Recommendations contained in Privacy Policy Guidance, Vol. 1

This document lists the recommendations contained in the pages of the first volume of the Privacy Policy Guidance series. This list is being provided to facilitate the Privacy Policy Subcommittee's consideration and deliberations considering submission of the document to the full Implementation Board.

Whether information collected about people no longer suspected of having committed a crime should be retained for use in subsequent investigations. [Page 9]

> **Recommendation:** Sound privacy protections concerning the accessibility of suspect names and associations, even among police officials, may be consistent with more efficient investigations by helping investigators hone their inquiries and make them more productive. The subcommittee recommends that this issue be discussed in greater detail as part of Privacy Policy Guidance, Volume 2, which will specifically address the privacy interests implicated by increased sharing of digital police incident report data.

Computer technologies may undermine Illinois's policy of limiting the public availability of compiled arrest histories. [Page 14]

> **Recommendation:** It may be advisable for the Illinois General Assembly to reexamine this issue and consider how collecting and sharing electronic arrest data may upset the balance between public oversight of the justice system and the privacy interests of those individuals who were arrested but not convicted.

Whether presentence investigation reports are public records or restricted to individuals identified in Illinois statutes. [Page 18]

> **Recommendation:** Presentence investigation reports are non-public records that are restricted to the individuals identified in Illinois statutes. The availability of presentence reports is a significant issue because state and local justice agencies are interested in improving the amount of information made electronically available to decision-makers. Restrictions on the accessibility of the information contained in presentence reports must be adhered to in any integrated justice information system developed in Illinois.

Whether probation officials may provide probationer information to police officials to warn of threats of violence. [Page 22]

> **Recommendation:** Where a probationer makes a specific threat of violence directed against a specific and readily identifiable victim, probation officials may share the probationer's identity and the substance of the threat with the potential victim and police officials. The General Assembly should revisit probation officials' ability to share information about probationers that may directly impact police officers' safety.

Whether privacy issues are implicated in the sharing of non-identifying incident information across jurisdictions. [Page 32]

> **Recommendation:** The subcommittee recognizes the significance of crime analysis to the justice system and recommends that integrated justice information

systems take steps to make incident information that does not personally identify the victim available to practitioners for crime analysis purposes.

Whether victims' identities and victimization histories should be made widely available across jurisdictions. [Page 33]

Recommendation: The subcommittee warns that the broad dissemination and use of victims' identities for investigative purposes may raise privacy concerns, especially among victims of sexual assault and domestic violence. Because of the breadth and vital importance of sharing victim information in the integrated justice context, the subcommittee recommends that this issue be considered at length in the second volume of the *Privacy Policy Guidance* series, which will focus on the privacy concerns that are created by the enhanced sharing of electronic police incident report information.

Whether witnesses' identities should be made widely available across jurisdictions. [Page 45]

Recommendation: The subcommittee warns that the broad dissemination and use of witnesses' identities for investigative purposes may raise privacy concerns not addressed under existing law. Because of the breadth and vital importance of sharing witness information in the integrated justice context, the subcommittee recommends that this issue be considered at length in the second volume of the *Privacy Policy Guidance* series, which will focus on the privacy concerns that are created by the enhanced sharing of electronic police incident report information.

Justice agencies should directly confront privacy risks created by integrated justice information systems [Page 48]

Chilling effects: To diminish these risks, integrated justice information systems should be as transparent as possible and subject to clearly defined limits and effective oversight.

Information processing risks: Careful consideration of the types and sources of data that will be collected and analyzed by an integrated justice information system can reduce data quality risks from source systems. To ensure the accuracy of the compilation process, sophisticated data matching algorithms and procedures for testing and monitoring the accuracy of data matches should be incorporated into the integrated justice information system.

Information dissemination risks: Developing procedures and technological tools that limit access to sensitive data can mitigate these risks. Additionally, tamper-proof audit trails combined with oversight in the form of real-time monitoring and subsequent analysis of system usage can provide a check on the dissemination risks posed by integrated justice information systems

Sound privacy principles for integrated justice information systems don't exist. [Page 51]

Recommendation: Because the Fair Information Practices (FIPs) don't meet the needs of an integrated justice information system, propose a set of privacy principles that permit justice officials to develop integrated systems and share data electronically while providing some procedural protections to individuals' whose information is being collected, analyzed, and shared.

(1) Justice information sharing policies, procedures, and practices will comply with all laws and constitutional requirements protecting individuals' privacy and civil liberties regarding the collection, use, and dissemination of their information.

(2) Justice information sharing policies, procedures, and practices will be made available to the public to ensure accountability for complying with privacy and civil rights laws.

(3) All instances of justice information sharing and data modification will be recorded to ensure accountability for the transactions.

(4) Every reasonable effort will be made to ensure that justice information is complete, accurate, and timely.

(5) Each individual is entitled to know, with limited and narrowly defined exceptions, whether information about him or her has been collected and maintained by the justice system and to review and challenge that information.

(6) Victims and witnesses of crime shall be treated with fairness and respect for their dignity and privacy throughout the justice system.