PRIVACY POLICY SUBCOMMITTEE MEETING NOTES
11 May 2006

Present at the ninth meeting of the IIJIS Privacy Policy Subcommittee were:

- Robert Boehmer, Institute for Public Safety Partnerships;
- Carol Cates, Illinois State Police;
- Kathy deGrasse, Illinois State Police;
- Paul Fields, Law Office of the Cook County Public Defender;
- James Ford, Office of the Circuit Court Clerk of Cook County;
- Carol Gibbs, Illinois State Police;
- Chad Grogman, Illinois State Police;
- Jim Hickey, Chicago Police Department;
- Robert Howlett, Illinois Sheriffs' Association;
- Ronald Lewis, Illinois Public Defender Association;
- Terry Mutchler, Office of the Illinois Attorney General (via telephone);
- Wil Nagel, Illinois Criminal Justice Information Authority;
- Steve Neubauer, Elmhurst Police Department;
- Gerald Nora, Cook County State's Attorney's Office;
- Jim Redlich, Office of the Illinois Attorney General;
- Marcel Reid, Illinois State Police, Bureau of Identification;
- Leslie Reis, The John Marshall Law School;
- Lyn Schollett, Illinois Coalition Against Sexual Assault;
- Art Sebek, Illinois State Police;
- Scott Slonim, Law Office of the Cook County Public Defender; &
- Jennifer Walsh, Office of the State Appellate Defender (via telephone).

Introductory comments and organizational matters

Mr. Boehmer thanked everyone for attending the long session and outlined the goals of the meeting. He explained that during the morning session the members would identify any concerns regarding *Privacy Policy Guidance* that had not yet been brought to the group's attention. Once the issues were identified, the group would then prioritize them and begin resolution discussions. He added that during the afternoon session the group would assist the Illinois State Police by explaining some of their concerns regarding the I-CLEAR data warehouse initiative.

Mr. Nagel stated that the IIJIS initiative was highlighted in the National Governor's Association Issue Brief, Protecting Privacy in Integrated Justice Systems. Additionally, members were provided a copy of Professor Daniel Solove's *A Taxonomy of Privacy*. Mr. Nagel explained that the article offered a brief description of 16 privacy issues and the social goals protected (and thus the harms involved with breaching) each. A very brief summary of the lengthy article was provided to members.

Identification & Prioritization of issues raised by *Privacy Policy Guidance Volume 1*

After a brief recap of the last meeting, the subcommittee discussed their concerns and made the following recommendations:

(1) Consider adding a supremacy clause or disclaimer that explains that the requirements contained in the *Privacy Policy Guidance* document are recommendations that are not intended to expand or diminish rights. Furthermore, the clause should explain that the law is constantly changing and that the law, not the document, controls appropriate information sharing standards.

(2) *Privacy Policy Guidance* should be an advisory document that contains a set of recommendations. It should not be a binding rule or policy. Specifically, it should explain which types of information sharing are mandated or prohibited by law. It should then explain which types of information sharing are permissible under existing laws. Finally, the document may include recommendations regarding rule changes and legislative amendments.

(3) The document should be used to discuss best practices, including those in information exchanges provided for by law and existing policies. It should serve as a starting point when a justice practitioner or member of the public needs to research an information sharing issue.

(4) *Privacy Policy Guidance* may eventually be useful as a "tie-breaker" in the development of detailed interagency agreements between participants in an integrated justice information system. Keep this potential use in mind when drafting the document and deliberating on its provisions.

(5) The transparency provisions in *Privacy Policy Guidance* should only reflect existing laws (e.g., Freedom of Information Act and its included exceptions). The document should not create a new public service nor should it provide overly broad access and review provisions to the point where individuals are granted access to every document in which their name appears. Members recommended that the policy distinguish between incidental references and instances where the individual is identified as a suspect or offender.

(6) The change from "probable cause" to "authority to arrest" in Section 201 should be reversed. Continue to use "probable cause" language but distinguish between a police officials' subjective belief and a court's finding that probable cause exists.

(7) *Privacy Policy Guidance* may need to explain how advancing computer technologies may thwart existing rules. For instance, Internet archives may contain records of convictions that have been appropriately expunged from an individual's criminal history record. Similarly, victim's in Illinois have received some level of privacy protection through existing practices (but not necessarily through Illinois law). New technologies may lessen these protections and the document should identity these threats to victim privacy.

(8) A best practice may be to include, in every written dissemination of data, the date of dissemination and the date the information was last updated or verified. It also may be a best practice to automatically deem certain types of information stale if they are not updated or verified within a fixed period of time.

(9) *Privacy Policy Guidance* should not attempt to regulate court filings. Even if so, Section 207(c)(2) is probably too vague to be useful.

(10) Consider adding a "Charged" status between arrestees and convicted persons. This may be a separate status that permits or authorizes different levels of information sharing due to the individual's position in the criminal justice process.

(11) Postpone the research and deliberations regarding juror information until a future volume. The issues surrounding the accessibility and sharing of juror information was recently brought into the public interest in the trial of former governor George Ryan. It is likely that recommendations will be developed with regard to this issue and the group should review this work before developing its own recommendations.

Brainstorming session: Issues confronting Illinois State Police's I-CLEAR initiative

Subcommittee members assisted the Illinois State Police by identifying and briefly characterizing the following challenges that they felt should be addressed by an I-CLEAR information sharing policy.

[A] Collection of records – The mere collection of information regarding individuals implicates privacy concerns. This is because the collection of information about individuals is usually premised upon some reasonable suspicion that they are acting unlawfully. Privacy issues are raised when the government collects information about individuals for investigatory purposes absent any suspicion of criminal wrongdoing. **Developers of the I-CLEAR data warehouse must be aware that the mere collection of personally identifiable victim and witness information raises genuine privacy concerns.**

- **[1]** Factors should be identified to balance the amount of data collected to address privacy concerns while still meeting legitimate law enforcement needs.
- **[2]** In addition to the collection of records, the compilation of various types of data in the absence of suspicion can also raise privacy concerns.

[B] Retention periods – In the past, paper files were purged largely due to storage constraints. As electronic storage becomes dominant, there is less of a physical need to purge information. As such, the retention of electronic law enforcement data in a data warehouse environment becomes a privacy issue that must be balanced with public safety (e.g., crime fighting) concerns. **How long should data entered into the I-CLEAR data warehouse be stored?**

- **[1]** Several factors weigh into this determination:
  - **[a]** The level of trust that the public has that the justice system will maintain the confidentiality of the data and use it appropriately is a substantial factor. The lower the level of trust, the higher the public's desire may be to destroy the data.
  - **[b]** How the information will be used must also be considered. It is generally understood that the data would be used to conduct various forms of crime analysis (e.g., analyzing similarities in crimes to connect them to a common offender, identifying who is associating with whom to commit crimes, etc.)
  - **[c]** Determining whether certain types of data become stale. Staleness is just one of several data quality factors that may weigh into this balancing test.
  - **[d]** The ability of ISP to successfully maintain the confidentiality of data warehouse information.
- **[2]** Many privacy concerns are raised by the collection and maintenance of personally identifying victim information primarily because victims do not choose to participate in the justice system.

[C] Appropriate uses of I-CLEAR data – How government agencies use the data they collect is of significant concern to the public. **An I-CLEAR Information Sharing Policy should clearly identify appropriate uses of the information contained in the data warehouse.**

- **[1]** If the data warehouse will be used for data mining purposes, appropriate checks and balances should be developed to ensure that the data mining is conducted within the proper scope and with appropriate authority.

[D] Accountability – Ensuring that users and participating agencies are accountable for any misuse of the data warehouse was identified as a significant issue facing the I-CLEAR initiative. Furthermore, the administrator of the I-CLEAR data warehouse should also be accountable for enforcing and complying with any official information sharing policies developed for its use.

[1] Key to implementing accountability provisions is ensuring that the data warehouse maintain audit logs capable of monitoring users' queries.

[E] Establish "ownership" of the data – Clearly establishing which entities have authority over and bear responsibility for the data contributed to the data warehouse is of paramount importance. It is possible that the Illinois State Police, as the administrator of the data warehouse, will have a substantial role to play in this regard.

[1] Who will ultimately be responsible for the fulfilling the following data management concerns?

[a] Ensuring data is of proper quality.
[b] Identifying inaccurate data and correcting it.
[c] Ensuring that data is not misused.
[d] Establishing data retention periods.
[e] Enforcing laws, regulations, and policies concerning use of the data.
[f] Etcetera.

[F] Identify authorized users – Currently, the Chicago Police Department issues user logons to employees who work for law enforcement agencies that possess an Originating Agency Identifier (ORI) number. ORI numbers are unique identifiers assigned by the US Department of Justice for use with its National Crime Information Center (NCIC). **Should an individual have to meet certain requirements before he is authorized to access the I-CLEAR data warehouse? What should those requirements be?**

[G] Determine who is responsible for responding to subpoenas or FOIA requests for I-CLEAR data – Under the Freedom of Information Act, a public body that maintains or possesses a requested state record must respond to the request within 7 days. Illinois case law reveals that merely referring a requestor to the original source of the record does not relieve a public body of its obligation to respond to the FOIA request and that such a referral constitutes a denial under the act. There are several exemptions under which a public body can refuse to disclose a requested record. The members raised the following issues:

[1] FOIA laws apply to state records. Section 2 of the State Records Act defines state records as "all books, papers, digitized electronic material, maps, photographs, databases, or other official documentary materials, regardless of physical form or characteristics, made, produced, executed or received by any agency in the State in pursuance of state law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its successor as evidence of the organization, function, policies, decisions, procedures, operations, or other activities of the State or of the State Government, or because of the informational data contained therein…." *See* 5 ILCS 160/2. **Are the records contained in the I-CLEAR data warehouse state records?**

[2] Under the first exemption contained in FOIA, a public body does not need to disclose information that is protected from disclosure by law or administrative rule. **Can the Illinois State Police promulgate a rule that would exempt data contained in the I-CLEAR data warehouse from disclosure under FOIA?**

[3] There are times when copies of a single record are possessed by more than one agency. When this happens, one possessing agency may desire to withhold the requested report under an exemption while the other possessing agency may wish to disclose that same report or may not be eligible to invoke the exemption utilized by the first possessing agency. Some states'

freedom of information acts address this circumstance by permitting or requiring the second possessing agency to invoke the first agency's exemption. Illinois' FOIA does not contain a similar provision. **Should Illinois's FOIA be amended to include this provision? Should the Illinois State Police, as the administrator of I-CLEAR, and contributing agencies enter into a written agreement to consult in these circumstances?**

[4] Subpoenas are ordinarily served upon registered agents. **Who will be I-CLEAR's registered agent?**

[5] The Illinois State Police may wish to pursue several statutory amendments to better meet its needs with regard to the I-CLEAR data warehouse.

[H] Sharing of juvenile data – Members identified the sharing of juvenile data as a concern that should be addressed by an I-CLEAR information sharing policy. Generally, the Juvenile Court Act limits the commingling of juvenile justice data with adult criminal justice data. However, some members explained that improving the sharing of juvenile justice data among law enforcement might actually support the implementation of formal and informal station adjustment laws.

[1] Section 5-905(5) of the Juvenile Court Act requires the law enforcement records concerning juveniles to be maintained separate from the records of adults unless otherwise permitted by law. Juvenile records are maintained in the CHRI repository because Section 1-7(B)(2) of the Juvenile Court Act permits the commingling of CHRI records. I-CLEAR does not have any similar statutory authority. **How will I-CLEAR maintain juvenile justice records separate from adult records?**

[2] While similar to determining retention periods for adult justice information, Illinois does have some policies that protect juvenile offenders who do not recidivate as adults. **How long will juvenile justice records be maintained in I-CLEAR?**

[I] Destruction of data – I-CLEAR data warehouse plans call for "snapshots" of data from source systems. These snapshots serve to keep the data contained in the data warehouse current and accurate. **Will old snapshots be wiped or merely deleted?**

[1] Members advised that these snapshots might themselves be state records under the State Records Act.

[2] Destruction of data is also implicated in the error correction process.

[J] Revealing victim identities to users – Members discussed how victims' information is different than suspect information and that it might be appropriate to treat it differently in the data warehouse. However, it might be problematic to classify victims based upon the type of crime and then assign an access level based upon that classification. **Should victim identities be available to all I-CLEAR users?**

[1] Collection of victim identifying information in a local records management system is different than contributing that information to the data warehouse for broad dissemination.

[2] How much information is enough to identify an individual?

[K] Quality of I-CLEAR data – Data quality is an important concern of any integrated justice information system. Data quality takes on significant importance in the development of sound information sharing policies. For instance, if the data contained in an information system is of uncertain quality, it is likely that the sharing of that data will be more restrictive than if the data could be verified as accurate. Restricting the sharing of potentially inaccurate data limits the possibility that users will act upon erroneous information.

[1] To ensure that the data warehouse is a valuable source of information, data contributed to the data warehouse may need to be validated or verifiable. **Will guidelines be developed to reduce the amount of inaccurate data contributed to the data warehouse?**

[2] Data quality concerns are not limited to the mere contribution of the data. Members explained that the quality of the association of the data was also an important factor to consider. This

also goes to the public's and the user's trust in the I-CLEAR system. **Will guidelines or rules be developed that regulate how the data will be compiled/associated in response to a user's inquiry?**

[L] Identify potential liabilities – Members highlighted some areas that the I-CLEAR system may want to consider as it develops its policies. The following areas have the potential to expose the I-CLEAR system to public scrutiny and criticism and should be addressed preemptively.

- **[1]** Identify any concerns with commingling fingerprint-based information with name-based records.
- **[2]** Identify the nature of the harms that can potentially be caused by misuse of information contained in the data warehouse.
- **[3]** Anticipate possible future abuses of data mining technology. Specifically consider its uses in background checks as opposed to criminal investigations. Today, time constraints limit these types of abuses.
- **[4]** Learn from the mistakes MATRIX made.

[M] Access & review permissions – Individuals already have the right to access and review their criminal history record information contained in the state's criminal history repository. However there are several types of justice information that do not provide such a right including state's attorney files and some IDOC records. Compiling police incident reports from multiple jurisdictions and analyzing them for investigative leads is a new and expansive use of the data collected in these reports. **To what extent, if any, should individuals be afforded the right to review and challenge police incident report information compiled into a data warehouse?**

- **[1]** Identify the factors that can help make this determination
  - **[a]** What other types of government information (justice and non-justice) are currently subject to access and review requirements?
  - **[b]** Should instances of identity theft impact an individual's access and review rights?
  - **[c]** Should the right extend to incidental references to an individual (i.e., the individual was named in a narrative as a possibly involved but is not formally described as a victim, suspect, or witness.)? Should the right be limited to only those individuals labeled by their government as suspects or offenders?
  - **[d]** There would probably have to be a limitation on this right where it would interfere with a pending investigation.
  - **[e]** Should the right to access and review, if granted, also include a listing of individuals and agencies to whom the information was previously disclosed?