART A. BUSINESS OF COURTS

Rule 1140. Bench Warrants for Failure to Appear.

A. *Issuance of* **[** ***warrant*** **]** ***Warrant***.

1) Before a bench warrant may be issued by a judge, the judge shall find that the subpoenaed or summoned person received sufficient notice of the hearing and failed to appear.

2) For the purpose of a bench warrant, a judge may not find notice solely based on first-class mail service.

3) The judge shall not issue an arrest warrant for a dependent child who absconds.

B. *Party.*

1) *Where to* **[** ***take the party*** **]** ***Take the Party***.

* * * * *

2) *Prompt* **[** ***hearing*** **]** ***Hearing***.

a) If a party is detained pursuant to a specific order in the bench warrant, the party shall be brought before the judge who issued the warrant, a judge designated by the President Judge to hear bench warrants, or an out-of-county judge pursuant to paragraph (B)(4) within seventy-two hours.

b) If the party is not brought before a judge within this time, the party shall be released.

3) *Notification of* **[** ***guardian*** **]** ***Guardian***. If a party is a child and is taken into custody pursuant to a bench warrant, the arresting officer shall immediately notify the child's guardian of the child's whereabouts and the reasons for the issuance of the bench warrant.

4) **[** ***Out-of-county custody.*** **]** ***Out-of-County Custody.***

* * * * *

5) *Time* **[** ***requirements*** **]** ***Requirements***. The time requirements of Rules 1242, 1404, 1510, and 1607 shall be followed.

C. *Witnesses.*

1) *Where to* **[** ***take the witness*** **]** ***Take the Witness***.

* * * * *

2) *Prompt* **[** ***hearing*** **]** ***Hearing***.

a) If a witness is detained pursuant to paragraph (C)(1)(c) or brought back to the county of issuance pursuant to paragraph (C)(4)(f), the witness shall be brought before the judge by the next business day.

b) If the witness is not brought before a judge within this time, the witness shall be released.

3) *Notification of* **[** ***guardian*** **]** ***Guardian***. If a witness who is taken into custody pursuant to a bench warrant is a minor, the arresting officer shall immediately notify the witness's guardian of the witness's whereabouts and the reasons for the issuance of the bench warrant.

4) **[** ***Out-of-county custody.*** **]** ***Out-of-County Custody*.**

* * * * *

E. *Return &* **[** ***execution of the warrant for parties and witnesses*** **]** ***Execution of the Warrant for Parties and Witnesses***.

* * * * *

Comment

Pursuant to paragraph (A), the judge is to ensure that the person received sufficient notice of the hearing and failed to attend. The judge may order that the person be served in-person or by certified mail, return receipt. The judge may rely on first-class mail service if additional evidence of sufficient notice is presented. For example, testimony that the person was told in person about the hearing is sufficient notice. Before issuing a bench warrant, the judge should determine if the guardian was notified.

Under Rule 1800, 42 Pa.C.S. § 6335(c) was suspended only to the extent that it is inconsistent with this rule. Under paragraph (A)(1), the judge is to find a subpoenaed or summoned person failed to appear and sufficient notice was given to issue a bench warrant. The fact that the party or witness may abscond or may not attend or be brought to a hearing is not sufficient evidence for a bench warrant. The normal rules of procedure in these rules are to be followed if a child is detained. *See* Chapter Twelve**[, Part D]**.

[Pursuant to paragraph (B)(1)(a), the party is to be taken immediately to the judge who issued the bench warrant or a judge designated by the President Judge of that county to hear bench warrants. Pursuant to paragraph (B)(1)(b), if a bench warrant specifically provides that the party may be detained, the party may be detained without having to be brought before the judge until a hearing within seventy-two hours under paragraph (B)(2)(a). Pursuant to this paragraph, if a hearing is not held promptly, the party is to be released. *See* paragraph (B)(2)(b).]

Paragraph (A)(3) does not preclude the issuance of a bench warrant for a case in which the child is subject to the jurisdiction of the dependency and delinquency court, see Rule 141 (Bench Warrants for Absconders), or an order for protective custody. Nor does the paragraph preclude judicial inquiry into efforts to locate a missing dependent child.

In paragraphs (B)(1)(c)(i), (C)(1)(c)(i), & (C)(4)(e)(i), "other placement as deemed appropriate by the judge" does not include a detention facility if a child is only alleged to be dependent because the use of detention facilities for dependent children is strictly prohibited. *See* 42 Pa.C.S. § 6302 & 6327(e).

Under paragraphs (B)(2) and (B)(4), a party taken into custody pursuant to a bench warrant is to have a hearing within seventy-two hours regardless of where the party is found. *See* Rule 1242(D).

Pursuant to paragraph (B)(4), the party may be detained out-of-county until transportation arrangements can be made.

[Pursuant to paragraph (B)(5), the time requirements of all other rules are to apply to children who are detained. *See, e.g.*, Rules 1242, 1404, 1510, and 1607.

Pursuant to paragraph (C)(1)(a), the witness is to be taken immediately to the judge who issued the bench warrant or a judge designated by the President Judge of that county to hear bench warrants. Pursuant to paragraph (C)(1)(b), if the judge is not available, the witness is to be released immediately unless the warrant specifically orders detention. Pursuant to paragraph (C)(1)(c), a motion for detention as a witness may be filed. If the witness is detained, a prompt hearing pursuant to paragraph (C)(2) is to be held by the next business day or the witness is to be released. *See* paragraph (C)(2)(b).]

Pursuant to paragraph (C)(4)(b), a witness is to be brought before an out-of-county judge by the next business day unless the witness can be brought before the judge who issued the bench warrant within this time. When the witness is transported back to the county of issuance within seventy-two hours of the execution of the bench warrant, the witness is to be brought before the judge who issued the bench warrant by the next business day. *See* paragraph (C)(4)(f).

[Pursuant to paragraph (E)(2), the bench warrant is to be returned to the judge who issued the warrant or to the judge designated by the President Judge to hear warrants by the arresting officer executing a return of warrant. *See* paragraph (E)(3).]

Pursuant to paragraph (E)(4), the bench warrant is to be vacated after the return of the warrant is executed so the party or witness is not taken into custody on the same warrant if the party or witness is released. "Vacated" is to denote that the bench warrant has been served, dissolved, executed, dismissed, canceled, returned, or any other similar language used by the judge to terminate the warrant. The bench warrant is no longer in effect once it has been vacated.

See 42 Pa.C.S. § 4132 for punishment of contempt for children and witnesses.

Throughout these rules, the "child" is the subject of the dependency proceedings. When a witness or another party is under the age of eighteen, the witness or party is referred to as a "minor." When "minor" is used, it may include a child. This distinction is made to differentiate between children who are alleged dependents and other minors who are witnesses. See also Rule 1120 for the definitions of "child" and "minor."

***Official Note*:** Rule 1140 adopted March 19, 2009, effective June 1, 2009. Amended April 21, 2011, effective July 1, 2011. **Amended April 23, 2018, effective July 1, 2018.**

Committee Explanatory Reports:

Final Report explaining the provisions of Rule 1140 published with the Court's Order at 39 Pa.B. 1614 (April 4, 2009).

Final Report explaining the amendments to Rule 1140 published with the Court's Order at 41 Pa.B. 2319 (May 7, 2011).

Final Report explaining the amendments to Rule 1140 published with the Court's Order at 48 Pa.B. 2615 (May 5, 2018).

FINAL REPORT[1]

Amendment of Pa.R.J.C.P. 1140

On April 23, 2018, the Supreme Court amended Rule of Juvenile Court Procedure 1140 to add paragraph (a)(3) to clarify that arrest warrants are not to be issued for absconding dependent children. Further, the Comment was revised to state that Rule 1140(a)(3) does not preclude the issuance of a warrant for a case in which the child is subject to the jurisdiction of the dependency and delinquency court or a pickup order for protective custody. Post-publication, the Juvenile Court Procedural Rules Committee recommended additional language in the Comment indicating that judicial inquiry into efforts to locate a missing dependent child is not precluded under the Rule.

Several portions of the Comment merely reiterative of the rule text were deleted to improve readability.

The amendment will become effective July 1, 2018.

[Pa.B. Doc. No. 18-677. Filed for public inspection May 4, 2018, 9:00 a.m.]

Title 246—MINOR COURT CIVIL RULES

PART I. GENERAL

[246 PA. CODE CH. 300]

Order Amending Rule 314 of the Rules of Civil Procedure Before Magisterial District Judges; No. 420 Magisterial Rules Doc.

Order

Per Curiam

And Now, this 20th day of April, 2018, upon the recommendation of the Minor Court Rules Committee, the proposal having been published for public comment at 47 Pa.B. 4082 (July 29, 2017):

It is Ordered pursuant to Article V, Section 10 of the Constitution of Pennsylvania that Rule 314 of the Pennsylvania Rules of Civil Procedure Before Magisterial District Judges is amended in the following form.

This Order shall be processed in accordance with Pa.R.J.A. No. 103(b), and shall be effective on July 1, 2018.

Annex A

TITLE 246. MINOR COURT CIVIL RULES

PART I. GENERAL

CHAPTER 300. CIVIL ACTION

Rule 314. Return, Waiver and Failure of Service; Reinstatement.

A. The person serving the complaint shall, at or before the time of the hearing, make proof of service which shall show (1) the manner of service, (2) the date, time, and place of service and, (3) the name and relationship or

[1] The Committee's Final Report should not be confused with the official Committee Comments to the rules. Also note that the Supreme Court does not adopt the Committee's Comments or the contents of the Committee's explanatory Final Reports.

title, if any, of the person on whom the complaint was served. The proof of service shall be filed with the original complaint.

B. When service is made by certified mail or comparable delivery method resulting in a return receipt in paper or electronic form, the return receipt shall be filed with the original complaint.

C. The appearance of a defendant in person or by representative or the filing by a defendant of a claim in the case shall be deemed a waiver of any defect in service but not a waiver of a defect in venue.

D. If the complaint is not served on the defendant in time to permit holding a hearing within 60 days of the filing of the complaint, the magisterial district judge shall dismiss the complaint without prejudice.

[E. Upon written request of the plaintiff, a complaint that has been dismissed without prejudice for failure to make service pursuant to subdivision D of this rule] **E.(1) When the complaint is dismissed without prejudice for failure to make service pursuant to paragraph D of this rule as to all defendants, upon written request of the plaintiff the complaint** may be reinstated at any time and any number of times. The date of reinstatement shall be the date upon which the request for reinstatement is filed.

(2) When the complaint has been filed against multiple defendants and subsequently dismissed without prejudice for failure to make service pursuant to paragraph D of this rule as to less than all defendants, any further action against an unserved defendant after a hearing on the merits or the entry of a default judgment must be initiated by the filing of a new complaint.

***Official Note*:** The provision concerning appearance not being a waiver of venue was inserted in **[subdivision]** **paragraph** C of this rule to prevent the concentration of business in the office of a favorable magisterial district judge. Also, the public cannot generally be expected to be aware of venue provisions. *See* Rule 302H regarding improper venue.

[Subdivision] **Paragraph** D is intended to prevent the accumulation of stale claims in the office of the magisterial district judge.

[Subdivision E] **Subparagraph E(1)** provides for the reinstatement, upon written request of the plaintiff, of a complaint that has been dismissed without prejudice for failure to make service under **[subdivision D]** **paragraph D against all defendants**. *Compare* **[Pa. R.C.P.]** **Pa.R.C.P.** No. 401(b). The written request for reinstatement may be in any form and may consist of a notation on the permanent copy of the complaint form, "Reinstatement of complaint requested," subscribed by the plaintiff. The magisterial district judge shall mark all copies of the reinstated complaint, "Complaint reinstated. Request for reinstatement filed on _____ (date)." If it is necessary to use a new form for the reinstated complaint, the reinstated complaint, except for service portions thereof, shall be an exact copy of the original complaint, although signatures may be typed or printed with the mark "/s/" indicating an actual signature. The language in **[subdivision E]** **subparagraph E(1)** that a complaint may be reinstated "at any time" will permit reinstatement after a faulty service without waiting for further proceedings in the case. Reinstatement must occur within the period of the statute of limitations from the date of the last filing or reinstatement. The cost for reinstating a complaint is specified in Section 1725.1 of the Judicial Code, 42 Pa.C.S. § 1725.1. In addition, there may be additional server costs for service of the reinstated complaint.

Subparagraph E(2) addresses the scenario involving multiple defendants when timely service is not made upon all defendants, resulting in a dismissal without prejudice as to some defendants. Subparagraph E(2) clarifies that the plaintiff may not reinstate the complaint after the hearing or entry of a default judgment in this circumstance, but must initiate an entirely new action by filing a new complaint, subject to the applicable fees and costs for a new filing.

FINAL REPORT[1]

Recommendation 1-2018, Minor Court Rules Committee

Amendment of Pa.R.C.P.M.D.J. No. 314

Reinstatement of Complaint

I. *Introduction*

The Minor Court Rules Committee ("Committee") recommended amendments to Rule 314 of the Pennsylvania Rules of Civil Procedure before Magisterial District Judges ("Rules"). Rule 314 addresses the reinstatement of a complaint following a dismissal without prejudice for failure to make timely service upon a defendant. The amendments distinguish the procedure for cases when the complaint is dismissed as to all defendants from dismissal for only some defendants.

II. *Background and Discussion*

Rule 314 addresses matters relating to service. Rule 314D provides for the dismissal of the complaint without prejudice for failure to make timely service on the defendant, and 314E provides for reinstatement of the complaint following a dismissal without prejudice for failure to make timely service.

The Committee received an inquiry regarding a dismissal without prejudice pursuant to Rule 314D and the ability to reinstate the complaint under Rule 314E when the complaint names multiple defendants, not all defendants have been served, the complaint is dismissed as to the unserved defendant(s), but the case moves forward against the served defendant(s), and proceeds to a hearing on the merits or a default judgment. In this scenario, a concern arises when the plaintiff subsequently locates an unserved defendant and requests reinstatement of the complaint pursuant to Rule 314E. The rule does not address this scenario, and reinstating an adjudicated case to proceed against the previously unserved defendants raises concerns with maintaining the integrity of the court's original judgment, including the appeal period applicable to the parties.

The Committee discussed the inquiry, and agreed that it would be appropriate to recommend the amendment of the procedures set forth in Rule 314E to distinguish between scenarios when the complaint has been dismissed as to all defendants and when the complaint has been dismissed as to less than all defendants.

III. *Rule Changes*

The Committee recommended amendment of Rule 314 by expanding Rule 314E into two subparagraphs. Sub-

[1] The Committee's Final Report should not be confused with the Official Notes to the Rules. Also, the Supreme Court of Pennsylvania does not adopt the Committee's Official Notes or the contents of the explanatory Final Reports.

paragraph E(1) provides that when the complaint is dismissed without prejudice as to all defendants for failure to make timely service, the complaint may be reinstated. Subparagraph E(2), in contrast, provides that when the complaint has been dismissed without prejudice for failure to make timely service as to less than all defendants, any further action against a previously unserved defendant must be initiated by filing a new complaint. The Official Note provides that the new action in subparagraph E(2) is subject to all applicable fees and costs for a new filing.

The Committee also recommended minor stylistic changes throughout Rule 314.

[Pa.B. Doc. No. 18-678. Filed for public inspection May 4, 2018, 9:00 a.m.]

Title 255—LOCAL COURT RULES

BUTLER COUNTY

Clerk of Courts' Schedule of Fees and Costs; Misc.; Administrative Doc. No. 1-2018

Order of Court

And Now, this 12th day of April, 2018, upon consideration of the Clerk of Courts' Petition to Increase Fees and Costs Pursuant to 42 Pa.C.S.A. § 1725.4 *It Is Hereby Ordered, Adjudged* and *Decreed*, that:

1. The revised fee schedule submitted by the Clerk of Courts of Butler County, Pennsylvania, a copy of which follows hereto and incorporated herein, is approved.

2. The revised fee schedule approved by this Order of Court shall be effective on May 1, 2018.

3. The Clerk of Courts is hereby directed to immediately cause the publication of the revised fee schedule in the *Butler County Legal Journal* once a week for two (2) successive weeks, and to file a copy of the Proof of Publication of the advertisement at the previously listed term and docket number.

4. The Clerk of Courts shall file one (1) certified copy hereof with AOPC and distribute two (2) certified copies plus a diskette to the Legislative Reference Bureau for publication in the *PA Bulletin*.

5. The Clerk of Courts is to distribute a copy of the fee schedule to each of the Judges of the Court of Common Pleas of Butler County and to the Butler County Bar Association.

6. Nothing contained herein shall prevent this Court to further revise the fee schedule approved by this Order of Court upon proper application made in accordance with law.

By the Court

MARILYN J. HORAN,
Judge

Clerk of Courts' Petition to Increase Fees and Costs Pursuant to 42 Pa.C.S. § 1725.4

And Now, comes Lisa Weiland Lotz, Clerk of Courts of Butler County, by and through Leo M. Stepanian II, Esquire, Solicitor, and respectfully petitions this Court as follows:

1. Petitioner is the duly elected Clerk of Courts of the Common Pleas Court of Butler County, Pennsylvania.

2. Butler County is a county of the fourth class.

3. Act 36 of 2000 provides in pertinent part:

> The amount of any fee or charge increased pursuant to paragraph (1) may be increased every three years, provided that the amount of the increase may not be greater than the percentage of increase in the Consumer Price Index for Urban Workers for the immediate three years preceding the last increase in the fee or charge.

42 Pa.C.S. § 1725.4(a)(2).

4. The Clerk of Courts last sought approval for and this Court last granted approval for an increase in the fees and costs charged by the Clerk of Courts in March 2015.

5. Pursuant to 42 Pa.C.S. § 1725.4(a)(2), the Clerk of Courts may request, and the President Judge may approve, an increase in the fees and costs charged by the Clerk of Courts based upon the increase in the Consumer Price Index for the period from July 2011 to June 2013.

6. Based upon the Consumer Price Index for Urban Workers (Urban Wage Earners and Clerical Workers), the Consumer Price Index has increased 3.45% (July 2011 to June 2013).

7. Following hereto as Exhibit "A" is a proposed fee bill for the Clerk of Courts of Butler County, Pennsylvania that takes into account the increase in the Consumer Price Index as previously set forth.

Wherefore, the Clerk of Courts of Butler County, Pennsylvania respectfully requests this honorable Court to authorize and adopt the schedule of fees and costs as proposed hereby.

LEO M. STEPANIAN, II,
Solicitor for the Clerk of Courts

Exhibit "A"

BUTLER COUNTY CLERK OF COURTS' FEE BILL (Effective 5/1/18)

Criminal Filings

Misdemeanor and Felony Case During or After Trial	$220.00
Misdemeanor and Felony Case Before Trial (Plea or ARD)	$164.50
Summary Case	$33.75
Juvenile Case	$21.75

Appeal Fees

Summary Appeal/Nunc Pro Tunc Filing Fee (Non-Refundable)	$61.00
Appellate Court Appeal (Payable to Clerk of Courts)	$66.25
Appellate Court Appeal (Check Payable to Superior/Supreme/Cw. Court)	Current Rate
Liquor Control Board Appeals	$21.75

Bench Warrant/Bail Related Fees

Processing all types	$21.75
Fee per dollar, for the first $1,000 .0525	$54.50
Fee per dollar, for each additional $1,000 .018	$18.75
Bail Forfeiture	$21.75
Bail Piece (Includes Certified Copy to Bondsman)	$33.75
Bench Warrant (Includes Certified Copy to Sheriff)	$33.75

Miscellaneous Filings/Fees

Automation Fee for Clerk of Courts' Office (All initiations—42 Pa.C.S.A. 1725.4(b))	$5.00
Certified Copy	$11.00
Constable—Bond/Oath/I.D. Card	$21.75
Copies (per page)	$0.50
Criminal Search (per name)	$21.75
Exemplifications	$21.75
Expungement (per case)	$73.50
Facsimile (fax) Fee	$5.50
NSF Check/Cancelled Money Order/Credit-Debit Card Reversals	$25.00
Private Detective (Individual) Bond/Oath per year	$100.00
Private Detective (Corporate) Bond/Oath per year	$150.00
Miscellaneous Case	$21.75
Road Docket	$21.75
Subpoenas	$4.25
File Retrieval From Iron Mountain	Current Rate

[Pa.B. Doc. No. 18-679. Filed for public inspection May 4, 2018, 9:00 a.m.]

Title 255—LOCAL COURT RULES

SCHUYLKILL COUNTY

Local Rule of Criminal Procedure No. 106, Continuances; AD 31-18

Order of Court

And Now, this 24th day of April, 2018, at 9 a.m., the Schuylkill County Court of Common Pleas hereby amends Local Rule of Criminal Procedure No. 106, Continuances, for use in the Schuylkill County Court of Common Pleas, Twenty-First Judicial District, effective 30 days after publication in the *Pennsylvania Bulletin*.

The Schuylkill County District Court Administrator is Ordered and Directed to do the following:

1) File one (1) copy of this Order and Rule with the Administrative Office of the Pennsylvania Courts via email to adminrules@pacourts.us.

2) File two (2) paper copies of this Order and Rule and (1) electronic copy in a Microsoft Word format to bulletin@palrb.us with the Legislative Reference Bureau for publication in the *Pennsylvania Bulletin*.

3) Publish the local rule on the Schuylkill County Court website at www.co.schuylkill.pa.us.

4) Incorporate the local rule into the set of local rules on www.co.schuylkill.pa.us within thirty (30) days after publication in the *Pennsylvania Bulletin*.

5) File one (1) copy of the local rule in the Office of the Schuylkill County Clerk of Courts for public inspection and copying.

6) Forward one (1) copy to the Law Library of Schuylkill County for publication in the *Schuylkill Legal Record*.

By the Court

WILLIAM E. BALDWIN,
President Judge

RULES OF CRIMINAL PROCEDURE

Rule 106. Continuances.

All motions for continuance of trial shall be in writing, on forms approved by the Court and served on the opposing party. A motion by the Defendant must be signed by defense counsel or by a pro se Defendant. All such motions shall be heard by the Court each Criminal Term on the date and at the time established by the published Court Calendar.

The Commonwealth must be represented at the hearing for all continuance motions.

The presence in Continuance Court of the Defendant and his or her counsel is only required in response to a Commonwealth motion for continuance when the Defendant opposes the motion; however, lack of opposition from the Defendant will not automatically result in the Commonwealth's motion being granted.

A Defendant who files a motion for continuance pro se must appear in Continuance Court, at which time the Court shall advise the Defendant of his or her rights pursuant to Pa.R.Crim.P. 600 before hearing the motion for continuance.

The presence of a Defendant who is represented by counsel shall be excused at Continuance Court if the motion for continuance includes a certification by defense counsel, on a form approved by the Court, that counsel has explained to the Defendant his or her rights pursuant to Pa.R.Crim.P. 600 and the impact of a defendant receiving a continuance on those rights, and further certifies that the Defendant is in agreement with counsel's request for the continuance. If the continuance motion fails to include such certification, the Defendant must be present at Continuance Court.

[Pa.B. Doc. No. 18-680. Filed for public inspection May 4, 2018, 9:00 a.m.]

DISCIPLINARY BOARD OF THE SUPREME COURT

Collection Fee and Late Payment Penalty; 2018-2019 Registration Year

Notice is hereby given that in accordance with Pennsylvania Rules of Disciplinary Enforcement 219(d)(2) and 219(f), The Disciplinary Board of the Supreme Court of Pennsylvania has established the collection fee for checks returned as unpaid and the late payment penalty for the 2018-2019 Registration Year as follows:

Where a check in payment of the annual registration fee for attorneys has been returned to the Board unpaid, the collection fee will be $100.00 per returned item.

Any attorney who fails to complete registration by July 31 shall be automatically assessed a non-waivable late payment penalty of $200.00. A second non-waivable late payment penalty of $200.00 shall be automatically added to the delinquent account of any attorney who has failed to complete registration by August 31.

SUZANNE E. PRICE,
Attorney Registrar

[Pa.B. Doc. No. 18-681. Filed for public inspection May 4, 2018, 9:00 a.m.]

DISCIPLINARY BOARD OF THE SUPREME COURT

Notice of Administrative Suspension

Notice is hereby given that the following attorneys have been Administratively Suspended by Order of the Supreme Court of Pennsylvania dated March 21, 2018, pursuant to Rule 111(b) Pa.R.C.L.E., which requires that every active lawyer shall annually complete, during the compliance period for which he or she is assigned, the continuing legal education required by the Continuing Legal Education Board. The Order became effective April 20, 2018 for Compliance Group 2.

Notice with respect to attorneys having Pennsylvania registration addresses, which have been administratively suspended by said Order, was published in the appropriate county legal journal.

Adelman, Cort Andrew
Marlton, NJ

El Fadl, Khaled Medhat Abou
Los Angeles, CA

Goldbas, Jacob Mervyn
Seattle, WA

Hafter, Jacob Louis
Las Vegas, NV

Hildebrand, W. B.
Haddonfield, NJ

Hogan, Mary Ellen
Tampa, FL

Johnson, III, Woodie
Fort Washington, MD

Kirschner, Meredith Anne
Haddon Township, NJ

Kuhlmann, Shirley Rose
Cambridge, MA

Mariam, Abiye
Seattle, WA

Masciocchi, Francis J.
Mount Laurel, NJ

McDonough, Sean M.
New Brunswick, NJ

Mullally, Kathe Flinker
Hull, MA

O'Connell, Robert Edward
Deerfield Beach, FL

Pascu, Paul Albert
Cherry Hill, NJ

Peace, Denise Ann
Kennesaw, GA

Porter, Marwan Emmett
Stuart, FL

Teitz, Corey Patrick
New York, NY

Tippett, John Milton
Wilmington, DE

Tipton, Kevin Thomas
Fairmont, WV

Wadhwa, Rubina Arora
Lansdowne, VA

Warren, Richard F.
Annandale, VA

SUZANNE E. PRICE,
Attorney Registrar

[Pa.B. Doc. No. 18-682. Filed for public inspection May 4, 2018, 9:00 a.m.]