State of Illinois
Rod R. Blagojevich, Governor

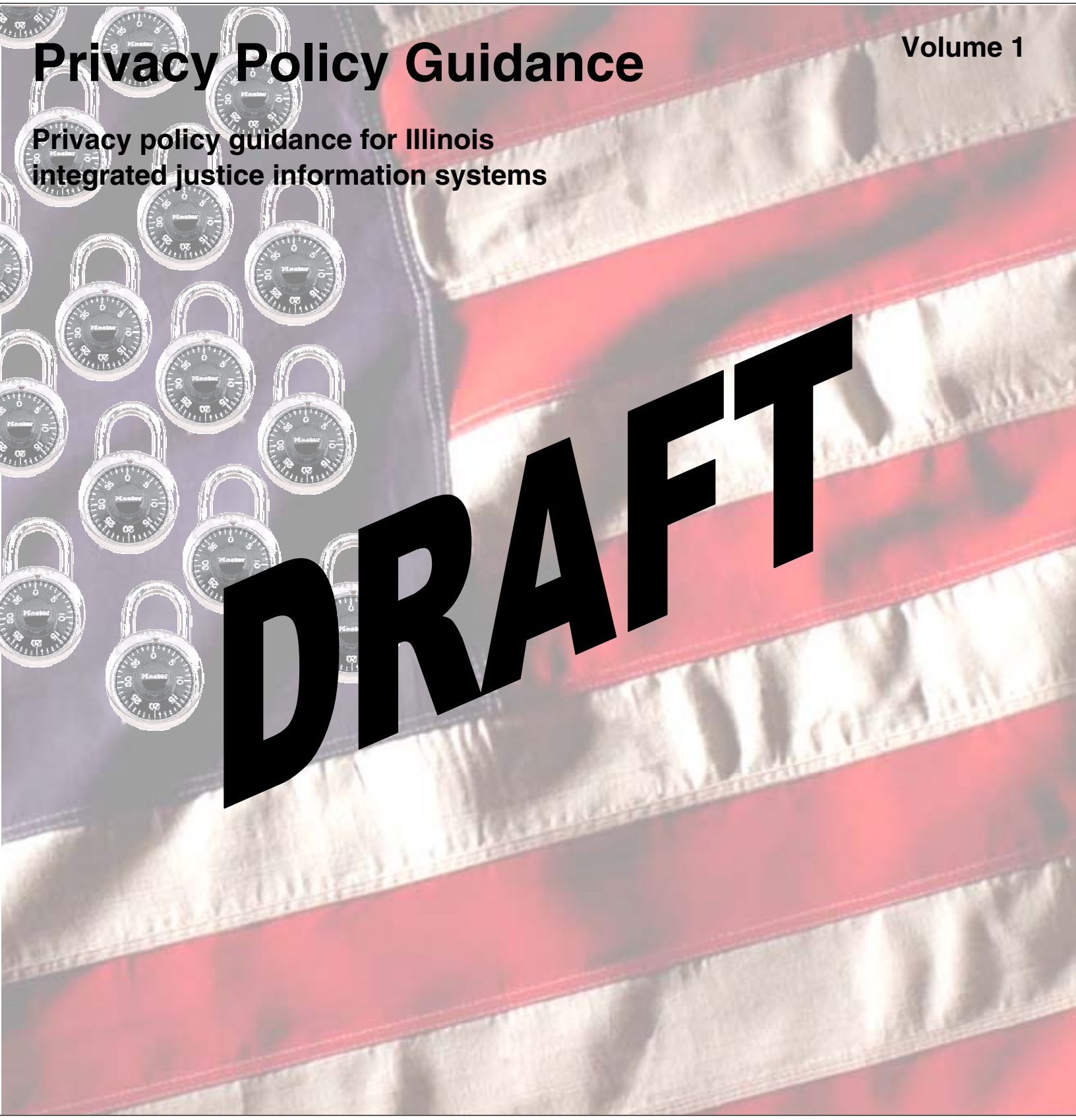
Draft: For discussion purposes only - Please do not disseminate

Illinois Integrated Justice Information System
Lori G. Levin, Chairperson

Privacy Policy Guidance

Volume 1

Privacy policy guidance for Illinois integrated justice information systems



IIJIS
Illinois Integrated Justice Information System

August 10, 2006

PRIVACY POLICY GUIDANCE FOR ILLINOIS INTEGRATED JUSTICE INFORMATION SYSTEMS

A Report of the Illinois Integrated Justice Information System Privacy Policy Subcommittee

Volume 1

August 2006

August 10, 2006

This project was supported by Grant 01-MU-CX-0031 awarded to the Illinois Criminal Justice Information Authority by the Bureau of Justice Assistance, U.S. Department of Justice. Points of view or opinions expressed in this document do not necessarily represent the official position or policies of the U.S. Department of Justice.

August 10, 2006

ILLINOIS INTEGRATED JUSTICE INFORMATION SYSTEM

Privacy Policy Subcommittee

120 S. Riverside Plaza
Suite 1016
Chicago, Illinois 60606

Tel: (312) 793-8550
Fax: (312) 793-8422
TDD: (312) 793-4170

www.icjia.state.il.us/iijis

Dear Members of the IIJIS Implementation Board:

Just over two years ago, the Privacy Policy Subcommittee was established to examine the privacy issues created by the integration of Illinois' justice information systems. Specifically, the subcommittee was charged with developing policies to ensure that the enhanced sharing of justice information, made possible through advancing information technologies, is carried out in accordance with Illinois law and its citizens' reasonable expectations of privacy. We are pleased to present to you our first in a series of six reports that will culminate in a comprehensive set of privacy policy recommendations that will govern the sharing of critical information between justice agencies and with the public.

The subcommittee agrees that the efficient and electronic sharing of information plays a critical role in the administration of justice. We believe that the following privacy policy recommendations protect privacy while facilitating the appropriate, effective, and efficient use of justice information.

While we have focused on existing laws and regulations, several issues required the subcommittee to make recommendations it believed were necessary to ensure meaningful privacy protections throughout the Illinois justice system. The recommendations fill the gaps in existing law and were designed to create a consistent, statewide standard to facilitate the appropriate sharing of justice information across local jurisdictions.

The subcommittee's deliberations have been substantive, wide-ranging, and collegial. These comments and the seriousness of our discussions reflect the importance and difficulty involved with developing recommendations of this nature.

The subcommittee's work was greatly aided by individualized meetings with practitioners from government agencies across all levels of state and local government, private industry, academia, and advocacy groups. We wish to take this opportunity to thank them for their time and for sharing their substantial knowledge with us. Finally, I express my gratitude for the commitment, cooperation, and diligent work of the subcommittee members.

Sincerely,

Robert P. Boehmer
Chairman

IIJIS Privacy Policy Subcommittee

Robert P. Boehmer, CHAIRMAN
Institute for Public Safety Partnerships

Kathleen deGrasse
Illinois State Police

Sidney DeLair
Illinois Probation and Court Services Association

Paul Fields
Law Office of the Cook County Public Defender

James Ford
Office of the Clerk of the Circuit Court of Cook County

James Hickey
Chicago Police Department

Robert Howlett
Illinois Sheriff's Association

Harold Krent
Chicago-Kent College of Law

Ronald Lewis
Illinois Public Defender Association

Michael McGowan
Office of the Chief Judge, Circuit Court of Cook County

Rachel McKinzie
Illinois Department of Corrections

Steve Neubauer
Illinois Association of Chiefs of Police

Gerald Nora
Cook County State's Attorney's Office

Marcel Reid
Illinois State Police

Leslie Reis
John Marshall Law School

Donald Rudolph
Illinois State Police

Lyn Schollett
Illinois Coalition Against Sexual Assault

Art Sebek
Illinois State Police

Nicole Sims
Office of the Clerk of the Circuit Court of Cook County

Michael Tardy
Administrative Office of Illinois Courts

Martin Typer
Illinois Association of Court Clerks

Jennifer Walsh
Office of the State Appellate Defender

Wil Nagel, *Illinois Criminal Justice Information Authority*
REPORTER

Acknowledgements

The subcommittee would like to acknowledge the valuable insights and observations contributed by the following individuals. This report would not have been made possible without their assistance.

Michael Glover, formerly Metro Chicago Health Care Council
John Jesernik, Illinois State Police
Lynne Johnston, Illinois State Police
Tammi Kestel, Illinois State Police
Allen Nance, formerly Probation and Court Services Association
Peggy Patty, formerly Illinois Coalition Against Domestic Violence
Deb Plante, Illinois State Police
James Redlich, formerly Office of the Illinois Attorney General
Scott Sievers, formerly Illinois Press Association
Scott Slonim, Law Office of the Cook County Public Defender

Contents

Introduction

The last several years have seen federal, state, and local justice agencies implementing new information systems designed to efficiently share critical information across agencies and jurisdictions. When information sharing works, it is a powerful tool. What these agencies and others like them are learning, however, is that the policy and legal issues confronting the integration of justice information systems can be more difficult than the technical ones.

Several technologies exist that help justice agencies exchange electronic data with one another. But clear and understandable rules for collecting, using, disseminating, and retaining the vast stores of data maintained by the Illinois justice system are lacking. This report is an attempt to establish a comprehensive set of practical privacy policy recommendations that simultaneously empower and constrain justice officials by explaining what data practices are and are not permitted.

But more than simply providing a statement of information sharing rules, this report is also an exercise in good government. How information is managed by the Illinois justice system should be made available to the public. This is so even if the information itself should not be publicly available. By clearly setting forth what information is collected, maintained, and shared by Illinois justice agencies, the public is invited to question those policies from a perspective that may be unavailable to those immersed in the administration of justice.

Transparency in government policy-making allows errors to be corrected through public criticism. Sometimes cogent and passionate arguments can persuade policy makers to see things in a truly new light. This report, and the others that will follow in the *Privacy Policy Guidance* series, are being placed before the public so that the information sharing policies of the State of Illinois can be improved – the ultimate goal of any integrated justice information system initiative.

Privacy Policy Subcommittee's Creation & Charge

In 2003, Governor Rod Blagojevich issued Executive Order No. 16, which created the Illinois Integrated Justice Information System (IIJIS) Implementation Board. This board is an intergovernmental effort dedicated to improving the administration of justice in Illinois by making complete, accurate, and timely information available to all justice decision-makers.

The Governor recognized the need to develop information systems that effectively support public safety efforts while protecting individuals from the inappropriate collection, use, or dissemination of their identities and sensitive information. As such, the executive order charged the Implementation Board with ensuring that the privacy and civil liberties of all citizens are enhanced rather than diminished by the expansion of integrated justice information systems in Illinois. The Privacy Policy Subcommittee, members of which are practitioners from the traditional criminal justice system, the press, schools of law, and victim services groups, was formed to fulfill this charge.

The Implementation Board sought to identify the privacy issues created by the enhanced collection, analysis, and sharing of information made possible with newly advanced computer technologies. Moreover, the board desired practical solutions to these issues in the form of a comprehensive set of privacy policy recommendations that could guide justice practitioners and system designers in the appropriate collection, use, and dissemination of electronic information throughout the Illinois justice system.

This report presents the Privacy Policy Subcommittee's first in a series of responses to these requests. It concentrates on the traditional justice information sharing because this phase underlies the day-to-day operation of the justice system. Specifically, this report: (1) identifies and discusses several of the privacy issues confronting the enhanced collection, analysis, and sharing of justice information made possible by advancing computer technologies; (2) sets forth the types of information sharing that are mandated by existing federal and state requirements; and (3) contains the subcommittee's recommendations concerning the proper treatment of justice information.

The establishment of the Privacy Policy Subcommittee has been very timely for Illinois. It is common for technologies to race ahead of public policy. Our nation has already seen pilot projects that help police officials generate leads and expedite investigations by using computer information management capabilities to more quickly access, share, and analyze records. We also have seen some of these projects shut down due to their failure to address the public's privacy concerns. It is the subcommittee's hope that publishing this report now will help ensure that Illinois justice agencies consider privacy issues contemporaneously with the development of their new information systems so that appropriate protections can be built into them.

How to utilize the Privacy Policy Guidance report

The Privacy Policy Subcommittee is developing its recommendations in a series of volumes for one primary reason – Illinois justice agencies are moving forward with their integrated justice systems now. It is the subcommittee's goal to provide these agencies with some privacy policy guidance while they are developing their systems, rather than after those systems have been competed.

This report begins with a brief overview of the privacy interests implicated by the enhanced collection, analysis, and sharing of information made possible by integrated justice information systems. The report then introduces the types of personally identifying information collected about actors in the criminal justice system. For each class of actor,[1] the report describes the types of information sharing that are mandated and permitted by existing federal and state requirements; it also sets forth the subcommittee's recommendations regarding how that information should be treated. The subcommittee chose to start with traditional justice information because it is essential for the day-to-day operation of the Illinois justice system.

The Privacy Policy Guidance report does have some limitations. First, the body of the report is intended to elucidate permissible justice information practices; it does not directly address the means through which individuals access that information. The report focuses on access to information, and not on whether an individual justice practitioner is authorized to review the information in paper form or electronically. Second, while the IIJIS initiative is intended to facilitate the sharing of information across the justice system, this report focuses on executive branch agencies. The subcommittee acknowledges that not all of the necessary safeguards are within the power of the executive branch. Nevertheless, out of respect for the co-equal nature of the judiciary, the subcommittee did not make recommendations concerning how courts should manage their information. Thus, this report does not contain recommendations regarding the information exchanges that take place under the supervision of a trial court.

Additionally, users of this document should consult their agency counsel for specific interpretations of federal and Illinois law. **As a set of recommendations, the *Privacy Policy Guidance* report is not intended to create, expand, or diminish individuals' rights with regard to the justice system's treatment of their information.** Federal and state laws are constantly changing and when a recommendation is in conflict with an existing or future law, the law ultimately controls the appropriate collection, analysis, and sharing of information throughout the justice system. Nevertheless, it is the subcommittee's hope that the recommendations contained in this document will be regarded as best practices by every justice agency in the State.

[1] It is possible for an actor to have more than one status or classification at the same time. For example, a witness could, upon further suspicion, become a suspect and an arrestee could already be on probation for a prior offense.

Privacy risks presented by integrated justice information systems

By enhancing the electronic sharing of data, integrated justice information systems help to ensure that justice practitioners have efficient and timely access to the information they need to make sound decisions. These systems also have the potential to centralize a substantial amount of personally identifiable information in the government, thereby creating risks to individuals' privacy and civil liberties.

Privacy risks presented by integrated justice information systems fall into three broad categories: (1) chilling effects and other surveillance risks; (2) information processing risks; and (3) information dissemination risks. The nature and extent of these risks are dependent upon the ways in which integrated justice information systems will be used, the types of data that they will analyze, and the amount of oversight that will be applied to their use.

Chilling effects

Individuals are already compelled to disclose a great deal of information to their government. The collection and aggregation of this information, discussed below, may have a chilling effect on social and political activities. Surveillance, whether it is real-time or simply the potential to track the behavior and associations of individuals, is a form of social control. People are likely to act differently if they know or expect that their conduct could be recorded and connected, whether correctly or incorrectly, to other individuals.

While some social control is desirable, there is a risk that individuals will become more cautious in the exercise of their protected rights of expression, protest, association, and political participation. For example, an individual who has been forced to provide information to the justice system may be less outspoken in his dissent of government policies or be reluctant to run for political office for fear that that information could be used in retribution. This may be especially true if there are few restrictions on the analysis or use of this information.

Information processing risks

Information processing risks arise from the storage, analysis, and use of data that has already been collected by the justice system.

Data aggregation

Several jurisdictions throughout the country have begun building integrated justice information systems that combine information about individuals from multiple sources. This aggregation of data implicates the chilling effects described above because it is a less direct form of surveillance that allows justice practitioners to track, albeit on a more limited basis, an individual's actions and associations. Additional problems may arise where the data compilation used to judge the individual is incomplete or results in a distorted portrait of the person because the information is disconnected from the original context in which it was gathered.

Data inaccuracy

Several factors contribute to the difficulties with ensuring that information about one person is correctly attributed to that individual and only that individual. The variety of ways in which a person's name can be recorded, the ability to change one's last name, and the number of people who may share the same name can raise significant challenges to connecting information to the correct individual. These issues, and many other facets of data quality, create the risk that a justice practitioner using an integrated justice information system may target one individual because of acts committed by another.

Information dissemination risks

Any information system is open to abuse or misuse by those authorized to access its contents. For example, a Los Angeles detective illegally ran a computer background check on a little league baseball coach he didn't like.[2] In Florida, a sheriff used a restricted database to obtain the address of a woman who described the sheriff as being too fat for basic police work in a letter to the editor.[3]

These abuses damage the relationship between citizens and their government because the breach of confidentiality is a betrayal of the public's trust. Additionally, the unintentional disclosure of the data contained in integrated justice information systems can threaten people's security by making them more vulnerable to physical, emotional, financial, and reputational harms. For example, many people have good reasons to keep their addresses secret, including victims of stalking and domestic violence attempting to hide from those who threaten them, police officials and prosecutors concerned about retaliation from criminals, and doctors who perform abortions desiring to protect their families' safety.

Conclusion

Integrated information systems are reducing the government inefficiencies that historically protected individual rights from centralized state power. While the concentration of personally identifying information raises concerns that citizens may be chilled in the exercise of their First Amendment rights, the literature reveals that there is also substantial fear that data related to an individual will be mismanaged or misinterpreted with real-world consequences to that person. Since integrated justice information systems are being developed throughout the nation, it is vital that jurisdictions recognize these privacy risks and develop meaningful policies that address these concerns. It is hoped that the findings and recommendations that follow will assist jurisdictions with this process.

Sources

- Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (Jan. 2006).
- Technology and Privacy Advisory Committee, U.S. DEP'T OF DEFENSE, Safeguarding Privacy in the Fight Against Terrorism (March 2004)
- K. A. Taipale, *Technology, Security And Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 7 YALE J.L. & TECH. 123 (2005).

[2] Report: LAPD let internal cases slide, CNN.com (May 19, 2003) http://www.cnn.com/2003/US/West/05/19/police.corruption.ap/.

[3] Sheriff apologizes to woman who described him as too fat, Local6.com (April 7, 2005) http://www.local6.com/print/4354943/detail.html.

Findings and recommendations regarding the sharing of information concerning actors in the justice system

In conducting the research to fulfill its charge, the subcommittee found that the State of Illinois had already made countless decisions concerning the collection, use, and sharing of justice information. These decisions exist in the form of statutes, regulations, and case law. This portion of the report attempts to compile Illinois's existing policy choices and present them in an organized and understandable manner.

The following pages also reveal instances where existing requirements either overlook a given information sharing practice or fail to provide what the subcommittee considered appropriate privacy protections. Where appropriate, the subcommittee identified these issues and formulated recommendations to address the privacy concerns implicated by the type of information being considered. Most of the recommendations are rooted in existing law and guided by the principles articulated by federal and Illinois case law. But some recommendations reach out beyond these existing requirements; this is because some legitimate privacy concerns may be implicated in circumstances not yet recognized by the law.

It is hoped that the findings and recommendations contained in this part of the report will help guide state and local justice agencies in the development of sound privacy and information sharing policies.

1. Information concerning suspects

It is necessary to distinguish between members of the general public, suspects, and arrestees. A member of the general public becomes a suspect when a police official reasonably infers from the circumstances that the person is committing, is about to commit, or has committed a crime.[4] Once a suspect is arrested, he is deemed an arrestee and his information should be treated as discussed in the next section, *Information concerning arrestees*.

The following discussion refers to suspects who are reasonably suspected of committing an offense but are not subsequently arrested. A suspect may avoid arrest where an investigator clears him of suspicion. Other times, an investigator may not be able to compile enough evidence to justify arresting the suspect. Police officials[5] collect information about suspects to further the investigation of a crime and ultimately to determine if probable cause exists to arrest and charge an individual with the commission of that or any other crime that comes to an investigator's attention.[6]

[4] The standard established in *Terry v. Ohio*, 392 U.S. 1 (1968) is codified in the Illinois Code of Criminal Procedure at 725 ILCS 5/107-14.

[5] "Police officials" is a term used throughout this report to broadly refer to peace officers including, but not limited to, federal law enforcement officials, state police, municipal police, and sheriffs.

[6] There was concern among some members of the subcommittee about this report's use of the phrase "probable cause." This concern arose primarily because probable cause has multiple meanings in the Illinois justice system. Specifically, there is a distinction between a police official's reasonable, subjective belief that probable cause exists

Mandatory information practices

(1) Police must collect suspect information – Police officials have a statutory duty to investigate crimes and criminal conduct. To fulfill this responsibility, police officials identify suspects and collect personally identifiable information about them.[7]

Prohibited information practices

(1) Police cannot provide suspect information to the public, generally – Information that personally identifies suspects is not available to members of the general public unless the suspect poses a danger to the community. Where a suspect poses a danger to the community, Illinois law permits, but does not require, the public release of a suspect's personally identifying information.

Commentary

The disclosure of police officials' investigatory records may seriously hamper enforcement efforts by discouraging or compromising confidential informants and disclosing the existence, targets, or methods of investigation. Although not fully codified by statute or rule, Illinois recognizes a limited privilege for law enforcement investigatory information.[8] This recognition is found in Section 7 of the Illinois Freedom of Information Act, which exempts from inspection law enforcement records that would: (a) interfere with pending or actually and reasonably contemplated proceedings; (b) disclose the identity of a confidential source; (c) disclose unique or specialized investigative techniques; (d) endanger the physical safety of any person; or (e) obstruct an ongoing investigation.[9] The privilege is also apparent in Illinois' policy to restrict public access to records of those individuals who have not been found guilty of a criminal offense by a court of law.[10] Restricting the disclosure of investigatory information serves to preserve the integrity of law enforcement techniques and confidential sources, to protect witnesses and police officials, to safeguard the privacy of individuals under investigation, and to prevent interference with the investigation.

Permissible information practices

(1) Police may collect suspect's name, address, and explanation – When a police official reasonably infers from the circumstances that an individual is committing, is about to commit, or has committed a criminal offense, the official may stop the suspect for a reasonable period of time and demand his name and address as well as an explanation of his actions.[11]

---

to arrest an individual and a court's finding that probable cause existed to support the arrest. For the purposes of this report, the probable cause standard is used as a triggering mechanism for the collection of personally identifiable information. As such, probable cause as used throughout this report refers to a police official's reasonable, subjective belief that probable cause exists to arrest an individual.

[7] *People v. Blitz*, 68 Ill.2d 287, 294 (1977).

[8] *In Re Daniels*, 240 Ill.App.3d 314, 324-331 (1st Dist. 1992).

[9] 5 ILCS 10/7(1)(c)(i), (iv), (v), (vii), (viii).

[10] *See* Illinois Criminal Identification Act, 20 ILCS 2630/3, /7. Section 3 distinguishes between the types of agencies that have access to arrest information and those that may only have access to conviction records. Section 7 provides that criminal history records maintained by the Illinois State Police shall not be made public except as provided under Illinois law. *See also*, Uniform Conviction Information Act, 20 ILCS 2635/2; 2635/5 (making conviction information, but not arrest data, publicly available).

[11] 725 ILCS 5/107-14 (providing "[a] peace officer, after having identified himself as a peace officer, may stop any person in a public place for a reasonable period of time when the officer reasonably infers from the circumstances that the person is committing, is about to commit or has committed an offense as defined in Section 102-15 of [the Code of Criminal Procedure], and may demand the name and address of the person and an explanation of his

(2) Police may collect public and law enforcement data about a suspect – When a police official reasonably infers from the circumstances that an individual is committing, is about to commit, or has committed a criminal offense, the official may investigate the suspect using any publicly available information and law enforcement information to determine if probable cause exists to arrest the individual.

Commentary

This discussion is limited to the collection of information about individuals who are reasonably suspected of some type of criminal conduct and merely documents current investigatory practices. It focuses on the types of information collected to establish whether probable cause exists. Police officials are not required by law to wait until they possess facts sufficient to form a reasonable inference that an individual is committing, is about to commit, or has committed a criminal offense before they can utilize law enforcement[12] or publicly available information.

There is a difference between publicly available information and the types of data that may appear in law enforcement data systems. For instance, publicly available information such as property ownership records and court case filings may not appear in an integrated law enforcement data system that contains police incident report information and outstanding warrants.

(3) Police may provide suspect information to prosecutors and other police agencies – Police officials may share any information they collect regarding suspects with police officials in other jurisdictions and prosecutors to aid in the determination of whether probable cause to arrest exists.

(4) Police may provide suspect information to the public, community safety exception – When police officials or prosecutors reasonably determine that a suspect poses a danger or threat of danger to the community, information about the suspect may be released to the public.[13] The release of information should be limited to identifying information and any other information that could reasonably protect the public from substantial harm.

Commentary

The subcommittee has not identified any statute or case law articulating what level of danger to the community may be required before information about a suspect can be disseminated to the public. Illinois Supreme Court Rules of Professional Conduct regarding trial publicity permit the dissemination of information concerning a suspect "when there is reason to believe that there exists the likelihood of substantial harm to an individual or to the public interest."[14] For example, a police department may provide a sketch or photo of a suspected rapist at large in the community.

---

actions. Such detention and temporary questioning will be conducted in the vicinity of where the person was stopped.").

[12] *People v. Blankenship*, 353 Ill.App.3d 322 (3d Dist. 2004).

[13] *See* ILL. R. OF PROF. CONDUCT 3.6(c)(6); (c)(7)(ii) (permitting an attorney to warn of danger concerning the behavior of a person involved, when there is reason to believe that there exists the likelihood of substantial harm to an individual or to the public interest and if the accused has not been apprehended, to provide information necessary to aid in the apprehension of that person).

[14] ILL. R. OF PROF. CONDUCT 3.6(c)(6). *See also* ILL. R. OF PROF. CONDUCT 3.8 (providing that "a public prosecutor or other government lawyer in criminal litigation shall exercise reasonable care to prevent investigators, law enforcement personnel, employees or other persons assisting or associated with the prosecutor in a criminal case

Issues identified

(1) Whether information collected about people no longer suspected of having committed a crime should be retained for use in subsequent investigations.

YES, INFORMATION ABOUT SUSPECTS SHOULD BE RETAINED FOR USE IN SUBSEQUENT INVESTIGATIONS. It has long been a basic tool of criminal investigators to start with known suspects and, with proper authorization, to look for information about them and the people with whom they interact. In integrated justice information systems, investigators may appropriately identify new individuals for investigation because of their connection with the suspect. Even though some of the connections revealed by an integrated justice information system might be tenuous, it is the role of detectives and police to exhaust investigative leads.

In some instances it may be appropriate for a suspect to become the subject of an intelligence investigation. Where this occurs, law enforcement agencies already must comply with federal criminal intelligence systems' operating policies.[15]

NO, INFORMATION ABOUT SUSPECTS SHOULD NOT BE RETAINED FOR USE IN SUBSEQUENT INVESTIGATIONS. When one considers the ease with which an individual can be considered a suspect, the retention and subsequent use of information collected about people who have been cleared of suspicion raises privacy concerns. In some instances a suspect may be cleared of suspicion. Simply restricting access to suspect information to police officials and prosecutors might not provide enough protection where an individual is repeatedly targeted for investigation on the basis of data that is either inaccurate (e.g., it reports that police officials still consider this person a suspect) or incomplete (e.g., it lacks the fact that the suspect was cleared of suspicion).

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.

2. Information concerning arrestees and those charged with crimes

An arrestee, for the purposes of this discussion, is an individual who was arrested and charged with the commission of a criminal offense but: (a) was not convicted; (b) was acquitted; or (c) had his conviction overturned on appeal. Once an arrestee has been convicted, he is deemed a convicted person for the purposes of this report and his information should be treated as discussed in the next section, *Information concerning convicted persons*.

---

from making an extra judicial statement that the public prosecutor or other government lawyer would be forbidden from making under Rule 3.6").

[15] These policies can be found at 28 C.F.R. Part 23 and include a five-year retention period that can be extended with proper validation. 28 C.F.R. § 23.20(h).

The justice system collects arrestees' personally identifying information for a number of reasons. An arrestee's information is collected to investigate the charges against him and establish the elements of the offense. The arrestee's information is also used to connect him to the facts surrounding his arrest so that a court can assess the police official's determination that probable cause existed to arrest the individual. In order to maintain complete and accurate criminal history records as well as to compile crime statistics, the Illinois State Police collect arrestee information.[16] Courts collect arrestee information to assess the need for financial security to assure the defendant's appearance at later proceedings and set conditions of release that will protect against the risks of nonappearance and the commission of new offenses.[17]

Mandatory information practices

(1) Police must collect arrestee information – Police officials must collect any information that: (a) helps to establish the identity of the arrestee; (b) justifies the determination of probable cause to arrest; (c) substantiates the charges; or (d) assists in the eventual prosecution of the arrestee.

Commentary

Information that tends to help establish an arrestee's identity includes his self-reported name, address, date of birth, and Social Security number; demographic information; photographs; DNA; and fingerprints. It can also include any unique identifiers assigned to the individual by government entities such as individual's actual Social Security number, the Illinois State Police SID number, and the FBI number.

(2) Pretrial services personnel must collect arrestee information – When an arrestee is to be presented for first appearance on felony charges, pre-trial services personnel must collect information concerning the arrestee's community ties, employment, residency, criminal record, and social background to assist the court in determining the appropriate terms and conditions of pretrial release.[18]

(3) Arresting police agencies must provide arrestee information to Illinois State Police – Police officials are required to share the identifying information and details regarding the felony and certain misdemeanor charges that they collect with the Illinois State Police for purposes of compiling a complete criminal history record.[19]

Commentary

Arrest information is an important component of criminal history record information. For instance, a court disposition will not be posted to a subject's record unless there is an underlying arrest; this is done to protect individuals from having a publicly available conviction mistakenly attached to their record. As such, arrest information is critical to decision making at virtually every juncture in the justice system because it is the foundation for the posting of subsequent criminal history record and transaction information concerning individuals.

To comply with the Illinois Criminal Identification Act, all police departments must submit to the Illinois State Police fingerprints, charges, and descriptions of persons arrested for violations of Illinois' penal laws.

[16] 20 ILCS 2630/2.1; 2630/8.
[17] 725 ILCS 185/7(b).
[18] 725 ILCS 185/7(a).
[19] 20 ILCS 2630/2.1(a); 2630/3(A).

(4) Police must provide arrestee information to prosecutors – Police officials must share any information they collect regarding arrestees with prosecutors to aid in the prosecution of the arrestees.[20]

(5) Police must provide arrestee information to probation and pretrial services personnel – Pretrial services personnel are required to monitor the arrest records of local police agencies to determine whether any supervised person has been formally charged with the commission of a new offense in violation of the terms of his conditional release. Upon request, police officials must share the identifying information and charging details regarding arrestees with pretrial service personnel.[21]

(6) Pretrial service personnel must provide information to parties and counsel of record – Pretrial services personnel must provide copies of the arrestee's pretrial services report to all parties and counsel of record.[22]

(7) Prosecutors must provide charging information to Illinois State Police – Prosecutors must provide charging details to the Illinois State Police for the purpose of maintaining complete and accurate criminal history records.[23]

(8) Prosecutors must provide information to defense counsel – Prosecutors must share facts underlying an individual's arrest and charges with defense counsel to protect the arrestee's right to a fair preliminary hearing and trial.

(9) Illinois State Police must provide arrest information to military officials upon request – The commander of any military installation in Illinois may access arrest information concerning anyone who seeks access to that installation's arms storage facility.[24]

(10) Illinois State Police must provide arrest information to other police agencies – Upon request, the Illinois State Police must provide arrest information to peace officers of the United States, of other states or territories, and to all peace officers of the state of Illinois.[25]

(11) Illinois State Police must provide arrest information to the Department of Children and Family Services for childcare licensing purposes – Upon request, the Illinois State Police must provide childcare license applicants' arrest information to the Department of Children and Family Services.[26]

[20] 725 ILCS 5/114-13(b).
[21] 725 ILCS 185/26 (providing that pre-trial services personnel must regularly monitor the arrest records of local police agencies).
[22] 725 ILCS 185/17.
[23] 20 ILCS 2630/2.1(b).
[24] 20 ILCS 2630/3(C).
[25] 20 ILCS 2630/3(A).
[26] 225 ILCS 10/4.1.

(12) Illinois State Police must provide arrest information to any agency authorized by law to receive it – Arrest information can be released to any individual or agency authorized to receive it under Illinois or Federal law.[27]

Commentary

This is a catchall finding that permits arrest information to be released pursuant to acts of Congress and the Illinois General Assembly. Currently, several statutes provide agencies access to arrest information.[28]

(13) Arresting police agencies must provide arrestee information to the news media – As soon as practicable within 72 hours of an individual's arrest, arresting police agencies must make available to the news media the following information:[29]

(a) The arrestee's identity (including his name, age, address, and photograph);
(b) Information relating to the charges for which he was arrested;
(c) The time and location of his arrest;
(d) The identification of the investigating or arresting agency;
(e) The amount of any bail or bond if the arrestee is incarcerated; and
(f) Any custodial information regarding the date and time of his receipt, discharge, or transfer from the arresting agency.

Commentary

Because the government's power to deprive persons of their physical liberty is among its most awesome, arrest records have always been available to the American press and the public as an essential check on this power. Courts and commentators have long recognized that the public availability of arrest information deters the government from making illegal arrests, promotes nondiscriminatory use of the government's arrest powers, promotes accurate fact finding in the government's investigations, and, perhaps most importantly, promotes the public confidence in the fairness of our justice system.

Some members expressed concern that this finding violated Rule 3.6 of the Illinois Rules of Professional Conduct, which prohibits trial publicity that could threaten an arrestee's right to a fair trial by polluting the potential jury pool. That rule identifies certain subjects that pose a serious and imminent threat to the fairness of judicial proceedings. The types of information released to the news media, however, are specifically provided for in Rule 3.6.[30]

[27] 20 ILCS 2630/7.

[28] *See*, among others, 5 U.S.C. § 9101 (federal agencies for positions of national security); 230 ILCS 10/22 (Illinois Gaming Board); 815 ILCS 5/11 (Securities Department of the Office of the Secretary of State).

[29] *See* 20 ILCS 2605/2605-302(a); 5 ILCS 160/4a; 50 ILCS 205/3b; and 110 ILCS 12/15 (note that these statutes set the time for which arrest information must initially be made available (within 72 hours); it does not provide for an availability expiration date).

[30] *See* ILL. R. OF PROF. CONDUCT 3.6(b)(6) (permitting disclosure of the defendant's arrested and the nature of the crime charged, provided it is explained that the charge is merely an accusation and that the defendant is presumed innocent); 3.6(c)(1) (permitting disclosure of the claim, offense, or defense involved in the case); 3.6(c)(7)(iii)(permitting disclosure of the fact, time, and place of arrest); 3.6 (c)(7)(iv) (permitting the identity of investigating and arresting officers or agencies and the length of the investigation to be released to the public); and 3.6(c)(4) (permitting public disclosure of the result of any step in litigation).

(14) Police agencies must make arrest blotters available to the public – Chronologically maintained arrest information must be made available by local police departments for public inspection and copying.[31]

Commentary

Traditionally, chronological arrest records were maintained in logs or ledger books as a routine business practice. However, in many departments, this practice has primarily been replaced by the generation of arrest blotter information from the data entered into a police department's records management system.[32] This means that arrest information that is potentially available to the public has the same life span as the arrest information accessible to the justice system.

Unless otherwise authorized by law, it is a civil rights violation for any employer to inquire into or use the fact of an arrest as a basis for any employment-related decision.[33]

Prohibited information practices

(1) No public access to arrest information contained in the criminal history repository – Arrest information maintained in the State's criminal history repository cannot be released to the public, absent an explicit statutory authorization.[34]

Commentary

Illinois law treats the arrest records maintained by the Illinois State Police as part of the State's criminal history repository differently than it treats arrest information maintained by local arresting agencies.[35] Certain arrest information maintained by local arresting agencies is required to be publicly available; arrest records maintained in the official repository, however, cannot be released to the public without specific statutory authorization.

This differing treatment of the same information is a legislatively enacted form of practical obscurity. The differing treatment of arrest information based upon where it is stored and whether it has been compiled with information from multiple agencies implements the balance struck between two differing policies – requiring public access to make certain the government isn't abusing its arrest powers on one hand, and ensuring that individuals aren't unnecessarily harmed by prior arrests lacking convictions on the other.

Permissible information practices

(1) Prosecutors and police officials may collect additional information concerning the arrestee – After establishing probable cause to arrest, a police officer or prosecutor may investigate the arrestee using any publicly available information, as well as law enforcement databases, to further the investigation and any prosecution of the arrestee.

---

[31] *See* 5 ILCS 140/7(1)(d)(i).

[32] The Iowa City, Iowa police department is an excellent example of this assertion. Their arrest blotter, limited to the past 30 days, can be found at http://www.iowa-city.org/police/arrests.asp.

[33] *See* 775 ILCS 5/2-103.

[34] 20 ILCS 2630/7.

[35] The phrase "local arresting agencies" includes the Illinois State Police when it acts as an arresting agency. *See* 20 ILCS 2605/2605-302(a).

(2) Police may provide arrest information to other police agencies – Police officials may share the information that they collect regarding arrestees with police officers in other jurisdictions.

(3) Defense counsel may access arrestee information in certain circumstances – When a court determines it will serve the interests of justice, defense counsel shall have access to arrest information concerning individuals other than their client.[36]

Commentary

Common defense counsel uses of an individual's arrest information include, but are not limited to, *voir dire*[37] and witness impeachment. Currently, the trial court decides whether it is appropriate to release an individual's arrest information to defense counsel.

(4) Arresting police agencies may withhold certain arrest information from the news media – Details other than the arrestee's identity and charge information can be withheld if their disclosure would:[38]

(a) Interfere with any pending or reasonably contemplated law enforcement proceedings;
(b) Place anyone's life in jeopardy; or
(c) Place a correctional facility at risk.

(5) Leaders of local units of government may examine their police agencies' arrest records – The leader of a local unit of government may examine arrest records maintained by the police department of that governmental unit for the purpose of investigating the conduct of the officers who participated in the arrest.[39]

(6) Police employers may consider arrest records for hiring purposes – Any government agency that employs police officers may access the arrest information of police applicants for use as a factor in determining the person's fitness for the position.[40]

(7) Courts may expunge or seal an arrestee's arrest records – Illinois law permits the court to order the sealing and expungement of arrest records under certain circumstances.[41]

(8) Expungement of pretrial service records – Two years after the date of the first interview with a pretrial services representative, the arrestee may apply to the chief circuit judge for an order expunging from the records of the pretrial services agency all files pertaining to the arrestee.[42]

---

[36] *See* e.g., *People v. Booker*, 274 Ill.App.3d 168 (1st Dist.1995) (holding the defendant's testimony that he was aware that victim had been charged with murder was admissible in murder prosecution, in which defendant raised claim of self-defense, as relevant to defendant's belief that he was in danger, though victim was acquitted of charge; defendant's knowledge of acquittal and effect such knowledge had on him would be proper areas for cross-examination, but did not preclude admission of testimony).

[37] *Voir dire* is the questioning of prospective jurors by a judge and attorneys in court. It is used to determine if any juror is biased or cannot deal with the issues fairly, or if there is cause not to allow a juror to serve (e.g., knowledge of the facts; acquaintanceship with parties, witnesses or attorneys; occupation which might lead to bias; prejudice against the death penalty; or previous experiences such as having been sued in a similar case).

[38] *See* 20 ILCS 2605/2605-302(a); 5 ILCS 160/4a; 50 ILCS 205/3b; and 110 ILCS 12/15.

[39] *See* 65 ILCS 5/3.1-35-20 and *People ex rel. Burgess v. City of Urbana*, 33 Ill. App. 3d 623 (4th Dist. 1975).

[40] 20 ILCS 2630/3(A); 20 ILCS 415/8b.1; 15 ILCS 310/10b.1.

[41] 20 ILCS 2630/5.

[42] 725 ILCS 185/24.

Issues identified

(1) Computer technologies may undermine Illinois's policy of limiting the public availability of compiled arrest histories.

BACKGROUND: The U.S. Department of Justice's regulations concerning criminal justice information systems do not prohibit a state from sharing the non-conviction, arrest information contained in its criminal history repository with the public. Rather, the regulations permit each state to decide whether its arrest information should be made available to the public.[43] Analysis of Illinois statutes reveals an intent on the part of the General Assembly to restrict access to compiled arrest records.[44] Nevertheless, the only way to ensure that the government isn't abusing its arrest powers (i.e., conducting secret arrests) was to provide the public with some limited access to arrest records. The General Assembly did this in the Illinois Freedom of Information Act[45] and the statutes granting news media certain access to arrest information within 72 hours of an arrest.[46]

INTEGRATED JUSTICE INFORMATION SYSTEMS MAY UPSET THE BALANCE BETWEEN PUBLIC OVERSIGHT AND THE PRIVACY OF INDIVIDUALS ARRESTED FOR, BUT NOT CONVICTED OF, COMMITTING A CRIME. Historically, it was extremely difficult, even for the justice system, to collect and compile these arrest records from the almost 2,000 police agencies across the state. As police and sheriff's departments provide arrest blotter information electronically, little stands in the way of an individual or corporation interested in compiling its own set of arrest histories and offering them for sale to the public.

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.

3. Information concerning convicted persons

Individuals who have been convicted of committing a criminal offense by a court of law are considered convicted persons for the purposes of this report; convicted persons are also called "offenders" throughout this report. Defendants placed on felony first offender probation under Section 10 of the Cannabis Control Act,[47] Section 410 of the Illinois Controlled Substances Act,[48] or Section 70 of the Methamphetamine Control and Community Protection Act[49] are not considered convicted persons for the purposes of the following discussion and their information should be treated in accordance with the sections of this report discussing arrestees' and probationers' information.

---

[43] 28 C.F.R. §§ 20.20(c); 20.21(b)(2).
[44] *See* 20 ILCS 2630/7 (restricting the disclosure of arrest records except as permitted by law) and 775 ILCS 5/2-103 (providing that unless otherwise authorized by law, it is a civil rights violation for any employer to inquire into or use the fact of an arrest as a basis for any employment-related decision).
[45] 5 ILCS 140/7(1)(d)(i) (requiring any chronologically maintained listing of arrests processed at the agency to be made publicly available).
[46] *Supra* note 29.
[47] 720 ILCS 550/10.
[48] 720 ILCS 570/410.
[49] 720 ILCS 646/70.

Once an individual has been convicted, the justice system collects his personally identifiable information to maintain complete and accurate criminal history records,[50] compile crime statistics,[51] assist the court in imposing an appropriate sentence,[52] and to help corrections officials make prisoner placement decisions. Criminal history records are maintained to implement sentence enhancement provisions for recidivists.[53] They are also used to ensure that civil disability statutes are properly applied. Civil disability statutes are laws that affect certain offenders', usually felons', rights to vote,[54] to serve as a juror,[55] to serve as a fiduciary,[56] or to hold public office.[57] These disabilities are also frequently referred to as collateral consequences of a conviction and may include selected employment disabilities[58] as well as sex offender registration.[59]

Mandatory information practices

(1) Court clerks must collect dispositions and sentences – Court clerk offices are responsible for documenting all dispositions and sentences in criminal cases.[60]

Commentary

The term "court clerks" is used to refer to the clerk of any trial- or appellate-level court in Illinois. It is the court clerk's duty to make and keep an accurate record of the proceedings in the court, including the dispositions of criminal cases.

(2) Court clerks must provide dispositions to Illinois State Police – Court clerk offices must furnish all reportable criminal dispositions and sentences to the Illinois State Police, within 30 days of the event, for purpose of compiling complete and accurate criminal history records.[61]

Commentary

Disposition information is collected for each separate charge and includes all: (a) judgments of not guilty, judgments of guilty including the sentence pronounced by the

[50] 20 ILCS 2630/2.1.
[51] 20 ILCS 2630/8.
[52] Absent a negotiated agreement, a judge cannot proceed to sentencing in a felony case without a presentence investigation (PSI). PSIs must be completed for felony sex offenders being considered for probation. Even though not required in misdemeanor cases, it is within the sentencing judge's discretion to order a PSI. 730 ILCS 5/5-3-1.
[53] *See*, among others, 720 ILCS 5/33B-1 (Habitual Criminal Act) and 730 ILCS 5/5-5-3(c)(8) (providing in pertinent part, "When a defendant, over the age of 21 years, is convicted of a Class 1 or Class 2 felony, after having twice been convicted in any state or federal court of an offense that contains the same elements as an offense now classified in Illinois as a Class 2 or greater Class felony and such charges are separately brought and tried and arise out of different series of acts, such defendant shall be sentenced as a Class X offender. This paragraph shall not apply unless (1) the first felony was committed after the effective date of this amendatory Act of 1977; and (2) the second felony was committed after conviction on the first; and (3) the third felony was committed after conviction on the second.").
[54] *See* 730 ILCS 5/5-5-5(c) (barring voting only during incarceration).
[55] While not specifically excluding convicted felons from jury service, the Jury Act requires jurors to be "[f]ree from all legal exception, of fair character, of approved integrity, [and] of sound judgment." 705 ILCS 305/2.
[56] *See* 755 ILCS 5/6-13(a), 5/9-1.
[57] *See* 730 ILCS 5/5-5-5(b)(barring one from holding public office during incarceration). *See also* Election Code, 10 ILCS 5/29-6, -10 (barring individuals convicted of mutilating election materials or perjury in an election matter from holding public office for a period of five years following completion of sentence).
[58] *See* 20 ILCS 415/8b.4 (candidates may be denied state employment for offenses involving "infamous or disgraceful conduct").
[59] 730 ILCS 150/1 *et seq.*
[60] *See* 705 ILCS 105/16-4.
[61] 20 ILCS 2630/2.1(c).

court, discharges, and dismissals; (b) appellate court orders which reverse or remand a reported conviction or that vacate or modify a sentence; (c) continuances to a date certain in furtherance of an order of supervision; and (d) judgments or court orders terminating or revoking a sentence of probation, supervision, or conditional discharge and any resentencing.[62]

(3) Probation officials must collect offender information, presentence investigation – When ordered to complete a presentence investigation, probation officials must collect information about the offender's:[63]

(a) History of delinquency or criminality;
(b) Physical and mental history and condition;
(c) Family situation and background;
(d) Economic status;
(e) Education;
(f) Occupation;
(g) Personal habits;
(h) Status since his arrest; and
(i) Eligibility for various sentencing alternatives.

Commentary

A presentence investigation report is an influential document in the sentencing of criminal defendants. The information contained in the report is a crucial aid to sentencing judges and provides vital information to probation and correctional officials in determining classification and supervisory decisions.

(4) Presentence investigation reports must be filed in a sealed envelope – Presentence investigation reports must be filed with the court in a sealed envelope.[64]

(5) Courts must provide conviction information to the public – Conviction and sentence information contained in court records is available to the public.[65]

(6) Illinois State Police must provide conviction information to the public – Upon request, the Illinois State Police must provide conviction information maintained in the criminal history repository to the public.[66]

Commentary

Despite the legislative proclamation that conviction information is public record, conviction records contained in the Illinois criminal history repository are not as publicly available as court records. For example, if a name-check request submitted to the Illinois State Police corresponds to more than one subject in the criminal history repository, the state police are prohibited from disclosing the information.[67] Although there are exceptions that allow the information to be disseminated in an emergency or "to administer criminal laws," these exceptions are not likely to apply to public requests for conviction information. As a result, requestors are asked to submit additional

[62] *Id.*
[63] 730 ILCS 5/5-3-2.
[64] 730 ILCS 5/5-3-4(a).
[65] 705 ILCS 105/16-6.
[66] 20 ILCS 2635/2(A); /5; /8.
[67] *See* 20 ILCS 2635/11(B).

information or fingerprints so that the request can be processed.[68] Presumably there is no similar chance of a fingerprint-based request corresponding to more than one subject because fingerprints (unlike names) are unique.[69]

The General Assembly has divided the burden of updating criminal history record information between the criminal history repository and the requestor. Within 30 days of a request for conviction information under the Uniform Conviction Information Act, the Illinois State Police has a duty to notify the requestor of any subsequently posted or modified convictions.[70] However, after that 30-day period has expired, the requestor has the duty to update the conviction information if he intends to use, rely on, or otherwise disseminate it.[71]

Prohibited information practices

(1) No public access to sealed and expunged conviction records – Conviction records that have been sealed or expunged pursuant to a court order shall not be publicly available.[72]

(2) Restricted access to presentence investigation reports – Presentence reports cannot be provided to anyone other than:[73]

(a) The sentencing court;
(b) The prosecutor and defense counsel;
(c) The appellate court hearing an appeal of the conviction or sentence;
(d) A department, agency, or institution having custody of the offender;
(e) Probation officials providing courtesy supervision when the offender is in another jurisdiction for a period of time;
(f) A probation department ordered by a court to conduct a presentence investigation of the offender;
(g) A mental health professional evaluating the offender under a petition brought pursuant to the Sexually Violent Persons Commitment Act;
(h) A prosecutor who is investigating a potential or actual petition brought pursuant to the Sexually Violent Persons Commitment Act;
(i) A facility, licensed or regulated by the Illinois Departments of Public Health, Public Aid, or Human Services, in which the subject of the report resides;[74]
(j) The Illinois Departments of Public Health, Public Aid, or Human Services, when the subject of the report resides in a facility regulated by one of these departments;[75] and
(k) Any individual by court order.

Permissible information practices

(1) Courts may expunge or seal an offender's conviction records – Illinois law permits the court to order the sealing and expungement of conviction records under certain circumstances.[76]

---

[68] *Id.*
[69] *See* 20 ILCS 2635/10.
[70] 20 ILCS 2635/12.
[71] 20 ILCS 2635/13.
[72] *See* 20 ILCS 2630/12 & /13.
[73] 730 ILCS 5/5-3-4(b); *see also* 730 ILCS 110/12(3), (4).
[74] 730 ILCS 110/12(11); 730 ILCS 5/3-14-1(c-5).
[75] 730 ILCS 110/12(11); 730 ILCS 5/3-14-1(c-5).
[76] 20 ILCS 2630/5.

Issues identified

(1) Whether presentence investigation reports are public records or restricted to individuals identified in Illinois statutes.

PRESENTENCE INVESTIGATION REPORTS ARE PUBLIC RECORDS. Circuits that make these presentence investigation reports part of the public record do so under what is interpreted as a conflict between Section 5-3-4 (restricting access to presentence investigation reports as discussed immediately above) and Section 5-4-1 of the Illinois Code of Corrections.[77] Section 5-4-1 provides that the trial judge must "specify on the record the particular evidence, information, factors in mitigation and aggravation or other reasons that led to his sentencing determination [and that the] full verbatim record of the sentencing hearing shall be filed with the clerk of the court and shall be a public record."[78] Under this interpretation, a presentence investigation report must be entered into the record because it was used to support the court's decision-making process.

PRESENTENCE INVESTIGATION REPORTS ARE NOT PUBLIC RECORDS. There are several arguments supporting the premise that presentence investigation reports are not matters of public record. First, the requirement in Section 5-4-1 that the judge set forth the basis of his sentence is permissive in nature;[79] thus, contrary to the above argument, the judge is not compelled to file the presentence investigation report in the publicly available court records. Moreover, the position that a presentence investigation report is a matter of public record undermines the requirement that presentence reports be filed in a sealed envelope and renders it superfluous.[80] Such an interpretation is contrary to accepted rules of statutory construction.[81]

Second, Section 5-3-4 provides very specific limitations on the accessibility of presentence investigation reports.[82] It is well settled that where there are two statutory provisions, one of which is general and designed to apply to cases generally, and the other which is particular and relates only to one subject, the particular provision must prevail and must be treated as an exception to the general provision.[83] Section 5-3-4, entitled "Disclosure of reports," is found in the article of the Unified Code of Corrections dealing with presentence procedure. That section sets forth eight categories of individuals who may inspect presentence reports. As the more particularized statute, Section 5-3-4 should control a court's analysis and determination of the non-public nature of presentence investigation reports.

Finally, as a probation record, a presentence investigation report is not a public record under the plain language of the Probation and Probation Officers Act.[84] Members of the subcommittee pointed out that those circuits that consider presentence investigation

[77] *See* 11TH JUD. CIR. CT. R. 205.
[78] 730 ILCS 5/5-4-1(c).
[79] *See People v. Davis*, 93 Ill.2d 155 (1982) (holding that the requirement that, in imposing a sentence for a felony conviction, a judge "shall" specify reasons for his or her sentencing determination is constitutional only when "shall" is construed to be permissive rather than mandatory).
[80] 730 ILCS 5/5-3-4(a).
[81] *Astoria Fed. Savings & Loan Ass'n v. Solimino*, 501 U.S. 104, 112 (1991) (explaining that statutes should be construed "so as to avoid rendering superfluous" any statutory language).
[82] 730 ILCS 5/5-3-4(b).
[83] *Bowes v. City of Chicago*, 3 Ill.2d 175 (1954); *People v. Villarreal*, 152 Ill.2d 368, 379 (1992).
[84] 730 ILCS 110/12(3), (4).

reports public records may violate HIPAA regulations if they fail to redact physical and mental health portions of the presentence report.[85]

RECOMMENDATION: Presentence investigation reports are non-public records that are restricted to the individuals identified in Illinois statutes. The proper accessibility 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.

4. Information concerning probationers

Probation is a sentencing alternative that provides selected offenders the opportunity to serve a criminal sentence in the community under the supervision of a probation officer. A sentence of probation may require an offender to pay fines or restitution, to seek counseling for substance abuse, or to address health or family problems. The goal of probation is to help reintegrate offenders into the community as responsible, law-abiding individuals.

To meet this goal, probation officials[86] initially collect considerable amounts of information to identify available sentence and treatment options.[87] After an offender is sentenced to probation, probation officials collect even more information to ensure the probationer's compliance with the court-ordered conditions and to protect against the risks of the probationer committing new offenses. Information about probationers is also collected to conduct research and evaluations designed to improve the quality of probation services.[88]

Mandatory information practices

(1) Probation officials must collect probationer information – To fulfill their supervisory function, probation officials collect any information about probationers that documents their compliance with the conditions of their probation.[89]

(2) Probation officials must report abuse and neglect of a minor – As mandated reporters under The Abused and Neglected Child Reporting Act, probation officials must provide probationer information to the Illinois Department of Children and Family Services where they have reasonable cause to believe that a child may be abused or neglected.[90]

(3) Probation officials must provide probationer information to certain public housing agencies – Where a probationer resides at an address that is owned, operated, or otherwise

[85] 45 C.F.R. Parts 160; 162; 164.
[86] "Probation officials" is a term used throughout this report to broadly refer to probation officers and pre-trial services personnel.
[87] 730 ILCS 5/5-3-2.
[88] 730 ILCS 110/15(1)(g); (j); (l).
[89] 730 ILCS 110/12.
[90] 325 ILCS 5/4; *see also* 18TH JUD. CIR. CT. R. 36.11(b)(4).

managed by a public housing agency, probation officials must notify the agency that the resident is on probation.[91]

(4) Probation officials must provide probationer information to Departments, regulated housing facilities – Where a probationer resides at a facility licensed or regulated by the Illinois Departments of Public Health, Public Aid, or Human Services, probation officials must affirmatively provide the following information to the regulating department and the regulated facility:[92]

(a) Presentence investigation reports;
(b) Probation orders and compliance plans; and
(c) The name and contact information for the assigned probation official.

(5) Public access to probationer information contained in the court records – Conditions of probation are part of a court's sentencing order and are a matter of public record. Where a probationer allegedly violates the conditions of his probation, the state's attorney files a petition to revoke the offender's probation. This petition is filed with the court and is set for a public hearing.

Commentary

Generally, the public only has access to probationer information when that information is the subject of an open court hearing. Victims are provided no more information about adult probationers than members of the general public. Nevertheless, victims of juvenile offenders do have more access to probationer information than the public.[93] This is interesting because Illinois law usually provides greater protections to juvenile offenders than to adult offenders.

Prohibited information practices

(1) Restricted access to probation files – Records maintained by probation officials are restricted to probation officers, judges, and any individual or agency pursuant to court order.[94]

Permissible information practices

The following practices may be more properly characterized as exceptions to the Probation and Probation Officers Act rather than permissive information practices. Nevertheless, the following practices include the types of information sharing that are necessary to further the goals of probation even though they are not explicitly provided for by the Act; they balance the goals of probation (i.e., encouraging treatment and building rapport between a probation officer and his client) and the law enforcement goals of the justice system.

(1) Probation officials may provide some probationer information to police and prosecutors – Probation officials may share with police officials and prosecutors any information about probationers that is already of public record or based on a probation official's visual public observation of the probationer.[95]

Commentary

[91] 730 ILCS 110/12(10).
[92] 730 ILCS 110/12(11).
[93] *See* 705 ILCS 405/1-8(A)(7) (granting victims of juvenile offenders access to the name and address of the minor as well as information pertaining to the disposition or the court's alternative adjustment plan).
[94] 730 ILCS 110/12(4).
[95] 18TH JUD. CIR. CT. R. 36.11(c).

This practice permits probation officials to share information that, while it may be contained in a their protected records, is already available to the public. For example, publicly displayed tattoos that are observed by a probation official may be shared with police officials. However, address updates and *modus operandi* information are not matters of public record and could not be shared pursuant to this practice.

(2) Probation officials may provide probationer violation information to prosecutors – Records that support an allegation that the probationer violated a court order may be shared with a prosecutor for the purpose of charging and proving the violation.[96]

Commentary

Although prosecutors are responsible for proving violations of probation, the evidence to prove the alleged violation is often contained in probation officials' records. This practice addresses the necessity of sharing information when a probationer is accused of violating the conditions of his probation.

(3) Probation officials may provide evidence of criminal conduct with police – When probation officials are in possession of reliable information that a probationer under their supervision is engaging in criminal conduct, probation officials may share information about the probationer with police officials.[97]

Commentary

This is a permissive practice that reflects probation officials' broad discretion to make difficult decisions concerning their probationers. Additionally, this information sharing may only take place where the reliable information is gathered directly by probation officials. Where police officials have collected reliable information that the probationer is suspected of criminal conduct, a court order is still required before probation officials may disseminate information about the probationer.

(4) Probation officials may provide information to anyone involved in fulfilling conditions contained in court orders – Probation officials may share information about probationers with anyone who is authorized by the probation department and involved in fulfilling the conditions contained in a court order.[98]

Commentary

This practice provides for instances where it is impossible to comply with a court order unless certain information about probationers is shared; for example, a treatment provider may require information about the probationer to administer court-ordered treatments. Permitting probation officials to share information in these instances improves efficiency by eliminating the need to go before the judge a second time when the intent of the court's order is readily ascertainable.

Issues identified

(1) Whether probation officials may provide probationer information to police officials to warn of threats of violence.

[96] 18TH JUD. CIR. CT. R. 36.11(b)(1).
[97] 18TH JUD. CIR. CT. R. 36.11(b)(5).
[98] 18TH JUD. CIR. CT. R. 36.11(b)(2). Alternatively, orders having an impact upon a probationer could provide: "The Department of Probation and Court Services is authorized to divulge necessary contents from its records to comply with this Court Order."

YES, PROBATION OFFICIALS MAY WARN POLICE OFFICIALS ABOUT PROBATIONER VIOLENCE. Probation officials may owe a duty to third persons because of the special relationship they have with their probationer.[99] Additionally, as an officer safety measure, probation officials should be permitted to provide a warning to police officials if a probationer posed a readily ascertainable danger (e.g., the probationer always carries a weapon). The practice would be permissive and would grant probation officials discretion in selecting the appropriate steps to ameliorate any risk posed by a probationer.

NO, PROBATION OFFICIALS MAY NOT WARN POLICE OFFICIALS ABOUT PROBATIONER VIOLENCE. This release of information concerning probationers from their probation files is not permitted under existing statutes. Furthermore, a bill before the General Assembly that would have *required* the sharing of specified identifying information when the safety of the public is at risk has failed to pass.[100]

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.[101] The General Assembly should revisit probation officials' ability to share information about probationers that may directly impact police officers' safety.

5. Information concerning prisoners

A prisoner is an individual who is involuntarily confined in any municipal lock-up, county jail, or facility administered by the Illinois Department of Corrections. The term, as used in the following discussion, is intentionally broad and encompasses individuals sentenced to such an institution under a criminal or civil statute as well as individuals detained pending arraignment, trial, or sentencing.

Generally, the following information practices apply regardless of the type of institution that confines the prisoner. Variations in the types of information collected, used, and disseminated by different institutions are indicated by specifying that the practice applies to the Illinois Department of Corrections (i.e., prisons), county jails, or municipal lock-ups. The differences in the amount of information collected are the result of the role of these facilities, the length of a prisoner's stay, and the types of treatment programs available. A summary of the types of information collected about prisoners is included in Table 1 located at the end of this report.

Corrections officials[102] collect information about prisoners to verify their identity and justify their confinement. Prisoner information related to the health, safety, and security of the facility is also collected. Although corrections officials document each prisoner's social, physical, and mental health condition, the following discussion does not address the information practices concerning these or any other types of medical information.

---

[99] *See generally, Doe 1 ex rel. Tanya S. v. North Cent. Behavioral Health Sys., Inc.*, 352 Ill.App.3d 284, 290 (3d Dist. 2004). *See also* Restatement (Third) of Torts § 41 (2004).
[100] H.B. 1105 94th Gen. Assembly (Ill. 2005)
[101] 18TH JUD. CIR. CT. R. 36.11(b)(3).
[102] "Corrections officials" is a term used throughout this report to broadly refer to state correctional officers, sheriffs, and police officials administering municipal lock-ups.

Mandatory information practices

Once a prisoner leaves the custody of the correctional facility, his records are retained, used, and disseminated in the same manner as the records of individuals still in custody.[103]

(1) Corrections officials must collect prisoners' information – Corrections officials must collect prisoner information:

(a) To verify the identity of the person before accepting custody;[104]
(b) To classify prisoners and determine appropriate facilities and programs;[105]
(c) To ensure compliance with court sentencing orders;[106]
(d) To identify individuals and groups of individuals who pose a threat to the safety and security of the facility;[107]
(e) To determine the prisoner's financial status for reimbursement purposes;[108]
(f) To conduct research and evaluations designed to improve the quality of corrections services;[109]
(g) To provide victims with information regarding the prisoner's custodial status;[110]
(h) For the purposes of maintaining complete and accurate criminal history records as well as compiling crime statistics.[111]

Commentary

Corrections officials collect a substantial amount of information about prisoners. For example, a prisoner's IDOC master record file contains: (a) all information from the committing court; (b) his reception summary; (c) evaluation and assignment reports and recommendations; (d) reports regarding his treatment program assignment and progress; (e) any reports of disciplinary infractions and disposition; (f) his presentence investigation report; (g) any parole plans and reports; (h) the date and circumstances of his final discharge; and (i) other pertinent data concerning the prisoner's background, conduct, associations and family relationships.[112] While medical records are not kept in a prisoner's master record file, there may be some documents, such as a presentence investigation report, that contain medical information.[113]

As part of the inmate classification process, the Illinois Department of Corrections is required to conduct a social evaluation of each prisoner's medical, psychological, educational, and vocational condition and history, including the use of alcohol and other drugs, and the circumstances surrounding his offense.[114]

---

[103] 730 ILCS 5/3-5-1(d); ILL. ADMIN. CODE tit. 20 § 107.310(d) (providing that access to the records of a person no longer in custody of IDOC shall be provided in accordance with procedures applicable to committed persons).
[104] 730 ILCS 5/3-8-1(b); *see also* 20 ILCS 2630/2.1(e).
[105] ILL. ADMIN. CODE tit. 20 § 503.20.
[106] 730 ILCS 5/3-8-1; 5/5-4-1(e).
[107] 730 ILCE 5/3-2-5(c).
[108] *See* 730 ILCS 5/3-7-6.
[109] *See* 730 ILCS 5/3-2-2(1)(g); 5/3-2-8.
[110] *See* 725 ILCS 120/8.5 (creating the statewide victim and witness notification system administered by the Illinois Attorney General).
[111] 20 ILCS 2630/2.1; 2630/8.
[112] 730 ILCS 5/3-5-1(a). *See also* ILL. ADMIN. CODE tit. 20 § 107.20.
[113] *See infra* Information concerning convicted persons, Subcommittee Recommendations.
[114] 730 ILCS 5/3-8-2(a).

(2) Corrections officials must collect inmate gang information – Corrections officials must collect information regarding the inmate gang population to control and limit gang activities within correctional facilities.[115]

Commentary

Prison gangs pose a serious danger to the operation of prisons and the safety of inmates and staff. In 2003, the Illinois Department of Corrections documented approximately 50% of the entire male prison population and approximately 18% of the entire female population as affiliated with a security threat group; nearly two thirds of the population housed at maximum-security facilities aligns with a security threat and at least 88 active security threat groups have been identified in the IDOC.[116]

(3) Illinois Department of Corrections must provide gang information to Governor – Personally identifying information regarding the membership and leaders of inmate gangs, and the measures taken by the Illinois Department of Corrections to segregate leaders, must be provided to the Governor annually.[117]

(4) Illinois Department of Corrections must provide gang information to General Assembly – The Illinois Department of Corrections gang intelligence unit must file annual reports with the General Assembly that include profiles of the inmate population associated with gangs and gang-related activities within correctional facilities.[118]

(5) Sheriff must provide prisoner information to the court clerk – The sheriff must provide to the court clerk the number of days that the prisoner has been held in custody for the purpose of crediting that time against the prisoner's sentence.[119]

(6) Prosecutors must provide prisoner information to court clerks, corrections officials – Prosecutors must provide the facts and circumstances of the prisoner's offense together with any information that may aid the correctional institution during its custody of the offender. This information must be filed with the court clerk to be transmitted to the correctional institution taking custody of the prisoner.[120]

(7) Court clerks must provide certain information to correctional institutions – When a prisoner is committed to a correctional institution, the clerk of the court must provide the following information to that institution:[121]

(a) The sentence imposed, including any statement by the court regarding the basis for imposing the sentence;
(b) Any presentence reports;

---

[115] 730 ILCS 5/3-2-5(c).
[116] ILL. DEP'T OF CORRECTIONS, Department Overview FY 2003, Intelligence and Investigations Section http://www.idoc.state.il.us/subsections/dept_overview/2003/investigations_intelligence.shtml. A security threat group is a group of individuals with a common interest, bond, or activity characterized by criminal or delinquent conduct, engaged in either collectively or individually, with the potential to create a security threat to correctional facilities or functions; security threat groups include, but are not limited to gangs and other groups that offer protection, financial reward and access to drugs and other contraband.
[117] 730 ILCS 5/3-2-2(1)(l-5).
[118] 730 ILCS 5/3-2-5(c).
[119] 730 ILCS 5/5-4-1(e)(4).
[120] 730 ILCS 5/5-4-1(d).
[121] 730 ILCS 5/5-4-1(e).

(c) Any sex offender evaluations;
(d) Any substance abuse treatment eligibility screening and assessment;[122]
(e) The number of days, if any, which the prisoner has been in custody and for which he is entitled to credit against the sentence;
(f) Any court finding of great bodily harm to the victim, when the sentence is imposed for: aggravated kidnapping for ransom, home invasion, armed robbery, aggravated vehicular hijacking, aggravated discharge of a firearm, or armed violence with a category I weapon or category II weapon;[123]
(g) Any statements filed by the prosecutor and defense counsel;[124]
(h) Any medical or mental health records;
(i) The municipality where the arrest of the offender or the commission of the offense has occurred;[125]
(j) Any statements or evidence offered by victims or other qualified individuals offered in aggravation or mitigation of prisoner's sentence;[126] and
(k) All additional matters as ordered by the court.

(8) Illinois State Police must provide prisoners' sealed records to Illinois Department of Corrections – Upon conviction for any offense, the Illinois Department of Corrections shall have access to all sealed records of the Illinois State Police pertaining to that individual.[127]

(9) Corrections officials must provide custodial information to Illinois State Police – Corrections officials must share all information concerning the custodial or sentencing status of prisoners with the Illinois State Police for the purpose of compiling a complete criminal history record.[128]

Commentary

A prisoner's custodial or sentencing status, which must be provided to the Illinois State Police, includes all information concerning the prisoner's receipt, escape, execution, death, release, pardon, parole, commutation of sentence, granting of executive clemency or discharge.[129]

(10) Corrections officials must provide information to other corrections officials upon prisoner transfer – When a prisoner is transferred from one custodial institution to another, information concerning the prisoner must accompany him to the new institution.[130]

[122] A state-designated provider must conduct the screening and assessment.
[123] 730 ILCS 5/5-4-1(c-1).
[124] 730 ILCS 5/5-4-1(d).
[125] This information is only transmitted where such municipality has a population of more than 25,000 persons.
[126] 730 ILCS 5/5-4-1(a)(7).
[127] 20 ILCS 2630/13(a).
[128] 20 ILCS 2630/2.1(e).
[129] *Id.*
[130] *See* 730 ILCS 5/3-5-1(c) (providing for the transfer of master record files between IDOC facilities and requiring a summary of the file to be forwarded when the prisoner is transferred to a department or agency outside of IDOC); 730 ILCS 5/3-4-4 (providing for the transfer of records between sending and receiving institutions under Article VI of the Interstate Corrections Compact); 730 ILCS 155/1 (providing for the transfer of records between municipal lock-ups and county jails); and 730 ILCS 5/3-8-1 (implemented by ILL. ADMIN. CODE tit. 20 §§ 107.20; 701.60) (providing for the transfer of records from county jails to IDOC).

(11) Illinois Department of Corrections must provide information to Illinois Department of Public Aid – Corrections officials must provide to the Illinois Department of Public Aid any information that may be necessary for the enforcement of child support orders.[131]

(12) Corrections, police must provide prisoners' names and charges to the public – Upon request, corrections and police officials must provide a prisoner's name and the charges for which he is being held.[132]

(13) Corrections officials must maintain dissemination logs – Corrections officials must keep a record of the following for all disclosures of prisoner information to outside personnel:[133]

(a) The identity of the requestor;
(b) The purpose for accessing the prisoner's information; and
(c) The information reviewed and copied.

Prohibited information practices

(1) Corrections officials cannot provide gang intelligence information to the public – Gang intelligence information collected or maintained by the Illinois Department of Corrections cannot be disclosed to the public.[134]

Permissible information practices

(1) Public agencies may provide information to Illinois Department of Corrections – Upon request, public agencies may supply unprivileged information concerning prisoners committed to the Illinois Department of Corrections.[135]

(2) Defense counsel may provide prisoner information to court clerks, corrections officials – Defense counsel may provide the facts and circumstances of the prisoner's offense together with any information that may aid the correctional institution during its custody of the offender; this information can be filed with the court clerk to be transmitted to the correctional institution taking custody of the prisoner.[136]

(3) Corrections officials may provide prisoner information to corrections, welfare, or police officials – Corrections officials may provide prisoner information to corrections, welfare, or police officials. [137]

(4) Corrections officials may provide gang intelligence information to police officials – Information regarding the inmate gang population may be shared with police officials in order to assist in the investigation, prevention, and prosecution of gang activity.[138]

---

[131] 730 ILCS 5/3-5-4.
[132] 5 ILCS 140/7(1)(d)(ii).
[133] 730 ILCS 5/3-5-1(b).
[134] 730 ILCS 5/3-2-5(c) (exempting gang information from disclosure under the Freedom of Information Act because the information is highly confidential and may be harmful if disclosed); 730 ILCS 5/3-2-2(1)(l-5) (providing that the confidential report to the governor containing gang intelligence information is not subject to public disclosure).
[135] 730 ILCS 5/3-5-1(e).
[136] 730 ILCS 5/5-4-1(d).
[137] 730 ILCS 5/3-5-1(b).
[138] 730 ILCS 5/3-2-5(c); ILL. ADMIN. CODE tit. 20 § 107.310(c).

(5) Correctional officials may restrict information concerning institutional security – Records that relate to or affect the security of any correctional institution or detention facility can be withheld from the public.[139]

(6) Illinois Department of Corrections may provide certain prisoner information to the public – The Illinois Department of Corrections may release the following information about former and current prisoners to the public:[140]

(a) Name;
(b) IDOC number;
(c) Parent institution;
(d) Current location or status;
(e) Vital statistics;
(f) Admission and release dates; and
(g) Charging or sentencing information.

Issues identified

None.

6. Information concerning individuals on supervised release

Supervised release is not parole. Illinois abandoned the traditional, discretion-based parole system in 1978.[141] From then on, all individuals who committed a crime were imprisoned on determinate sentences that provided for a set period of mandatory supervised release to be served after their prison sentences.[142] At present, less than 350 prisoners confined by the Illinois Department of Corrections are eligible for "true" parole. This report does not discuss the types of information collected and used in making release decisions for inmates eligible for parole. Furthermore, because the information practices concerning the supervision of sex offenders are somewhat different, they will be addressed in a later volume.

Because the Illinois Department of Corrections maintains custody of all persons placed on supervised release,[143] the information practices concerning prisoners described above apply to individuals on supervised release. The following discussion focuses on the additional information practices that concern individuals released under the supervision of corrections officials.

Supervisory corrections officials collect information necessary to ensure the individual's compliance with the conditions set by the Prisoner Review Board. Officials must remain

[139] 5 ILCS 140/7(1)(e) (permitting the correctional facility to withhold facility security information).
[140] Illinois Department of Corrections, http://www.idoc.state.il.us/subsections/records/default.shtml.
[141] Even though the institution of parole has been replaced with mandatory supervised release, the term "parole" is still used throughout the Illinois justice system. For example, IDOC continues to use the term in responses to its inmate query found in the IDOC website and corrections officials who supervise released individuals are still called "parole officers." Nevertheless, there are distinctions between parole and mandatory supervised release and it is proper to use precise terms when discussing any policy issue.
[142] *See* 730 ILCS 5/5-8-1(d).
[143] 730 ILCS 5/3-14-2(a).

informed of their clients' conduct and protect against the risks of the released individual committing new offenses.

Mandatory information practices

(1) Individuals on supervised release must provide information to supervisory officials – Individuals on mandatory supervised release must continuously provide updated information to supervisory officials. An individual on supervised release is required to, among other things, provide his employment and residence information, report any arrests, provide information regarding his adjustment in the community, and secure the supervisory official's permission before leaving the state or county.[144]

(2) Illinois Department of Corrections must notify certain prosecutors, police officials of felon's release – When a prisoner convicted of a felony is released, the Illinois Department of Corrections must notify:[145]

(a) The State's Attorney, the Sheriff, and the municipal police department of the jurisdiction where the crime was committed;
(b) The State's Attorney, the Sheriff, and the municipal police department of the jurisdiction into which the individual will be released;
(c) The arresting police agency; and
(d) The police department of the municipality where the individual resided at the time he committed the crime.

(3) Corrections officials must notify concerned citizens, victims of prisoner releases – Upon request, corrections officials must inform victims and any concerned citizens when individuals are released to supervision and when they are discharged from supervision.[146]

(4) Illinois Department of Corrections must provide prisoner information to certain public housing agencies – When an individual on supervised release resides at an address that is owned, operated, or otherwise managed by a public housing agency, the Illinois Department of Corrections must notify the agency that the resident is under the supervision of the corrections officials.[147]

(5) Illinois Department of Corrections must provide prisoner information to Departments, regulated housing facilities – When an individual on supervised release resides at a facility licensed or regulated by the Illinois Departments of Public Health, Public Aid, or Human Services, corrections officials must provide the following information to the regulating department and the regulated facility:[148]

(a) The mittimus and any presentence investigation reports;
(b) Any social evaluations;
(c) Any pre-release evaluations;
(d) Reports of disciplinary infractions and dispositions;

[144] 730 ILCS 5/3-3-7; ILL. ADMIN. CODE tit. 20 § 1610.120.
[145] 730 ILCS 5/3-14-1(c).
[146] 725 ILCS 120/4.5(d) (providing that a recent photograph of the released individual may be included in the notification).
[147] 730 ILCS 5/3-14-1(c).
[148] 730 ILCS 5/3-14-1(c-5).

(e) Orders issued by the Prisoner Review Board as well as any violation reports and dispositions; and
(f) The name and contact information for the assigned supervisory official.

(6) Illinois Department of Corrections must provide prisoner information to Prisoner Review Board, chief police officials – Where an individual on mandatory supervised release becomes a resident of a facility licensed or regulated by the Illinois Departments of Public Health, Public Aid, or Human Services, the Illinois Department of Corrections shall provide written notification of such residence to the Prisoner Review Board as well as to the chief of police and sheriff in the municipality and county in which the licensed facility is located.[149]

Prohibited information practices
None identified.

Permissible information practices
None identified.

Issues identified
None.

7. Information concerning victims of crime, generally
In Illinois, as in many other states, victims of certain crimes are granted more privacy protections than victims of other crimes. To better organize the subcommittee's findings, this report separates victims into five categories – (1) victims of sexual offenses; (2) victims of domestic abuse; (3) victims of identity theft; (4) child victims; and (5) victims of all other crimes. This discussion sets forth the information practices that are applicable to all victims of crime in Illinois. The discussions regarding the more specific types of victim that follow supplement, and in some instances override, the information practices contained in this section.

Victims' information is collected primarily to further the investigation of the crime, to substantiate charges, and to assist in the prosecution of the person charged with the offense. Victims update the contact information they provide to the justice system to keep informed about the status of their case.[150] In some instances, victim information is used to protect the victim from further contact with the person charged with the offense.

Mandatory information practices
(1) Police must collect victim information – When a crime is discovered, reported, or investigated, police officials collect a victim's name, address, and other identifying information in addition to information about any acts that occurred to the victim and his resulting condition.

Commentary

The Rights of Crime Victims and Witnesses Act offers little guidance with respect to what information about victims is kept confidential by the Illinois justice system.

[149] 730 ILCS 5/3-14-1(c-10).
[150] *See* 725 ILCS 120/8.5 (creating the statewide victim and witness notification system administered by the Illinois Attorney General).

Although the Act requires a significant amount of information to be provided to victims concerning the offender's prosecution, its only privacy provision holds that victims should be "treated with fairness and respect for their dignity and privacy throughout the criminal justice process."[151]

(2) Probation officials must collect victim information – For purposes of conducting a presentence investigation, probation officials must assess the effect the offense committed has had upon the victim.[152]

Commentary

Probation officials collect information to assess how the victim was affected by the crime and to determine whether various sentencing alternatives could compensate the victim.

(3) Police must provide victim information to prosecutors – Police officials must share with prosecutors the victim information they collect as part of an investigation including, but not limited to, each victim's personally identifying information, the details of the crime, and each victim's resulting condition.[153]

(4) Courts must provide victim information to the public – Victim information contained in court records is available to the public.[154]

Commentary

Illinois discovery rules for criminal cases provide some methods of reducing the amount of personally identifying victim information contained in the court's records. Illinois Supreme Court Rule 415 requires documents received by parties during discovery to remain in counsel's exclusive custody and further provides for protective orders when there is substantial risk to any person of physical harm, intimidation, or retribution that outweighs any usefulness of disclosing the individual's identity.[155] Protective orders that prohibit the parties from revealing the alleged victims' names or other identifying information to the general public are enforceable if drafted narrowly enough to protect the alleged victim and also permit both parties to engage in full pretrial investigation and discovery.[156]

Prohibited information practices

None identified.

Permissible information practices

(1) Police may share victim information with other police officials – When necessary to investigate or prosecute a crime, police officials may share a victim's identifying information, the details of the crime, and the victim's resulting condition with police officials from other jurisdictions.

(2) Defense counsel may access victim information in certain circumstances – When it will serve the interests of justice, defense may have access to:

[151] 725 ILCS 120/2.
[152] 730 ILCS 5/5-3-2(a)(3).
[153] 725 ILCS 5/114-13(b).
[154] 705 ILCS 105/16(6).
[155] ILL. SUP. CT. R. 415(c), (d).
[156] *Bush v. Catholic Dioceses of Peoria*, 351 Ill.App.3d 588 (3d Dist. 2004).

(a) Victimization information concerning their client and other individuals;[157] and
(b) Statements regarding the crime or its circumstances made to victim counselors.[158]

Commentary

Illinois Supreme Court Rule 412(a)(i) requires the State to disclose to defense counsel the names and last known addresses of persons whom it intends to call as witnesses, together with their relevant written or recorded statements, memoranda containing substantially verbatim reports of their oral statements, and a list of memoranda reporting or summarizing their oral statements. This is relevant because the State's witnesses frequently include the victim of the crime.

Some states do not grant the defendant access to the victim's contact information; instead, these states only provide the victim's contact information to defense counsel.[159]

If a party alleges that statements made during victim counseling are necessary to the determination of any issue before the court, the court, after an *in camera* hearing about the relevance of the statements, can order the statements to be disclosed.

Issues identified

Victims are not voluntary participants in the justice process. Nevertheless, they can be required to disclose a substantial amount of sensitive information to the government solely because they were victimized.[160] If the justice system's treatment of this information threatens victims' privacy, they may regard not reporting a crime as the only alternative to these data collection practices.[161]

(1) Whether privacy issues are implicated in the sharing of non-identifying incident information across jurisdictions.

BACKGROUND: Incident information is routinely used to compile crime statistics and perform analyses that aid in preventing crime, apprehending offenders, managing justice resources, training officers, and conducting research. The goals of crime analysis are to utilize incident information to identify crime patterns and series,[162] forecast future occurrences of crime, apprehend offenders, and recover stolen property.[163] A review of existing police crime analysis operations reveals that burglary, robbery, auto theft, larceny, fraud, sex crimes, aggravated assaults, and murder are the crimes most likely to be solved through traditional crime analysis techniques.[164] The categories of data that are considered most useful for crime analysis include:

[157] ILL. SUP. CT. R. 412(a)(i).
[158] 735 ILCS 5/8-802.2.
[159] *See* CAL. PENAL CODE §841.5; ALASKA STAT. §12.61.120.
[160] A bill that would have allowed persons submitting information of a crime to remain anonymous failed to pass the Illinois General Assembly. *See* H.B. 1018, S. Amend. 1, 93d Gen. Assembly (Ill. 2004).
[161] ILLINOIS CRIM. J. INFO. AUTH., The Extent and Nature of Adult Crime Victimization in Illinois 62 (2002) (finding that 34% of those respondents who decided not to report a crime against their person did so because the victimization was "a private or personal matter or took care of it informally").
[162] A crime pattern is merely a set of similar offences happening in a specific geographical area while a crime series is a crime pattern that appears to be done by either the same person or group of persons. Shawn A. Hutton & Mark Myrent, Incident-Based Crime Analysis Manual 34 (ILL. CRIM. J. INFO. AUTH. 1999).
[163] Steven Gottlieb, *et al*., Crime Analysis: From First Report to Final Arrest 14-16 (1994).
[164] *Id.* at 133. In 2004 there were 75,944 burglaries, 22,561 robberies, 40,780 motor vehicle thefts, 294,750 thefts (including larceny and fraud), 5,813 criminal sexual assaults, 41,806 aggravated assaults, and 776 murders. Crime in Illinois 2004 (ILL. STATE POLICE 2005).

- Geographic factors[165]
- Time factors
- Victim descriptors
- Property loss descriptors
- Physical evidence descriptors
- Specific Modus Operandi ("MO") factors
- Suspect descriptors
- Suspect vehicle descriptors

A brief summary of the types of information that experienced analysts have found useful to determining if a crime pattern exists can be found in *Table 2: Categories of information most useful for traditional crime analysis*.

VICTIMS' IDENTITIES ARE NOT NECESSARY FOR ALL TYPES OF CRIME ANALYSIS. The victim descriptors utilized in traditional crime analysis are those pieces of information that are useful in determining an offender's preferences for certain types of targets. Police officials use this understanding of an offender's preferences to predict when, where, and against whom he will commit his next criminal offense. Thus, where police officials have not identified a suspect, it can more helpful to collect and share a victim's demographic and other vulnerability factors rather than their identities.

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.

(2) Whether victims' identities and victimization histories should be made widely available across jurisdictions.

YES, VICTIMS' IDENTITIES SHOULD BE MADE WIDELY AVAILABLE. Victims' identities are already shared across jurisdictions when the need to do so arises. Integrated justice information systems will help police officials determine when and where that need may exist. For example, a person who files multiple theft reports in various jurisdictions might reasonably be suspected of committing some type of fraud. Absent an integrated justice information system, an officer taking an incident report in one city might not be aware of the reports the individual filed in another jurisdiction.

Additionally, integrated justice information systems can help identify relationships between offenders and victims across different crimes. In the context of gang violence, it is not uncommon for a victim of a battery at the hands of a rival gang member to seek revenge. The victim in this crime, or his associates, might attack members of the rival gang in retribution for the earlier attack. Electronically sharing victims' identities and compiling them with offender information may reveal relationships not apparent in the paper-based world and can lead to the apprehension of more criminals and even prevent future acts of violence.

[165] Although spot maps can be of great assistance to the analyst, they will only depict crime patterns. Additional information is necessary to determine if a crime pattern is also a crime series.

NO, VICTIMS' IDENTITIES SHOULD NOT BE MADE WIDELY AVAILABLE. It is clear that a justice practitioner assigned to investigate, prosecute, or otherwise work on a specific criminal matter should have access to the identities of those who were harmed during the commission of that crime. Nevertheless, dignity issues are raised when a piece of information (e.g., a victim's personally identifiable information) is initially collected by the government to assist the victim but is subsequently used to cast suspicion upon them.

Although proponents of the widespread sharing of victims' identities provide valuable examples, it is unclear how the identities of victims of sexual violence or domestic violence should be treated in such an integrated justice information system. This is because, as will be explained in the following discussions, such victims have additional protections under Illinois law. This means that including *every* victim's identity in an integrated justice information system may not be advisable.

Some members that acknowledged the potential usefulness of sharing victims' identities across jurisdictions suggested that the user of an integrated justice information system should be required to certify that he has a demonstrable need to know a victim's identity. This way, victims' names could be included in the system for purposes of linking and associating data, but would not be revealed to a user until his investigation required that information. This limit on the accessibility of the information is based upon the premise that an inquiry to an integrated justice information system may return some results that are not pertinent to the crime being investigated.

Integrated justice information systems have the potential to not only disseminate a victim's identity across numerous jurisdictions, but also to compile that individual's victimization history. This means that a user of the system could determine, with relative ease, the number of times a person has been victimized and by which types of criminal activity. It is unclear how useful this functionality is in solving and preventing crimes. Furthermore, the risk exists that people who are repeatedly victimized may be treated differently than first-time victims with respect to the quality of investigation that an officer conducts.

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.

8. Information concerning victims of sexual offenses

Because of the fear and stigma that often result from sexual offenses, many victims hesitate to seek help even where it is readily available. The subcommittee found several protections in existing law to ensure that victims of sexual violence feel comfortable reporting the crime.[166]

[166] Callie Marie Rennison, Ph.D., US DEP'T OF J., Rape and Sexual Assault: Reporting to Police and Medical Attention, 1992-2000 3 (August 2002) (finding that most rapes and sexual assaults were not reported to the police

These information practices operate in addition to the protections of victims of general crimes discussed above.

Mandatory information practices

None identified.

Prohibited information practices

(1) Justice system cannot collect rape crisis records without victim consent – Rape crisis service records are confidential and can be collected by the justice system only with the victim's consent.[167]

(2) Restricted access to the identities of victims of juvenile sex offenders – A victim's personally identifying information contained in the impounded court file is restricted to the following parties and is provided to them only when necessary for the discharge of their official duties:[168]

(a) A judge of the circuit court and members of the court's staff;
(b) Parties to the proceedings and their attorneys;
(c) Victims and their attorneys, except that where there are multiple victims of sex offenses the information identifying the non-requesting victims must be redacted;
(d) Probation officials, police officials, and prosecutors; and
(e) Adult and juvenile Prisoner Review Boards.

Commentary

A victim of a juvenile offender has greater protections than a victim of an adult offender. Not only is the court's file impounded because of the offender's juvenile status, but also the victim's identity can only be disclosed to justice practitioners in the performance of their duties.

(3) Restricted access to information about victims of juvenile sex offenders – So long as the information does not identify the victim, the details of the crime and the victim's resulting condition contained in the court's impounded files is restricted to the following individuals and is provided to them only when necessary for the discharge of their official duties:[169]

(a) Authorized military personnel;
(b) Persons engaged in bona fide research;
(c) The Illinois Secretary of State;
(d) The administrator of a bona fide substance abuse student assistance program; and
(e) Any entity having custody of the juvenile.

(4) Information about victims of juvenile sex offenders cannot be disclosed to the public – Information contained in law enforcement or court records that identify victims and alleged

---

and that when victims of rape, attempted rape, and sexual assault did not report the crime to the police, the most often cited reason was that the victimization was a personal matter).

[167] *See* 735 ILCS 5/8-802.1 (providing an absolute privilege for information provided to rape crisis personnel by victims of sexual violence; this absolute privilege bars the court from conducting any *in camera* examination because of the strong policy involved).

[168] 705 ILCS 405/5-901(1)(a).

[169] 705 ILCS 405/5-901(1)(b).

victims of sex offenses committed by juveniles shall not be disclosed or open to public inspection under any circumstances.[170]

Commentary

Illinois law only prohibits the disclosure of information about victims of juvenile sex offenders. Nothing officially prevents the press from publishing the identities of individuals victimized by adult offenders.[171] Nevertheless, the Society of Professional Journalists' Code of Ethics cautions against identifying the victims of sex crimes and such information is traditionally not published.[172]

Permissible information practices

(1) Courts may seal sexual assault court records – After an offender is convicted of sexual assault, the victim may request, through the prosecutor's office, that the court's records be sealed; upon a showing of good cause, the court may make sealed records available for public inspection.[173]

(2) Police, prosecutors may provide victim identities to rape crisis service centers – Police officials and prosecutors may provide a sexual assault victim's identity to rape crisis service personnel for the sole purpose of referring her to the center.

Commentary

Nothing prohibits police officials and prosecutors from releasing rape victims' identities other than the concern for the victim's privacy. The exemptions contained in the Illinois Freedom of Information Act do not prohibit the dissemination of this information; rather they merely authorize agencies to withhold that information if they so desire.[174] Furthermore, the exemptions only apply where the release of information would pose a "clearly unwarranted invasion of personal privacy."[175] Here, where police officials would be providing information about rape victims to rape crisis service centers, it may be difficult to argue that such a release of the victims' identities is an unwarranted invasion of their privacy. Given the nature of sexual violence, it is reasonable for police officials and prosecutors to make efforts to provide assistance to victims who may be too traumatized to seek such assistance on their own.

Issues identified

None other than those specified in § 7 *Information concerning victims of crime, generally*.

---

[170] 705 ILCS 405/5-905(2) (applying to law enforcement records); 705 ILCS 405/5-901(3) (applying to court records).

[171] A rape victim does not have a right of action against the press for publishing her identity where the publication was accurate, and the information was lawfully obtained. *Cox Broad. Co. v. Cohn*, 420 U.S. 469 (1975). This is so even if the government erred in providing the press with the rape victim's name. *The Florida Star v. B.J.F.*, 491 U.S. 524 (1989).

[172] *See* http://www.spj.org/ethics_code.asp.

[173] 20 ILCS 2630/5(c-5). This section applies only when the offender is convicted of criminal sexual assault, aggravated criminal sexual assault, predatory criminal sexual assault of a child, criminal sexual abuse, or aggravated criminal sexual abuse. Furthermore, the sealing only applies to court records, not the records maintained by the arresting agency or the Illinois State Police.

[174] *Roehrborn v. Lambert*, 277 Ill.App.3d 181, 186 (1st Dist.1995).

[175] 5 ILCS 140/7(1)(b).

9. Information concerning victims of domestic violence

Persons attempting to escape from actual or threatened domestic violence frequently establish new addresses in order to prevent their assailants from finding them. As such, Illinois law emphasizes the confidentiality of domestic violence victims' location information. These information practices operate in addition to the protections of victims of general crimes previously discussed in this report.

Mandatory information practices

None identified.

Prohibited information practices

(1) Individuals cannot be compelled to provide certain domestic violence information – No person or domestic violence program can be compelled to disclose the location of any shelter or the identity of any domestic violence advocates or counselors. Only where a court determines that the failure to disclose this information would result in an imminent risk of serious bodily injury can the information be disclosed *in camera*, under a protective order, and the information must not be made a part of the written case record.[176]

(2) Restricted access to certified victims' address information – The Illinois Attorney General cannot provide a certified victim's actual address to anyone other than:[177]

(a) Police officials;
(b) Prosecutors; and
(c) Individuals identified in a court order permitting the disclosure.

(3) Disclosure of a domestic violence victim's location is prohibited – It is unlawful for any person to publish, disseminate, or otherwise disclose the location of any domestic violence victim, without the victim's consent, where there is a substantial likelihood the disclosure could result in bodily harm.[178]

Permissible information practices

(1) Victims of domestic violence may provide information to Illinois Attorney General – Domestic violence victims may provide personally identifying information to the Illinois Attorney General to participate in an address confidentiality program.[179]

Commentary

The Address Confidentiality for Victims of Domestic Violence Act requires the Attorney General to administer an address confidentiality program. Under this program, a victim of domestic violence may apply to have the Attorney General's Office serve as the victim's substitute address.[180] Once certified, the victim may request that State and local agencies use the substitute address designated by the Attorney General as her address when creating a new public record.[181]

[176] 750 ILCS 60/227.1.
[177] 750 ILCS 61/35.
[178] 720 ILCS 5/45-2.
[179] 750 ILCS 61/11, /15.
[180] 750 ILCS 61/15(a).
[181] 750 ILCS 61/25(a).

(2) Petitioners for protection orders may withhold address information from the court – Where the disclosure of petitioner's address would risk abuse or reveal the confidential address of a domestic violence shelter, that address may be omitted from all documents filed with the court.[182] Similarly, if the petitioner is seeking to have a child protected by the order, the petitioner may omit the child's school address where the disclosure of the school's location would risk abuse.[183]

(3) Police, prosecutors may provide victim identities to domestic violence service centers – Police officials and prosecutors may provide a victim's identity to domestic violence service personnel for the sole purpose of referring her to the center.

Commentary

Nothing prohibits police officials and prosecutors from releasing the identities of domestic violence victims other than the concern for their privacy. The exemptions contained in the Illinois Freedom of Information Act do not prohibit the dissemination of this information; rather they merely authorize agencies to withhold that information if they so desire.[184] Furthermore, the exemptions only apply where the release of information would pose a "clearly unwarranted invasion of personal privacy."[185] Here, where police officials would be providing information about domestic violence victims to domestic violence service centers, it may be difficult to argue that such a release of victims' identities is an unwarranted invasion of their privacy. Given the repetitive nature of domestic violence, it is reasonable for police officials or prosecutors to provide assistance to those victims who may be too intimidated to seek assistance on their own.

Issues identified

None other than those specified in § 7 *Information concerning victims of crime, generally*.

10. Information concerning victims of identity theft

The Illinois Identity Theft Law allows an individual who reasonably believes that he is the victim of identity theft to request a judicial determination of his factual innocence where the perpetrator of the identity theft was arrested for, cited for, convicted of, or otherwise charged with committing a crime under the victim's identity. Individuals can also request the same relief if they believe that their identity has been mistakenly associated with a criminal conviction.

Mandatory information practices

(1) Police must collect information about identity theft victims – When an individual has learned or reasonably suspects that his personally identifying information has been unlawfully used by another, he may contact police officials who must take a police report of the matter and either begin an investigation of the facts or refer the matter to the police agency where the suspected crime was committed.[186]

---

[182] 750 ILCS 60/203(b). Where disclosure is necessary to determine jurisdiction or venue, the court will collect the petitioner's address orally and *in camera*.
[183] 750 ILCS 60/203(c).
[184] *Roehrborn v. Lambert*, 277 Ill.App.3d 181, 186 (1st Dist.1995).
[185] 5 ILCS 140/7(1)(b).
[186] 720 ILCS 5/16G-30(a).

Prohibited information practices
None identified.

Permissible information practices
(1) Individuals may provide information to courts – Victims of identity theft may provide identifying information to the court for the purpose of petitioning the court for a judicial determination of the victim's factual innocence when the victim's identity is wrongfully associated with an arrest or conviction.[187]

(2) Courts may label, seal, or delete the names of identity theft victims – After a determination of an identity theft victim's factual innocence, the court may seal or delete the victim's name and associated personal identifying information contained in the court's publicly accessible records, files, and indexes, or the court may order that the victim's personally identifying information be labeled to show that the offender impersonated the victim's identity.[188]

Issues identified
None.

11. Information concerning child victims
The objective of this report is to provide the subcommittee's findings and recommendations concerning the collection, use, and dissemination of traditional, adult justice information. Detailed findings and recommendations concerning juvenile justice information will be provided in a future volume of the *Privacy Policy Guidance* series. Nevertheless, it is reasonable to discuss the child victims in this report.

Most of the information practices identified by the subcommittee concerned missing children and child victims of sexual violence. Justice practitioners collect information about missing children to develop and improve techniques used by police officials when responding to reports of missing children, and to provide a factual and statistical base for research addressing the problem of missing children.[189] Illinois's policy is to protect juveniles regardless of whether they become involved in the justice system as offenders or victims. As such, the following information practices operate in addition to the protections of adult victims of general crimes previously discussed in this report.

Mandatory information practices
(1) Police must collect information about missing children – When a child is reported missing, police officials must collect descriptive information including the child's name, age, physical description, photograph, as well as the suspected circumstances of the disappearance.[190]

[187] 720 ILCS 5/16G-30(b).
[188] 720 ILCS 5/16G-30(c).
[189] 325 ILCS 40/6(h).
[190] 20 ILCS 2605/2605-375(b)(1); 325 ILCS 55/6 (providing that police officials must investigate all requests for records concerning missing children).

(2) Illinois State Police must provide certain information about missing children to Illinois Department of Children and Family Services – When a child is reported missing, the Illinois State Police must provide the Illinois Department of Children and Family Services with the child's personally identifying information and the geographic area from which the child was reported missing.[191]

Commentary

The Department of Children and Family Services uses this information to determine if that child had been abandoned within the previous two months.

(3) Police must provide information about missing children to police in other jurisdictions – Police officials must enter the information they collect about missing children into the Illinois State Police LEADS system; [192] missing children information must also be provided to the National Crime Information Center of the U.S. Department of Justice.[193]

(4) Illinois State Police must provide certain information about missing children to Illinois Registrar of Vital Records, child's school – When a child is reported missing, the Illinois State Police must notify the Illinois Registrar of Vital Records and the child's last known Illinois elementary or secondary school of the child's disappearance.[194]

Commentary

Under the Missing Children Registration Law, the Illinois Registrar of Vital Records, as well as local government custodians, must flag the missing child's birth certificate record. This ensures that the Registrar is made aware of any request for a copy of the missing child's birth certificate.[195] When a written request for the birth record is received, the Registrar or local custodian must notify police officials and provide them with a copy of the request.[196]

When notified that one of its students has been reported missing, the school flags the child's record. Schools must notify police officials whenever a flagged record is requested.[197]

The Illinois Registrar of Vital Records, and the child's last known Illinois elementary or secondary school, are also notified when the missing child is recovered so that they can remove their flags.[198]

(5) Local police must provide information about missing children to Illinois State Police – When local police officials are notified that a missing child's record has been requested, the local officials must immediately notify the Illinois State Police and investigate the request.[199]

[191] 325 ILCS 40/3.5; ILL. ADMIN. CODE tit. 89, § 431.80(e).
[192] 325 ILCS 40/7; 20 ILCS 2605/2605-375(b)(3).
[193] 42 U.S.C. § 5779(a); 20 ILCS 2605/2605-375(b)(7)(D).
[194] 325 ILCS 55/2.
[195] 325 ILCS 55/3.
[196] 325 ILCS 55/4(c).
[197] 325 ILCS 55/5.
[198] 325 ILCS 55/2; /5.
[199] 325 ILCS 55/6.

(6) Juvenile victims must be afforded the same confidentiality protections as juvenile offenders – A minor who is the victim of a juvenile offender must be afforded the same confidentiality regarding the disclosure of his identity as the minor offender.[200]

Prohibited information practices

(1) Restricted access to the identities of child victims of sexual violence – The personally identifiable information about child victims contained in law enforcement records and court files is restricted to the following individuals, provided they are directly involved with the investigation or criminal proceedings of that victim's case:[201]

(a) Judges;
(b) Prosecutors;
(c) The defendant and his defense counsel;
(d) Psychologists;
(e) Psychiatrists;
(f) Social workers;
(g) Doctors; and
(h) Parents.

Commentary

Under Section 3 of the Privacy of Child Victims of Criminal Sexual Offenses Act, the court may prohibit the disclosure of the child victim's identity to any entity after giving notice and a hearing to all affected parties. The court's decision to prohibit disclosure of the minor victim's identity is based upon the best interest of the child and whether disclosure would further a compelling state interest.[202]

(2) Restricted access to the identities of child victims of sexual violence – When a sexual offense against a minor is committed by a school district employee or during a school-sponsored activity, the identity of the child victim must be made available to that school district's superintendent.[203]

Commentary

The superintendent is not permitted to disclose the victim's identity without the victim's valid, written consent.[204]

(3) Information about victims of juvenile sex offenders cannot be disclosed to the public – Information contained in law enforcement or court records that identify victims and alleged victims of sex offenses committed by juveniles shall not be disclosed or open to public inspection under any circumstances.[205]

(4) Press is prohibited from publishing child victims' identities obtained during closed hearings – When the press is permitted to attend an otherwise closed hearing, members of the

[200] 705 ILCS 405/5-901(3).
[201] 725 ILCS 190/3.
[202] 725 ILCS 190/3.
[203] 725 ILCS 190/3.
[204] 725 ILCS 190/3.
[205] 705 ILCS 405/5-905(2) (applying to law enforcement records); 705 ILCS 405/5-901(3) (applying to court records).

press are not permitted to disclose the identities of victims that it obtains during the court hearing.[206]

Commentary

The Juvenile Court Act provides that "the general public except for the news media and the victim shall be excluded from any hearing."[207] The prohibition against publishing the victim's identity does not apply where the press learns the identity of the minor through routine, reportorial techniques other than their attendance at the closed hearing.[208]

Permissible information practices

(1) Police may provide information about missing children to the public – Police officials may activate an AMBER Alert and provide to the public descriptive information about a missing child and/or the suspected abductor where the following conditions are met:[209]

(a) The child has been confirmed as abducted;
(b) The child is under the age of 16 or has a proven mental or physical disability;
(c) The child is in danger of serious bodily injury;
(d) There is enough descriptive information to believe that a broadcast alert will help.

(2) Court may impound its records – The court may impound its records in order to protect the names of child abuse victims from public disclosure.[210]

Commentary

Access to public records is not absolute and is subject to the inherent power of the trial court to impound its own records. Although there is a presumption favoring public access to judicial records, a court, in its sound discretion, may impound records if it is shown that the interests asserted for restricting access outweigh those in support of access.[211]

(3) Court may, in limited circumstances, close its proceedings – Where the alleged victim of a sexual offense is a minor, the court may exclude all persons who do not have a direct interest in the case. Persons may be excluded only during the child victim's testimony.[212]

Commentary

Although the Illinois Code of Criminal Procedure does not provide for the exclusion of the press from prosecutions for sex offenses where the victim is a minor,[213] the court still has the power to do so. Such a closure must be based upon a compelling governmental interest, and narrowly tailored to serve that interest.[214] Even though safeguarding the physical and psychological well-being of a minor is a compelling state interest, the trial judge should determine, on a case-by-case basis, whether the court should be closed to the press and the public, taking into account the minor victim's age, psychological

[206] *In re a Minor*, 149 Ill.2d 247 (Ill. 1992).
[207] 705 ILCS 405/1-5(6).
[208] *In re a Minor*, 149 Ill.2d 247, 252 (Ill. 1992).
[209] State of Illinois Amber Alert Notification Plan <http://www.isp.state.il.us/docs/amberplanrev0803.pdf>.
[210] *John Doe v. Carlson*, 250 Ill.App.3d 570, 574 (2d Dist. 1993).
[211] *Id.*
[212] 725 ILCS 5/115-11.
[213] 725 ILCS 5/115-11 (specifically exempting the media from its provisions).
[214] *Globe Newspaper Co. v. Superior Court for the County of Norfolk*, 457 U.S. 596, 606-607 (1982).

maturity and understanding, the nature of the crime, the desires of the victim, and the interests of parents and relatives.[215]

(4) Court may prohibit individuals from disclosing the identity of child victims of sexual violence – The court may, for the child's protection and for good cause shown, prohibit any person or agency present in court from further disclosing the identity of a child victims of sexual violence.[216]

Issues identified

None other than those specified in § 7 *Information concerning victims of crime, generally*.

12. Information concerning witnesses, generally

Information about witnesses is collected to further the investigation of a crime, to substantiate charges, and to prosecute the person charged with the offense. Witnesses also provide information to justice officials so that they can be kept informed regarding the status of the prosecution.[217]

Despite the crucial role that witnesses play in the justice system, most states' laws, including those of Illinois, focus on requiring witnesses to testify, not on protecting the confidentiality of their information.[218] Furthermore, case law supports the notion that those involved in a crime, even inadvertently or peripherally, lose some of their privacy rights due to the newsworthiness of the event.[219]

Illinois's Rights of Crime Victims and Witnesses Act was passed, in part, "to increase the effectiveness of the criminal justice system by affording certain basic rights and considerations to the witnesses of violent crime who are essential to prosecution."[220] However, the rights specifically afforded to witnesses do not address the confidentiality of their information. Rather, the Act essentially affords witnesses the rights to be notified about the trial, to have a waiting room away from defendants, and to have translators present if necessary.[221] This is not to say that witnesses' personally identifying information is completely unprotected. Several justice agencies across the state indicated that they voluntarily take steps to ensure the confidentiality of witness information.

---

[215] *Id.* at 607-608.
[216] 725 ILCS 190/3.
[217] *See* 725 ILCS 120/8.5 (creating the statewide victim and witness notification system administered by the Illinois Attorney General).
[218] Some states do provide some confidentiality protections. *See* MASS. GEN. LAWS ch. 258B, §3(h) (restricting the disclosure of the residential address, telephone number, or place of employment or school of the victim or a witness upon granting a witness's request for confidentiality); CAL. PENAL CODE § 964 (requiring each county to establish procedures that "protect confidential personal information regarding any witness or victim contained in a police report…."); NEV. REV. STAT. § 178.5691 (providing that "All personal information, including, but not limited to, a current or former address, which pertains to a victim, relative, witness or other person…is confidential.").
[219] 57 A.L.R.3d 16, Waiver or Loss of Rights of Privacy, §10(b); *see also Elmhurst v. Pearson*, 153 F2d 463 (DC Cir. 1946) (stating, "[o]ne who even unwillingly comes into public view because he is involved in a publicized criminal prosecution is subject to limitations upon his right of privacy").
[220] 725 ILCS 120/2.
[221] 715 ILCS 120/5.

Because victims and witnesses share many of the same characteristics (i.e., even though they are not voluntary participants in the justice system, they play a significant role to the administration of justice), the justice system treats their information very similarly. To better outline the Subcommittee's findings, this report separates its discussion of witness information into two categories, adult witnesses and juvenile witnesses. The following discussion does not address the sharing of information about a witness who is participating in a witness protection program.[222]

Mandatory information practices

(1) Police must collect witness information – When a crime is discovered, reported, or investigated, police officials collect a witness's name, address, and other identifying information in addition to information about the conduct and conditions observed by the witness.

(2) Police must provide witness information to prosecutors – Police officials must share with prosecutors the witness information they collect as part of an investigation including, but not limited to, each witness's personally identifying information and the details of the witness's observations.[223]

(3) Courts must provide witness information to the public – Witness information contained in court records is available to the public.[224]

> Commentary
>
> Illinois discovery rules for criminal cases provide some methods of reducing the amount of personally identifying witness information contained in the court's records. Illinois Supreme Court Rule 415 requires documents received by parties during discovery to remain in counsel's exclusive custody and further provides for protective orders when there is substantial risk to any person of physical harm, intimidation, or retribution that outweighs any usefulness of disclosing the individual's identity.[225] Protective orders that prohibit the parties from revealing witnesses' names or other identifying information to the general public are enforceable if drafted narrowly enough to protect the witness and also permit both parties to engage in full pretrial investigation and discovery.[226]

Prohibited information practices

None identified.

Permissible information practices

(1) Police may share witness information with other police officials – When necessary to investigate or prosecute a crime, police officials may share a witness's identifying information and the details of his observations with police officials from other jurisdictions.

---

[222] *See* 435 ILCS 535/15.1 (permitting the Illinois State Police to obtain a registration of a fictitious vital record to provide witnesses with new identification to protect them during and following criminal investigations or proceedings).
[223] 725 ILCS 5/114-13(b).
[224] 705 ILCS 105/16(6).
[225] ILL. SUP. CT. R. 415(c), (d).
[226] *See Bush v. Catholic Dioceses of Peoria*, 351 Ill.App.3d 588 (3d Dist. 2004).

(2) Defense counsel may access witness information in certain circumstances – When it will serve the interests of justice, defense counsel may obtain information about witnesses including, but not limited to, their identities, criminal history records, and any statements collected by police officials or prosecutors.

Commentary

Illinois Supreme Court Rule 412(a)(i) requires the State to disclose to defense counsel the names and last known addresses of persons whom it intends to call as witnesses, together with their relevant written or recorded statements, memoranda containing substantially verbatim reports of their oral statements, and a list of memoranda reporting or summarizing their oral statements. Furthermore, the Comments to Rule 412 provide that some types of impeachment evidence tend to be exculpatory or mitigating, such as certain prior convictions of State witnesses, information concerning promises or expectations of leniency for a State witness, or prior inaccurate or unsuccessful attempts at identification of the perpetrator by an occurrence witness.

Illinois case law has established a two-step procedure for parties seeking the disclosure of privileged information or records of a witness. The party must first show that the records are material and relevant to the credibility of the witness. Once this is done, the records are discoverable but must be examined by the trial court in camera if the witness claims or asserts a statutory privilege.[227]

A witness's mental health records are privileged against judicial disclosure; nevertheless, an interested party may request an *in camera* inspection of a witness's treatment records.[228] The privilege must yield when the mental health records are necessary for meaningful cross-examination of an important prosecution witness.[229]

Issues identified

Apprehension about who might have access to the information collected by the justice system in police reports, pre-sentence investigations, and court files may prevent witnesses from calling the police or participating in a criminal prosecution. Integrated justice information systems and data warehouse applications significantly improve the sharing of various forms of justice information, including the identities of witnesses; these systems also can drastically increase the number of individuals who have access to names, addresses, and other potentially sensitive information about witnesses.

(1) Whether witnesses' identities should be made widely available across jurisdictions.

YES, WITNESSES' IDENTITIES SHOULD BE MADE WIDELY AVAILABLE. Witnesses' identities can already be shared across jurisdictions when the need arises. Integrated justice information systems will help police officials determine when and where that need may exist. For instance, if the same vehicle is seen near warehouse fires that took place in three different cities, officers might reasonably suspect the car's owner of arson and take steps to interview him. Absent an integrated justice information system, an officer investigating one of the fires might miss the connection to the other two fires.

[227] *People v. Harlacher*, 262 Ill.App.3d 1, 9 (2d Dist. 1994).
[228] 740 ILCS 110/10.
[229] *People v. Williams*, 131 Ill.App.3d 597, 607 (1st Dist. 1985).

NO, WITNESSES' IDENTITIES SHOULD NOT BE MADE WIDELY AVAILABLE. It is clear that a justice practitioner assigned to investigate, prosecute, or otherwise work on a specific criminal matter should have access to the identities of those who observed the suspect or the commission of that crime. Nevertheless, witnesses might be less willing to come forward if they fear the information they provide to the justice system will later be used to cast suspicion upon them.

Some members that acknowledged the potential usefulness of sharing witnesses' identities broadly across jurisdictions suggested that the user of an integrated justice information system should be required to certify that he has a demonstrable need to know a witness's identity. This way, witnesses' names could be included in the system for purposes of linking and associating data, but would not be revealed to a user until an investigator required that information. This limit on the accessibility of the information is based upon the premise that an inquiry to an integrated justice information system may return some results that are not pertinent to the crime being investigated.

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.

13. Information concerning child witnesses

The following discussion focuses on the information practices that specifically apply to minor witnesses of criminal conduct. The practices that follow supplement the protections afforded to adult witnesses discussed above.

Mandatory information practices

None identified.

Prohibited information practices

None identified.

Permissible information practices

(1) Defense counsel may access juvenile justice records of a minor witness in certain circumstances – When it will serve the interests of justice, the court may permit the use of a minor witness's juvenile justice records for impeachment purposes.[230]

Commentary

The provision in Illinois statutes that protects a minor's police record from publication is not to be construed as prohibiting access to the records of juvenile delinquents when those records are sought in order to impeach the credibility of a juvenile as a witness by

[230] 705 ILCS 405/5-150.

showing a possible motive for testifying falsely.[231] Currently, a trial court balances the importance of a youthful witness's testimony against the State's policy of preserving the anonymity of a juvenile offender when deciding whether juvenile justice records may be used to impeach a minor witness.[232]

(2) Court may, in limited circumstances, close its proceedings – The court may deny the public the right to attend a criminal trial when it is necessary to safeguard the physical or psychological well-being of a minor witness.[233]

Commentary

The court can exclude the press and public from a criminal trial to inhibit the disclosure of sensitive information such as the identity of minor witnesses. The closure must be based upon a compelling governmental interest, and narrowly tailored to serve that interest.[234] Even though safeguarding the physical and psychological well-being of a minor is a compelling state interest, the trial judge should determine, on a case-by-case basis, whether the court should be closed to the press and the public, taking into account the minor's age, psychological maturity and understanding, the nature of the crime, the witness's desires, the nature of his testimony regarding the crime, his relationship to the accused and to persons attending the trial, and the interests of his parents and relatives.[235] The court might also consider whether requiring the child to testify in open court would cause psychological harm to him, hinder the ascertainment of truth, or result in his inability to effectively communicate due to embarrassment, fear, or timidity.

Issues identified

None other than those specified in § 12 *Information concerning witnesses, generally*.

[231] *People v. Holsey*, 30 Ill.App.3d 716, 720 (1st Dist. 1975).
[232] *Id.*
[233] *People v. Holveck*, 141 Ill.2d 84 (1991).
[234] *Globe Newspaper Co. v. Superior Court for the County of Norfolk*, 457 U.S. 596, 606-607 (1982).
[235] *Id.* at 607-608.

Recommendations for integrated justice information systems

Agencies contemplating the development of integrated justice information systems face many substantial challenges. One of the most significant challenges is the lack of guidance for dealing with public apprehension regarding the government's enhanced ability to collect, analyze, and share substantial amounts of personally identifiable information for law enforcement purposes. Our nation has already seen several pilot programs to share justice information fail due to their inability to address these concerns. Yet there is no comprehensive document that sets forth the public's privacy concerns and explains what justice practitioners and system designers can do to assuage these concerns.

Although it is far from comprehensive, the subcommittee hopes that this report, and the volumes that will follow in the series, is a step in the right direction. The previous section set forth Illinois's existing mandatory and permissible information sharing practices; it also provided some specific recommendations concerning the Illinois justice system's treatment of the types of information traditionally utilized to make sound decisions. The recommendations that follow, however, are broader in scope. Other documents have suggested certain processes that can be followed to develop a privacy policy.[236] There is, however, little guidance concerning the recommended substance of those policies. This section is intended to fill this gap by providing justice agencies with some advice on the substance of their privacy policies.

Directly confront integrated justice privacy risks

It is important for individuals who develop and use integrated justice information systems to understand the risks to privacy created by the enhanced collection, analysis, and sharing of information for law enforcement purposes. It is equally important for justice agencies to address those privacy risks directly. Anything less than directly confronting the privacy risks created by integrating justice information systems endangers the success of the initiative. This discussion focuses on the privacy risks identified at the beginning of this report. Although the risks fall into three categories, they can all be addressed using similar methods, namely by holding the justice system accountable for what information it collects and how it uses that information. Failing to include sufficient oversight and transparency in a privacy policy is certain to undermine any integrated justice initiative.

Chilling effects

Integrated justice information systems increase the amount of information about individuals that is made available to justice practitioners. This is true despite the fact that the information is already available to justice officials in a non-compiled form. Combining this information creates the risk that individuals will become more cautious in the exercise of their protected rights of expression, protest, association, and political participation. To diminish these risks, integrated

[236] *See* Global Justice Information Sharing Initiative, U.S. DEP'T OF JUST., Privacy Policy Development Guide (2005).

justice information systems should be as transparent as possible and subject to clearly defined limits and effective oversight.[237]

One method to address the potential chilling effects of integrated justice information systems may be to set an acceptable error rate for a particular application in the context of its use.[238] This does not suggest that these error rates can be perfectly calculated; rather, any such analysis must take into account the totality of the circumstances at the point and time the information system is being used to generate investigative leads. Factors that weigh into the totality of circumstances analysis include the scope and method of inquiry, the sensitivity of the data being analyzed, and the particular crime or threat being investigated. Admittedly, this type of error rate analysis does not lend itself to rigid proscriptions. But acknowledging that error rates impact the public's perception of the appropriate uses of integrated justice information systems and taking steps to incorporate error rates into information sharing policies may have a considerable effect on the public's acceptance of the system.

Information processing risks

Information processing risks are implicated by the quality of data contained in source systems and the accuracy of the compilation that takes place when records about individuals are aggregated from multiple sources. 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.[239]

A concern that emerges as integrated justice information systems compile greater amounts of data for law enforcement purposes is that the government will mismanage or misinterpret information relating to an individual with real-world consequences to that individual. Incorporating into the system procedural protections and technical features that recognize the potential for error and permit due process mechanisms to correct or discard bad data can ameliorate this aggregation risk.[240] Less directly, an agency developing an integrated system can address this data processing risk by developing appropriate error rates for each type of analysis or matching conducted by the system. This is the same mechanism used to reduce the chilling effect discussed above.[241]

During the Privacy Policy Subcommittee's discussions, a concern arose that an integrated justice information system would function like an "electronic grand jury" (i.e. automatically analyzing its data stores to identify individuals it believes are committing crimes). To address this concern, agencies may consider making it clear to the public that these technologies are utilized only as investigative tools to allocate law enforcement resources, and that the data contained therein will

[237] *See* Technology and Privacy Advisory Committee, U.S. DEP'T OF DEFENSE, Safeguarding Privacy in the Fight Against Terrorism 36 (March 2004) ("TAPAC Report").
[238] *See* K. A. Taipale, *Technology, Security And Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 7 YALE J.L. & TECH. 123, 147-8 (2005).
[239] TAPAC Report at 39.
[240] *See* Taipale, *supra* note 238 at 157.
[241] *See* Taipale, *supra* note 238 at 156.

not be used for evidentiary purposes.[242] Data aggregation and analysis are not substitutes for human decision-making.

Information dissemination risks

Integrated justice information systems make substantial amounts of information available to justice decision-makers. The amount of information collected and maintained by integrated information systems also increases the potential for harm if that information is misused. 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.[243]

In some instances, the potential for abuse of a set of data is so great that those developing an integrated justice information system might consider not even collecting it. Already Illinois law permits certain individuals to either provide alternate address information to the government or withhold the information completely. For instance, a victim of domestic violence can omit her residential address from her petition for a protective order where the disclosure would risk abuse or reveal the confidential address of a domestic violence shelter.[244] Domestic violence victims can also participate in an address confidentiality program under which the victim can request that State and local agencies use the substitute address designated by the Attorney General as her address when creating a new public record.[245] Similarly, a police officer may furnish the address of his police headquarters instead of his residence address when registering his vehicles.[246] The same right extends to any family members residing with the officer.

This is not to say that excluding particular types of information from an integrated justice information system is a feasible option in all circumstances. In other cases, several technologies may provide a method of protecting exceptionally sensitive pieces of information. For instance, agencies can anonymize the personally identifying information contained in their system. By using a hash algorithm, personal data (e.g., the name and address of a sexual assault victim) can be represented in the system as an encrypted digital signature that does not reveal the victim's identity but permits the data to be exchanged or matched against other data. If a match occurs, the justice practitioner would then follow appropriate procedures before being granted access to the victim's identity. This and additional types of technologies that protect privacy will be discussed in greater detail in future volumes of the Privacy Policy Guidance series.

Sound privacy principles for integrated justice information systems

In 1973, the U.S. Department of Health, Education, and Welfare published a groundbreaking report responding to concerns that harmful consequences may result from the storing of personal information in computer systems. That report, entitled "Records, Computers and the Rights of

[242] *See* Taipale, *supra* note 238 at 157.
[243] *See* Taipale, *supra* note 238 at 151.
[244] 750 ILCS 60/203(b); Similarly, if the petitioner is seeking to have a child protected by the order, the petitioner may omit the child's school address where the disclosure of the school's location would risk abuse. 750 ILCS 60/203(c).
[245] *See* 750 ILCS 61/1 –/45.
[246] 625 ILCS 5/3-405.

Citizens," articulated several principles the department deemed essential to the fair collection, use, storage, and dissemination of personal information by electronic information systems.[247] The report was one of the earliest acknowledgements by the federal government that the public's privacy needed to be protected against arbitrary and abusive record-keeping practices. The report also recognized the need to establish standards of record-keeping practices appropriate for the computer age.

The Fair Information Practices are a set of standards governing the collection and use of personal data and addressing issues of privacy and accuracy. The practices include eight guiding principles that evolved from the 1973 report:

1. *Collection Limitation Principle* – There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. *Data Quality Principle* – Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. *Purpose Specification Principle* – The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. *Use Limitation Principle* – Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except: (a) with the consent of the data subject; or (b) by the authority of law.
5. *Security Safeguards Principle* – Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. *Openness Principle* – There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. *Individual Participation Principle* – An individual should have the right to: (a) obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
8. *Accountability Principle* – A data controller should be accountable for complying with measures which give effect to the principles stated above.

Although universally recognized as a solid foundation on which to build privacy legislation and policies, the fair information practices were not originally developed to operate within the

[247] U.S. DEP'T OF HEALTH, EDUC., & WELFARE, Records, Computers and the Rights of Citizens: Report of The Secretary's Advisory Committee on Automated Personal Data Systems xx-xxi (1973), available at http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

context of the justice system. The National Criminal Justice Association and the Global Justice Information Sharing Initiative (Global) Advisory Committee have both considered the need to modify the practices to include the flexibility necessary to ensure public safety by providing relevant information to justice decision-makers.[248] However, modifying the practices themselves, as opposed to creating discrete exceptions to their operation, risks stripping the fair information practices of their significance as guidelines.

Instead of modifying the fair information practices, this report proposes a new model that can provide guidance to justice practitioners and systems designers. The six principles that follow reflect the philosophical underpinnings of the justice system's collection, use, and dissemination of the information it requires to promote the public's safety. These principles, and their accompanying commentaries, were developed in the context of electronic information sharing and it is hoped that they can help justice agencies resolve privacy issues that might not be specifically addressed in existing laws or policies.

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.

Commentary

Integrated justice information systems should conform to existing and evolving notions of privacy and civil liberties. Civil liberties are fundamental individual rights such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. It is these rights that protect individuals from improper government action and arbitrary governmental interference.[249]

This is a traditional check on the justice system that is appropriately applied to the tools utilized by justice practitioners. The goal of incorporating this principle into a privacy policy is to promote the public's confidence and trust in law enforcement information systems by subjecting them to the same legislative and judicial checks and balances that legitimately constrain the administration of justice.

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.

Commentary

There is a growing recognition that promoting public confidence in the administration of justice is one of the primary goals of good government. One way to promote public confidence is to increase the transparency surrounding how information is managed by the Illinois justice system, even if the information itself cannot be released to the public. Doing so serves two purposes: (1) it invites constructive comments regarding the

[248] *See* NAT'L CRIM. JUST. ASS'N, Justice Information Privacy Guideline (2002), available at http://www.ncja.org/pdf/privacyguideline.pdf; Global Privacy and Information Quality Working Group web page http://www.it.ojp.gov/topic.jsp?topic_id=55#3706 (indicating that some of the individual principles may not apply in all instances of an integrated justice system).

[249] BUREAU OF JUSTICE ASSISTANCE, U.S. DEP'T OF JUST., National Criminal Intelligence Sharing Plan 5 (June 2005).

operation of the justice system, and (2) it is a mechanism to hold the justice system accountable for adhering to the very rules and procedures it develops.

This principle is limited to the public disclosure of policies, procedures, and practices regulating the collection, use, and dissemination of data contained in an integrated justice information system. The level of detail contained in these documents and practices will understandably vary based upon the audience to which they are directed. For instance, a system administrator will need more detail than a mere user of the system. There may also be users with varying amounts of access to the system. A user with greater access permissions will be subject to additional and more detailed regulations than a user with more limited access. Although agencies are not required to disclose any documents that may disclose unique or specialized investigative techniques that are not generally used and known,[250] the type of policies recommended by this report should be made publicly available.

3. ALL INSTANCES OF JUSTICE INFORMATION SHARING AND DATA MODIFICATION WILL BE RECORDED TO ENSURE ACCOUNTABILITY FOR THE TRANSACTIONS.

Commentary

In an age where information is increasingly equated with power, it is important that new information systems be developed with accountability mechanisms in place. The goal of this principle is to deter and discover users' abuse and misuse of an integrated justice information system. The principle calls for immutable audit trails to be built into integrated justice information systems and implies that system audit logs will be reviewed for inconsistencies that raise a suspicion of abuse. Keeping records of who has access to what information and whether a person has modified a record might discourage some access. Nevertheless, such audit capabilities can be an effective means to discourage unnecessary or inappropriate use of the system and trace any improper uses to the wrongful party.

4. EVERY REASONABLE EFFORT WILL BE MADE TO ENSURE THAT JUSTICE INFORMATION IS COMPLETE, ACCURATE, AND TIMELY.

Commentary

For decades the Illinois justice system has been concerned with ensuring that the information utilized by justice practitioners is accurate, complete, and current. Nevertheless, these concerns take on added significance in the context of integrated information systems because the goal of these systems is to increase the amount of electronic information collected and shared throughout the justice system. Agencies incorporating this principle into their policies should carefully consider the accuracy of data contained in source systems and document the specific protocols that will be used to locate and correct erroneous information. By making these considerations and procedures available for inspection, justice agencies can forestall the public's data quality concerns.

[250] 5 ILCS 140/7(1)(c)(v) and *In Re Daniels*, 240 Ill.App.3d 314 (1st Dist. 1992) (utilizing exemptions contained in the FOIA as a basis for recognizing investigatory privilege to not disclose investigatory records).

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.

Commentary

Existing laws already provide individuals with limited rights to access and review certain types of justice information.[251] Setting an appropriate level of access and review in the context of an integrated justice information system was a point of contention for subcommittee members. Some recommended broad rights on the grounds that greater transparency and error correction promoted public trust in the administration of justice. Others, premised upon many ways an individual could be incidentally mentioned in an integrated justice system, advocated limiting individuals' access and review rights to instances where the government labeled that individual a suspect or offender. These members argued that it was not the justice system's purpose to provide a new service whereby individuals could request and be provided a comprehensive list of every time they are referred to in justice records. This principle does not set a specific scope or breadth of the right of access and review granted to individuals. The principle does, however, call for agencies to articulate exceptions to the right to review and challenge.

6. VICTIMS AND WITNESSES OF CRIME SHALL BE TREATED WITH FAIRNESS AND RESPECT FOR THEIR DIGNITY AND PRIVACY THROUGHOUT THE JUSTICE SYSTEM.

Commentary

This principle has its root in Illinois law.[252] It is based upon the recognition that victims and witnesses are not voluntary participants in the justice process. The subcommittee's findings revealed that victims of different types of crimes have different degrees of privacy protections. The members discussed the difficulty of classifying victims and of implementing these varying levels of protection in an integrated justice information system. Even though the subcommittee was unable to make recommendations concerning these technological and policy questions, the principle, and Illinois law, affords certain rights and considerations to victims and witnesses due to the essential nature of their role in the administration of justice.

[251] *See* 28 C.F.R. § 20.21(g); implemented by 20 ILCS 2630/7 and ILL. ADMIN. CODE tit. 20 § 1210.20 (providing individuals the right to review and challenge their criminal history record information contained in the state's official repository) *c.f.* Smith v. Cook County Probation Department, 151 Ill.App.3d 136 (1st Dist. 1986) (denying a probationer access to probation records concerning him under FOIA).

[252] Ill. Const. Art. I, § 8.1; 725 ILCS 120/2.

Conclusion

Illinois justice agencies should be encouraged to use advanced information technologies to collect, analyze, and share digital information to fight crime, but should protect privacy while doing so. The recommendations contained in this report are intended to help agencies address the public's privacy concerns as they develop and use integrated information systems.

The Privacy Policy Subcommittee's work is far from complete; Appendix A discusses the group's continuing efforts. Ultimately, it is the Privacy Policy Subcommittee's goal to develop recommendations that will provide justice agencies with the tools they need to enhance public safety confident in the knowledge that they are respecting the public's privacy and liberty interests.

Table 1: Information collected about prisoners

The amount of information collected about prisoners depends upon whether the prisoner is housed in a municipal lock-up, county jail, or state prison. The differences in the amount and types of information collected are the result of the role of these facilities, the length of a prisoner's stay, and the available treatment programs. The types of information collected by each institution are listed below.[253]

State Prison	County Jail	Municipal Lock-up
❑ Identifying information	❑ Identifying information	❑ Identifying information
❑ Emergency contact	❑ Emergency contact	❑ Emergency contact
❑ Employment history	❑ Occupation	❑ Occupation
❑ Offense information	❑ Offense information	❑ Offense information
❑ Date and time of admission	❑ Date and time of admission	❑ Date and time of admission
❑ Criminal history record information	❑ Criminal history record information	❑ Criminal history record information
❑ Personal property record	❑ Personal property record	❑ Personal property record
❑ Mittimus or judgment order including sentence and court findings concerning offender status.	❑ Case disposition, judge, and trial court	❑ Disposition of case and authority
❑ Number of days in custody and transfer records	❑ Date of release or transfer	❑ Date of release or transfer
❑ Parole plans and reports	❑ Probation or parole status	
❑ Medical or mental health records or summaries	❑ Physical and mental health assessments	
❑ Health and physical condition	❑ Health and physical condition	
❑ History of substance abuse	❑ History of substance abuse	
❑ Educational history	❑ Education level	
❑ Religion or religious preference	❑ Religion or religious preference	
❑ Sexual orientation	❑ Sexual orientation	
❑ Gang activity, affiliations, and ranks	❑ Gang activity	
❑ Record of disciplinary infractions and dispositions	❑ Record of misconduct and subsequent discipline administered	
	❑ Name and telephone number of the prisoner's attorney	
❑ Presentence reports	❑ Prisoner status: pretrial; awaiting sentence; sentenced	
❑ Basis for imposing sentence		
❑ State's Attorney's statement of facts		

[253] Sources: State Prisons (730 ILCS 5/3-2-5(c); 730 ILCS 5/3-5-1–2; 730 ILCS 5/3-8-1–2; ILL. ADMIN. CODE tit. 20 §§ 701.60; 107.20; 503.20); County Jails (ILL. ADMIN. CODE tit. 20 §§ 701.40; 701.70); Municipal Lock-Ups (ILL. ADMIN. CODE tit. 20 § 720.120).

Table 2: Categories of information most useful for traditional crime analysis

Police agencies utilize crime analysis to prevent and suppress crime, apprehend offenders, and recover stolen property.[254] Crime analysis is usually conducted on offenses with discernable patterns and trends that can be prevented or reduced through the implementation of directed action plans.[255] A review of existing police crime analysis operations reveals that burglary, robbery, auto theft, larceny, fraud, sex crimes, aggravated assaults, and murder are the crimes most appropriate for crime analysis.[256] Experienced analysts have found that the factors listed below (the numbers in parentheses suggest the order in which the data should be searched) often help determine if a pattern exists.[257]

Residential Burglaries	Commercial Burglaries
❑ Geographic factors (1) ❑ Time factors (2) ❑ Property loss descriptors (2) ❑ Victim descriptors[258] (2) ❑ Physical evidence descriptors (2) ❑ Specific modus operandi factors[259] (2) ❑ Suspect vehicle descriptors (3) ❑ Suspect descriptors (3)	❑ Geographic factors (1) ❑ Victim descriptors (1) ❑ Specific modus operandi factors (1) ❑ Property loss descriptors (2) ❑ Physical evidence descriptors (2) ❑ Time factors (3) ❑ Suspect vehicle descriptors (3) ❑ Suspect descriptors (3)
Thefts From Vehicles	**Sexual Offenses**
❑ Geographic factors (1) ❑ Property loss descriptors (1) ❑ Suspect vehicle descriptors (1) ❑ Time factors (2) ❑ Victim descriptors[260] (2) ❑ Physical evidence descriptors (2) ❑ Specific modus operandi factors (2) ❑ Suspect descriptors (3)	❑ Time factors (1) ❑ Victim descriptors (1) ❑ Suspect descriptors (1) ❑ Victim-suspect relationship (1) ❑ Geographic factors (2) ❑ Physical evidence descriptors (2) ❑ Specific modus operandi factors[261] (2) ❑ Suspect vehicle descriptors (2)

[254] Steven Gottlieb, *et al.*, Crime Analysis: From First Report to Final Arrest 14-16 (1994)
[255] *Id.*
[256] *Id.* at 133.
[257] *Id.* at 318-320; DEP'T OF THE ARMY, U.S. DEP'T OF DEF., Physical Security FM 3-19.30 B-8 (2001).
[258] Victim descriptors for burglaries include the type of building that was attacked and whether it was occupied or unoccupied.
[259] MO factors for burglaries include the point of entry (i.e., door, window, etc.) and the method of entry (i.e., unsecured door, forced door, forced window, etc.).
[260] Victim descriptors for thefts from vehicles include whether the vehicle or property was secured or unsecured and the type of vehicle or property stolen (sports car, motorcycle, stereo, tires, etc.).
[261] MO factors for sexual offenses include the degree of force used against the victim.

Strong-Arm Robberies	Armed Robberies
❑ Geographic factors (1) ❑ Time factors (1) ❑ Victim descriptors[262] (1) ❑ Property loss descriptors (2) ❑ Physical evidence descriptors (2) ❑ Specific modus operandi factors[263] (2) ❑ Suspect descriptors (2) ❑ Suspect vehicle descriptors (3)	❑ Geographic factors (1) ❑ Time factors (1) ❑ Suspect descriptors (1) ❑ Victim descriptors (2) ❑ Specific modus operandi factors (2) ❑ Suspect vehicle descriptors (2) ❑ Property loss descriptors (3) ❑ Physical evidence descriptors (3)

[262] Victim descriptors for robberies include the injuries the victim suffered and any actions by the victim that contributed to his being targeted.
[263] MO factors for robberies include the number of perpetrators and the type of weapon used during the offense.

Appendix A: Privacy Policy Guidance series

The goal of the *Privacy Policy Guidance* series is to help Illinois justice agencies develop privacy policies for their integrated justice information systems. This report, and the volumes that will follow, describes the public's privacy concerns and provides recommendations to justice practitioners and system designers about how to address those concerns. Because many agencies are already moving forward with the development of integrated justice information systems, the subcommittee decided to publish its recommendations in a series of reports to ensure that agencies receive guidance as it becomes available.

Ultimately, the *Privacy Policy Guidance* series will consist of six volumes. The subcommittee has prioritized the issues that it will address in the hopes of keeping abreast of justice agencies' systems development. The topics that will be addressed in each volume are set forth below.

Volume 1

This report focuses on the types of information traditionally collected, used, and disseminated about the actors in the Illinois justice system. It also proposes a set of principles that should be incorporated into any integrated justice system's privacy policy.

Volume 2

Several initiatives currently underway that will improve the electronic sharing of incident report information. Specifically, Illinois State Police is developing the Illinois Citizen and Law Enforcement Analysis and Reporting (I-CLEAR) system. A primary component of this system will be a data warehouse that will store, analyze, and disseminate various types of justice information including incident reports from municipal and county police departments across the state. Furthermore, the Federal Bureau of Investigation is continuing to develop the National Data Exchange (N-DEx) system, which will provide a nationwide capability to exchange data derived from incident and event reports with other agencies. The Department of Justice has largely left the states to determine the amount of police incident report data that will be transmitted to the N-DEx system.

Volume 2 of the series will identify the privacy concerns created by the enhanced collection, analysis, and sharing of electronic police incident report information made possible by several initiatives under development in Illinois. The report will also address these privacy concerns by developing clear guidance on how to properly treat the types of sensitive data that are frequently included in police incident reports.

Volume 3

There are several types of data that might be collected, used, and disseminated by an integrated justice system that don't fall neatly into the actor-based or incident-based discussions of the first two volumes. Volume 3 of the *Privacy Policy Guidance* series will discuss the privacy issues surrounding several of these types of information, including, but not limited to, officer safety

information; Social Security numbers; fingerprints; DNA profiles; medical information; expunged and sealed records; warrants; offender registration information; and statistical data.

Volume 4

The fourth volume of the series will focus on the accountability and oversight of integrated justice information systems. Specifically, it will contain recommendations concerning privacy policy compliance audits and how to ensure the accuracy of data contained in justice information systems.

Volume 5

Privacy Policy Guidance, Volume 5 will focus on the collection, use, and dissemination of juvenile justice information in an integrated justice information system. It will discuss statutory requirements to keep juvenile data separate and to provide greater levels of privacy for minors who come into contact with the justice system.

Volume 6

Volume 6 will review the types of intelligence information gathered by the Illinois justice system and discuss the proper treatment of this information taking into account federal and state laws regulating this information.