Minutes of the
Committee on Judicial Information Policy
February 5, 2009

Those present: Hon. Marshall Berger, Ms. Elizabeth Bickley, Hon. David Borden, Mr. Timothy Callahan, Atty. Janice Calvi, Hon. Patrick Carroll, Atty. Jorene Couture, Atty. Joseph D'Alesio, Mr. P. J. Deak, Ms. Krista Hess, Professor Elizabeth Marsh, Hon. Aaron Ment, Atty. Louis Pace, Ms. Dalia Panke, Hon. Joseph Pellegrino (chair), Atty. Norman Roberts II, Atty. Kevin Shay, Mr. Donald Turnbull, and Atty. Elizabeth Yen.

The meeting was called to order at 1:15 PM by Judge Pellegrino.

1. Welcome – Judge Pellegrino introduced the new members of the committee. Upon motion and second, the minutes of the meeting of November 13, 2008 were then approved unanimously.

2. Presentation on Public Access to Court Records - Judge Ment then introduced Dr. Thomas M. Clarke, the vice president of Research and Technology at the National Center for State Courts. Dr. Clarke is a leading expert on privacy and was invited to provide the committee with an overview on how privacy and security issues related to access to court records are being handled nationally. The presentation covered issues, including the nature of a court record, privacy exceptions to access rules; the retroactive application of access policies; the identification of the standard case types and data types that are excluded from access (including adoption, mental health records); strategies for protecting identifying information, problems in the family law area; the competing interests and needs of data users; whether to implement a single access policy for all records or to treat electronic records differently from paper records; practical obscurity and redaction options; challenges in enforcing privacy policies; and identity theft.

   Dr. Clarke made the point that little consensus exists nationally in handling any of these issues. For example, some options on providing access include maintaining practical obscurity; placing the onus and liability for redacting information on the filer; or placing the onus and liability for redacting information on the clerk. Two counties in Florida, for example, employ a combination of automated redaction software and manual review of files. Maryland and Washington have made policy decisions that information is either open or closed, regardless of whether it is available online or at the courthouse. This policy caused both states to close some case types and data types that had previously been open at the courthouse. Also, the search capability provided varies from state to state for records displayed online, including the option to search by case number or party names, by attorney name, by case type, by judge, or by combinations of these options.

   Dr. Clarke also suggested that providing electronic records is inevitable and that courts have an obligation to protect the confidential data in those records. A combination of "before-the-fact" redaction by the filer, some type of "after-the-fact" redaction software, and an effective manual review policy would be an excellent means of protecting confidential information. Implementing this method of protecting confidential information will require a major cultural change. The Bar and self-represented parties would have to be given extensive training and education about the expectation of privacy in court records and the requirements for redaction in

order to make “before-the-fact” redaction effective. Courts would also have to rethink what personal identifying information is required to carry out the business of adjudicating cases.

Dr. Clarke also provided a best practices approach to protecting information that the public should not be permitted to see because of security issues, including identity theft. That approach requires an assessment of the threat, both as to the type of threat and its probability of occurring; an assessment of the potential business impact, including the cost of the threat and the cost of mitigating the threat; and a prioritization of the security controls needed, based upon the assessments. For example, the most probable threat that would result in the highest cost and be the least expensive to prevent would be addressed first. It is impossible to eliminate all possible exposure, but what the courts should do is to make the cost of obtaining the information more expensive than its resale value. He also suggested implementing commonsense controls over what is made available from court records online, including redacting social security and financial account numbers and limiting database wide searches of electronic case files without prior redaction.

3. Questions and Answers – The discussion included the nature and handling of exhibits; methods of posting records online, including “read only” access, to make it difficult to copy or transmit these records; instituting levels of search capability; determining policy choices on availability of records in all forms; the potential risks of relying on current redaction software programs; the use of automated redaction coupled with manual review; methods used by data miners or others to circumvent limits placed on search capability and data gathering; the availability of bulk data and the potential revenue resulting from providing that data; problems experienced by other states that had to remove records that had been posted online; and the difficulty in identifying the source of stolen data in identity theft situations.

   Judge Pellegrino expressed the committee’s appreciation to Dr. Clarke.

4. Future Meetings – The next meeting of the Committee on Judicial Information Policy will be in early April.

The meeting adjourned at 3:10 PM.