# Drafting Privacy Policy in an Integrated Justice Environment:
A PROCESS PROPOSAL

**Step 1:**

Proposed Privacy Committee Membership

**Step 2:**

Discussion of Broad Privacy Policy Design Principles

(A) The Fair Information Practices (FIPs) and Their Limitations

(B) The Inevitable Decline of Practical Obscurity and the Aggregation Problem

**Step 3:**

Compile Statutory Responses to Privacy Concerns

(A) Federal Statutes & Regulations

(B) Illinois Statutes & Regulations

(C) Justice Agencies' Current Privacy Policies

**Step 4:**

Policy Creation: Privacy Issues & Desired Practices

(A) Information Life Cycle

(B) Individual Access to Records Contained in Integrated Justice Information Systems

(C) Accountability of the Integrated Justice System

(D) Availability of Statistical Information Made Easily Available by Integrated Justice Information Systems

(E) Accessibility of Victim & Witness Information

(F) Accessibility of Offender and Victim Health information

(G) Collection, Use, & Dissemination of Social Security Numbers

**Step 5:**

The Privacy Committee Final Report

# Step 1
## Proposed Privacy Committee Membership

By its very definition, an integrated justice system encompasses interagency, interdisciplinary, and intergovernmental information systems that access, collect, use, and disseminate critical information at key decisions points throughout the justice process.[1] Because of the multiple agency nature of an integrated justice system initiative, the utilization of a committee to draft the privacy policy is vital if that policy is to bind the participating agencies. Furthermore, the collaboration of participating justice practitioners on the development of the privacy policy will help ensure their agencies' buy-in of terms contained within completed policy.

While essential to the development of the privacy policy, merely including participating agencies will not accomplish the goals of the privacy policy. Rather, by virtue of its subject matter, the privacy committee will require representatives from academia, victims' rights advocates, media and commercial sectors, as well as the general public to be complete. These parties are necessary to ensure a sufficiently diverse committee able to identify relevant privacy issues and articulate potentially opposing privacy policy perspectives.[2] If one of the goals of the integrated justice system is to secure legislation enacting the privacy policy, then a representative from the state legislature may also be appropriate. In addition to ensuring that the privacy committee includes representatives with diverse privacy interests, this broad range of representation will also facilitate public buy-in of the integrated justice system's privacy policy.

IIJIS PRIVACY COMMITTEE
(__ members)

*Criminal Justice System:*
Illinois State Police
Illinois Criminal Justice Information Authority
Illinois Department of Corrections
Illinois Association of Court Clerks Member
Illinois Association of Chiefs of Police Member
Illinois Sheriffs' Association Member
State's Attorneys' Association Member
Illinois Probation & Court Services Association
Public Defenders' Association Member
Circuit Court Clerk of Cook County
Chief Judge's Office, Cook County
Chicago Police Department

*Academia:*
John Marshall Law School *Center for Information Technology and Privacy Law*
Chicago-Kent College of Law *Illinois Technology Center for Law & the Public Interest*

*Victims' Rights Advocates:*
Illinois Coalition Against Domestic Violence
Illinois Coalition Against Sexual Assault

[1] NATIONAL CRIMINAL JUSTICE ASSOCIATION, JUSTICE INFORMATION PRIVACY GUIDELINE 16 (2002) *available on-line at* <http://www.ncja.org/pdf/privacyguideline.pdf> [hereinafter *Guideline*].
[2] Id. at 36.

*Media:*
Illinois Press Association

*Commercial Sector:*
Chicagoland Chamber of Commerce
ISP will determine the largest users of CHRI [this will probably include healthcare and teachers although these sectors' interests are protected by statute]

*General Public Member:*
Member of the Illinois Criminal Justice Information Authority
Illinois State Bar Association Member

Most often, background research would be prepared beforehand by privacy committee staff whose responsibility it will be to take the raw privacy material and synthesize it into useful papers for committee members. By providing the committee with clear, concise, and focused research on privacy issues, the committee can make informed policy decisions, fully aware of their potential consequences and anticipated repercussions.

In some instances, however, it may be desirable for committee members to draft short position papers supporting or opposing a specific privacy policy based upon that policy's affect upon their agency. This would allow the person or agency with the most detailed knowledge to educate the committee on the effects of the proposed policy. Whenever possible, a supporting and an opposing paper should be provided to the committee.

While important to any privacy policy creation endeavor, issues such as juvenile confidentiality and criminal justice intelligence data sharing are beyond the scope of this committee's expertise. It is expected that specific committees would be convened with memberships better equipped to address these complex issues.

# Step 2

## Discussion of Broad Privacy Policy Design Principles

While many state and federal privacy provisions exist to protect justice information, current statutes and policies may not be sufficient to encompass the collection, analysis, use, and dissemination of justice information within an integrated justice system.[3] Current privacy provisions may be insufficient for two main reasons. First, the expanded information sharing capabilities of an integrated justice system are likely to blur the lines between traditional and non-traditional justice information. Non-traditional justice information may include sensitive social service, educational, and medical records that once in the possession of the justice enterprise may fall outside the scope of existing legal frameworks.[4]

[3] Paul F. Kendall et al., Gathering, Analysis, and Sharing of Criminal Justice Information by Justice Agencies: The Need for Principles of Responsible Use, 21st Annual International Conference on Data Protection and Information Privacy, Hong Kong 16 (Sept. 1999) (visited May 20, 2003) <http://www.pco.org.hk/english/infocentre/files/kendall(formatted).doc>.
[4] Guideline, supra note 1 at 19.

Secondly, utilizing the expanded information sharing capabilities of an integrated justice system, justice agencies can gather, accumulate, and analyze various types of information to create a digital biography of an individual which may then be shared by components of the justice system in order to make decisions affecting that individual.[5] Where existing legal frameworks fail to address these issues, it is appropriate for the integrated justice system to address these issues in a manner consistent with the State's existing privacy protections.

To do this, the privacy committee needs to be familiar with relevant Federal and State privacy policies as well as the theoretical bases for those policies. This requires a review of relevant statutes and regulations as well as the eight primary fair information practices (FIPs) incorporated therein. It is important to note that the FIPs remain universally recognized as a solid foundation on which to build everything from privacy legislation and policies to self-regulated privacy standards for the private sector.

## A. THE FAIR INFORMATION PRACTICES (FIPS) AND THEIR LIMITATIONS

The committee should be provided with a more detailed discussion of each FIP as well as an understanding of the practices' interaction with one another. Generally speaking, the function of the FIPs is to limit the collection, use, and disclosure of information in the absence of a compelling interest. However, because there are several compelling interests involved with the justice enterprise, the exceptions threaten to swallow the FIPs in the integrated justice context.

### **FIP 1.** Purpose Specification

An agency's purpose for collecting personal information should be specified in writing not later than the time of data collection. Each component of the justice system should have a set of stated purposes for collecting personal information. These purpose statements should be harmonized in an integrated setting.

*Limitations of Purpose Specification:*

- Too narrowly or too broadly drafting purpose statements dramatically reduces the efficacy of the Purpose Specification FIP and drafting meaningful purpose statements will prove very difficult.
- An integrated justice system and its component agencies will be subject to public access requirements by virtue of their governmental nature. Being subject to a public access requirement may influence the subsequent use and disclosure of personal information in a manner potentially inconsistent with the indicated purposes for which the information was initially collected.
- Purpose statements are limited to the collection and subsequent use of *existing* personal information by justice agencies and thus they do not impact information *created* by the activities of the justice system such as fingerprint verified identification numbers and statistical data.

### **FIP2.** Collection Limitation

Limits on the collection of personal information take two forms: means and relevance. First, personal information for use in the justice system should only be acquired through lawful and fair means. Second, agencies should avoid collecting extraneous personal information.

[5] Kendall et al., supra note 3 at 2. (using "virtual picture" nomenclature in place of Professor Solove's "digital biography"); *see generally* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137 (2002).

*Limitations of Collection Limitation:*

- The past thirty years of Fourth Amendment case law have provided justice practitioners a great deal of guidance on what constitutes fair and lawful means of collecting information.
- Restricting the collection of 'extraneous' information poses a more complex challenge because of the difficulties involved with defining the term extraneous and the nature of law enforcement investigations.[6]

### **FIP3.** Use Limitation

Agencies should limit the use and disclosure of personal information to the purposes stated in their purpose statement. However, personal information can be used for any number of reasons not related to the justice system when (a) the subject of the data consents, (b) the agency has the legal authority to do so, (c) the safety of the community is at issue, or (d) a public access policy permits the disclosure.

*Limitations of Use Limitation:*

- The definition of consent must be address in detail in order to explain its precise scope [i.e., whether a global waiver of information is sufficient to fulfill the consent requirement or if a more precise and unambiguous agreement is necessary].
- What constitutes sufficient risk to the community's safety is not currently articulated under the public safety exception. [This is significant because unequal privacy treatment may result if the privacy policy does not inform what constitutes a sufficient risk necessitating a disclosure of information.[7]]
- Valid uses of personal information also include its retention and destruction; traditionally, the FIPs call for the destruction of personal information when it no longer serves its original processing purposes.

### **FIP4.** Data Quality

Agencies should be required to verify the accuracy, completeness, and currency of their information. This FIP includes provisions for (a) data source identification, (b) data management, (c) record retention, and (d) administrative standards for modifying an incorrect record.

*Limitations of the Data Quality FIP:*

- Several difficulties exist in measuring the accuracy, completeness, and timeliness of expungement processes.
- Raw investigative as well as intelligence data may be fraught with inaccuracies until it is verified or crosschecked with other data.

---

[6] For example, the Department of Justice proposed to exempt several of the Federal Bureau of Investigation's information systems from the Privacy Act "because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed…would limit the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement." Privacy Act of 1974; Implementation, 68 Fed. Reg. 4974, (2003) (to be codified at 28 C.F.R. pt 16) (proposed Jan. 31, 2003).

[7] For instance, while we expect the police to provide a sketch or photo of a suspected murderer at large in the community, does this exception also allow a local police department to distribute a flyer entitled "Active Shoplifters" containing the arrest booking photos of shoplifting suspects who were arrested but not necessarily convicted? While not addressing this precise question, Paul v. Davis, 424 U.S. 693 (1976) contains a factually similar situation.

**FIP5.** Openness

Agencies should provide notice about how they collect, maintain, and disseminate the personal information they collect. Agencies should also communicate to affected individuals that their justice records were requested, sold, or released to third parties.

*Limitation of the Openness FIP:*

- Should the justice system provide notice to affected persons when their justice records are requested, sold, or released to third parties?
- Does the failure to provide such notice could deny the collector of the information the right to use it?

**FIP6.** Individual Participation

Agencies should allow easy and convenient access by individuals to their personal information. Except where it would compromise an investigation, case, or court proceeding, individuals should have the right to:

(a) Obtain confirmation of whether or not the agency has data relating to him;
(b) Have the data communicated to him in a reasonable time and manner at reasonable cost;
(c) Challenge a denied request under (a) and (b); &
(d) Challenge incorrect data and if successful have the data erased, rectified, completed, or amended with notification to all parties who received the incorrect information.

*Limitations of Individual Participation:*

- Standards should be developed for how quickly and how often the integrated justice system should provide the requested information to the data subject.
- The form and manner in which the information is provided to the requestor should be standardized.
- The information reviewed should include how the information is being used, whether it is being used, and to whom the information was disclosed.
- What are the administrative standards for modifying an incorrect record?

**FIP7.** Security Safeguards

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data. Because security is an area of privacy that is driven by available technologies and because technology should not drive privacy policy, security safeguards will most likely only be addressed as an FIP.

**FIP8.** Accountability

Agencies should have a means of ensuring that their policies are adhered to. Due process mechanisms should be created through which an individual may challenge the information system's compliance with any of the principles made a part of the policy. A timely and fair response should be provided to the challenging party. In the instance of a breach, penalties for breaching agencies should be available and affected individuals contacted and informed of their recourses.

*Limitations of Accountability:*

- Administrative procedures through which the integrated justice system's compliance with the privacy policy can be challenged will need to be developed.
- What is the feasibility of periodic audits to determine the integrated justice system's level of compliance with the privacy policy?

- Who will determine the penalties for breaching any of the provisions of the privacy policy?

## B. THE INEVITABLE DECLINE OF PRACTICAL OBSCURITY AND THE AGGREGATION PROBLEM

Arguably the most significant of privacy issues created by an integrated justice system can be attributed to the decline of practical obscurity. Integrated justice systems are designed to enhance querying capabilities of regional, statewide, and national databases as well as aggregate and report critical information regarding the people or cases queried. Integration initiates are efforts to improve the operation of the justice enterprise by eliminating barriers to accessing information. Those barriers are the substance of practical obscurity.

The rubber hits the road where freedom of information acts provide for the release of vast quantities of information that were previously obscure and information technologies provide the capability to aggregate those records into personal dossiers. Freedom of information acts serve three purposes: "first and most important, ensure public access to the information necessary to evaluate the conduct of government officials; second, ensure pubic access to information concerning public policy; and third, protect against secret laws, rules and decision making."[8] Thus, freedom of information acts created a checks and balances system in which the public could monitor and regulate government agencies.[9] Statutes serving these purposes are often referred to as "open access," "right to know," or "sunshine" laws.

Much of the information contained in public records, however, does not necessarily shed light on the way government carries out its functions; rather, this information reveals more about the people who are the subjects of the government's regulatory machinery.[10] Freedom of information acts turn agencies into information brokers instead of providing a window for public oversight of governmental operations.[11] Add the technological capability to relate disparate pieces of a person's information to this state of affairs and the stage is set for the data aggregation problem.

Viewed in isolation, each piece of information created by our day-to-day activities is not at all telling; however, viewed in combination, that information begins to paint a portrait of our personalities.[12] This is the aggregation problem. It arises from the fact that integrated systems enable information from disparate sources to be easily collected and analyzed. In a system such as this, information breeds information: information such as one's Social Security number, while not in and of itself informative, provides access to a host of additional information such as financial, educational, and medical records.

---

[8] Solove, *Access and Aggregation*, supra note 5 at 1161 *citing* Fred H. Cate et al., The Right to Privacy and the Public's Right to Know: The "Central Purpose" of the Freedom of Information Act, 46 ADMIN. L. REV. 41, 65 (1994).
[9] *See* Victoria S. Salzmann, *Are Public Records Really Public?: The Collision Between the Right to Privacy and the Release of Public Court Records Over the Internet*, 52 BAYLOR L. REV. 355, 357-359 (2000)
[10] Solove, *Access and Aggregation*, supra note 5 at 1195-1196.
[11] Salzmann, supra note 9 at 358 *see also* Solove, *Access and Aggregation*, supra note 5 at 1196.
[12] Solove, *Access and Aggregation*, supra note 5 at 1185.

# Step 3

Compile Statutory Responses to Privacy Concerns

An analysis of Federal and Illinois law reveals a patchwork of statutes that can properly be characterized as "reactive rather than anticipatory, incremental rather than comprehensive, and fragmented rather than coherent."[13] Because of this eclectic approach, it is difficult to determine whether in combination these statutes collectively are greater than the sum of their parts or more accurately mirror Humpty-Dumpty after the great fall.

What protection federal and state laws do afford individuals must, however, be analyzed and presented to the privacy committee for its review and discussion. Research staff must sort through the eclectic array of federal and state laws that may influence how and to what extent information can be shared seamlessly within an integrated justice system. Additionally, laws that contain public access provisions should also be reviewed for any impact they may have.

Following is a substantial, but nevertheless partial, listing of Federal and Illinois statutes.

## A. FEDERAL STATUTES & REGULATIONS

*Justice Information:*

- The Omnibus Control Act and Safe Streets of 1968
- Criminal Justice Information Systems, 28 C.F.R. pt. 20
- Criminal Intelligence Systems Operating Policies, 28 C.F.R. pt. 23
- Identity Theft & Assumption Deterrence Act of 1998
- USA PATRIOT Act
- The Homeland Security Act of 2002
- The Foreign Intelligence Surveillance Act of 1978
- Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations

*Information Contained in Government Information Systems:*

- E-Government Act of 2002
- The Privacy Act of 1974
- The Freedom of Information Act of 1974
- The Electronic Freedom of Information Act of 1996
- The Privacy Protection Act
- The Federal Records Act
- The Paperwork Reduction Act of 1980

*Financial Information:*

- Financial Modernization Services Act
- The Gramm-Leach-Bliley Act of 1999
- The Right to Financial Privacy Act of 1978

[13] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan. L. Rev. 1393, 1444 *citing* Colin J. Bennett, *Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?*, in Technology and Privacy: The New Landscape 99, 113 (Philip E. Agre & Marc Rotenberg eds., 1997).

- The Fair Credit Reporting Act of 1970
- The Electronic Fund Transfer Act of 1978 and Regulation E
- Provisions of the IRS that mandate the privacy of taxpayer information

*Motor Vehicle Information:*

- The Driver's Privacy Protection Act of 1994

*Educational Information:*

- The Family Education Rights and Privacy Act of 1974

*Telecommunications Information:*

- The Children's Online Privacy Protection Act of 1998
- Child Online Protection Act of 1998
- The Electronic Communications Privacy Act of 1986
- The Computer Matching and Privacy Protection Act of 1988
- The Telephone Consumer Protection Act
- Video Privacy Protection Act
- The Computer Fraud and Abuse Act
- The Cable Communications Policy Act of 1984
- Telecommunications Act of 1996

*Health Information:*

- Health Insurance Portability and Accountability Act of 1996

B. ILLINOIS STATUTES & REGULATIONS

*Justice Information:*

Criminal Identification Act[14]
Firearm Owners Identification Card Act[15]
Illinois Uniform Conviction Information Act[16]
Department of State Police Law[17]
Probation And Probation Officers Act[18]
Statewide Organized Crime Database Act[19]
Unified Code Of Corrections[20]
Sex Offender & Child Murderer Community Notification Law[21]
Sex Offender Registration Act[22]
Sexually Violent Persons Commitment Act[23]
Statewide Senior Citizen Victimizer Database Act[24]

[14] 20 ILL. COMP. STAT. 2630/1 *et seq,. implemented by* ILL. ADMIN. CODE tit. 20 § 1210; ILL. ADMIN. CODE tit. 20 § 1240; ILL. ADMIN. CODE tit. 20 § 1265.
[15] 430 ILL. COMP. STAT. 65/1 *et seq.*
[16] 20 ILL. COMP. STAT. 2635/1 *et seq., implemented by* ILL. ADMIN. CODE tit. 20 § 1215.
[17] 20 ILL. COMP. STAT. 2605/2605-1 *et seq.*
[18] 730 ILL. COMP. STAT. 110/9 *et seq.*
[19] 20 ILL. COMP. STAT. 2640/1 *et seq.*
[20] 730 ILL. COMP. STAT. 5/1-1-1 *et seq., implemented by* ILL. ADMIN. CODE tit. 20 § 701; ILL. ADMIN. CODE tit. 20 § 720; ILL. ADMIN. CODE tit. 20 § 107; ILL. ADMIN. CODE tit. 20 § 1285.
[21] 730 ILL. COMP. STAT. 152/101 *et seq., implemented by* ILL. ADMIN. CODE tit. 20 § 1282.
[22] 730 ILL. COMP. STAT. 150/1 *et seq., implemented by* ILL. ADMIN. CODE tit. 20 § 1280.
[23] 725 ILL. COMP. STAT. 207/1 *et seq.*

*Information Contained in Government Information Systems:*
Illinois State Auditing Act[25]
Vital Records Act[26]

*Juvenile Information:*
Abused And Neglected Child Reporting Act[27]
Department of Children and Family Services Powers Law[28]
Intergovernmental Missing Child Recovery Act of 1984[29]

*Health Information:*
AIDS Confidentiality Act[30]
Alcoholism & Other Drug Abuse & Dependency Act[31]
Illinois Health Statistics Act[32]
Department of Public Health Powers And Duties Law[33]
Medical Patient Rights Act[34]
Mental Health & Developmental Disabilities Code[35]
Mental Health & Developmental Disabilities Confidentiality Act[36]

### C. JUSTICE AGENCIES' CURRENT PRIVACY POLICIES

Either during or after the research staff's investigation into relevant federal and state laws, committee members should be requested to provide their various agencies' official information use policies. These policies should be reviewed for the ways in which they implement the statutorily required privacy practices. Some of these policies may also provide reliable language that can be utilized in the integrated justice privacy policy.

## Step 4
Policy Creation: Privacy Issues & Desired Practices

It is expected that we will find that the majority of the IIJIS Privacy Policy is already written in the form of the many statutes and regulations already being implemented statewide. The challenge lies in compiling these diverse statutes and regulations into a single comprehensive document that can be easily referenced by justice practitioners.

---

[24] 20 ILL. COMP. STAT. 2645/1 *et seq.*
[25] 30 ILL. COMP. STAT. 5/1-1 *et seq.*
[26] 40 ILL. COMP. STAT. 535/1 *et seq., implemented by* ILL. ADMIN. CODE tit. 77 § 500.
[27] 325 ILL. COMP. STAT. 5/1 *et seq.*
[28] 20 ILL. COMP. STAT. 510/510-1 *et seq.*
[29] 325 ILL. COMP. STAT. 40/1 *et seq., implemented by* ILL. ADMIN. CODE tit. 20 § 1260.
[30] 410 ILL. COMP. STAT. 305/1 *et seq.*
[31] 20 ILL. COMP. STAT. 301/1-1 *et seq., implemented by* ILL. ADMIN. CODE tit. 77 § 2030.
[32] 410 ILL. COMP. STAT. 520/1 *et seq., implemented by* ILL. ADMIN. CODE tit. 77 § 1005.
[33] 20 ILL. COMP. STAT. 2310/2310-1 *et seq.*
[34] 410 ILL. COMP. STAT. 50/1 *et seq.*
[35] 405 ILL. COMP. STAT. 5/1-100 *et seq.*
[36] 740 ILL. COMP. STAT. 110/1 *et seq.*

There may issues not addressed by current statutes and regulations by virtue of the novel nature of integrated justice initiatives. Other issues will be familiar but contain greater levels of complexity when discussed in the integrated justice context. A brief discussion of the issues we expect to encounter follows.

A series of objectively prepared research papers should be prepared on each of the following issues in order to inform policy decisions. These research documents should be made part of the committee's final report and placed near the relevant sections of the privacy policy to demonstrate that the committee made informed policy decisions and, furthermore, that those policy decisions were purposeful.

## A. INFORMATION LIFE CYCLE

Historically, justice agencies faced with physical storage limitations developed policies for maintaining quantities of paper files out of practical necessity. Additionally, the utility of old documents was marginal as stored documents were not easily retrievable, even with detailed indexing systems. With practically unlimited storage capabilities and the enhanced access, retrieval, and analysis of stored documents available in an integrated justice system, the decision on whether to keep or destroy records becomes a part of a privacy policy rather than a practical necessity.

Furthermore, the General Assembly routinely makes policy decisions concerning the expungement of criminal history records. These expungement statutes need to be referenced and their impact upon an integrated justice system examined. For instance, it is very likely that current expungement statutes, when applied to an integrated justice information system, would not, lead to the total expungement of a criminal history record because the various data flows and repositories contained within the integrated system are not specifically referenced by the statute.

*Information Life Cycle issues to be addressed:*

- What impact does the sealing records have on the availability of information in the integrated justice system?
- Similarly, what impact does the expungement of records have on the availability of information in the integrated justice system?
- Can a record *truly* be expunged?
- Secondary dissemination of information contained in the integrated justice system should also be addressed, for example:
- If once a record becomes public it is forever public, then why does it matter how long public records are retained?
- Is the information life cycle more applicable to non-public information retention?

## B. INDIVIDUAL ACCESS TO RECORDS CONTAINED IN INTEGRATED JUSTICE INFORMATION SYSTEMS

Several statutes already provide an individual with access to records concerning him that are contained in a government information system. Criminal History repositories funded with federal funds are required to provide an individual with access to his criminal history information.[37] Law enforcement data systems, however, tend to not allow an individual to access the data contained therein.[38] The Privacy Committee will need to determine what information contained in the integrated justice system the individual it relates

[37] *See* Criminal Justice Information Systems Regulations, 28 C.F.R. part 20.34.
[38] *See* Law Enforcement Agencies Data System (LEADS) Regulations, ILL. ADMIN. CODE tit. 20 § 1240.30.

to can access. This determination will most likely be based upon current practices revealed through an analysis of current statutes and regulations and the underlying policies they further.

*Individual Access issues to be addressed:*

- How quickly and how often should the integrated justice system provide the requested information to the data subject?
- In what form and manner should the information be provided to the requestor?
- Should this form and manner be standardized?
- How much of the information contained in the integrated justice system is considered to concern the individual?
- Does this information include how the information is being used, whether it is being used, and to whom the information is disclosed?
- What should the administrative standards for modifying an incorrect record be?

## C. ACCOUNTABILITY OF THE INTEGRATED JUSTICE SYSTEM

Determining the accountability of the integrated justice system to the public is of significant importance to the privacy policy. Because the public bears the ultimate risk that personal information contained in the integrated justice system may be accessed or released inappropriately, causing possible loss of employment, diminished social status, or other adverse consequences, the integrated justice system should be held responsible for complying with the privacy policy.

The accountability provisions contained in current statutes and regulations should be researched and their current applicability to the integrated justice information system evaluated. In the instances where there is no current accountability, the Privacy Committee should develop accountability provisions to ensure compliance with the Privacy Policy.

*Accountability issues to be addressed:*

- How do freedom of information acts impact the operation of the integrated justice system?
- How do the First Amendment and common law access to court records affect the integrated justice system?
- Is there a presumption of public access to records contained in the integrated justice system? If so, to what extend does that presumption influence the privacy policy?
- How often should compliance audits be performed and who should perform those audits?
- What administrative procedures should be created to challenge the integrated justice system's compliance with the privacy policy? Would the individual need to suffer injury before he can challenge (standing)?
- What other recourses will an affected party have to affect redress of a violation of the privacy policy that harms him?
- Will the privacy policy or state law provide a civil cause of action for aggrieved individuals?
- Will the individual have to exhaust any administrative remedies first? What will those administrative remedies be?
- Will the state law make willful non-compliance with the privacy policy a crime?

## D. AVAILABILITY OF STATISTICAL INFORMATION MADE EASILY AVAILABLE BY INTEGRATED JUSTICE INFORMATION SYSTEMS

Theoretically, an integrated justice information system can easily run reports of the transactional information generated by the criminal justice system. Statistical information such as the number of arrests, the number of times charges are brought or dropped, the number of convictions, guilty pleas, and acquittals, sentencing statistics (perhaps even indexed by judge), the number of prisoners released, and even recidivism rates could potentially be generated by the integrated justice information system. These pieces of statistical information may be very useful in the oversight of the justice system—oversight both by justice policy makers and the general public.

First, it must be determined whether the integrated justice information system has these capabilities and, if not, whether it should have them. Second, provided the integrated justice system can generate these types of statistical reports, it must be determined whether those reports are of such a nature that they should or shouldn't be released. The Privacy Committee should examine current freedom of information acts for guidance and may also want to address the issue of whether the system should be made to generate specific reports upon a public request.

## E. ACCESSIBILITY OF VICTIM & WITNESS INFORMATION

In many cases, a crime victim's most fundamental need is for physical safety. To achieve physical safety, victims of crime need a broad range of relief—from privacy regarding the violence that occurred to confidential addresses and counseling. Victims of crime may forego legal protections if they are achieved at the expense of privacy. Fear about who might have access to police reports, pre-sentence investigations, victim compensation files, or victim impact statements may prevent victims from notifying authorities or participating in a criminal prosecution.

*Victim & Witness Information issues to be addressed:*

- What is the purpose for collecting specific information from crime victims?
- What harm could come to the crime victim and her family if this information was disclosed to the offender or the public?
- In light of any identified risk, should this information be recorded at all?
- If the information is necessary to the function of the particular justice agency, what should that record contain and how should it be shared in an integrated justice system?

## F. ACCESSIBILITY OF OFFENDER AND VICTIM HEALTH INFORMATION

Health information collected by the justice system includes otherwise confidential medical and mental heath records. These records can include information ranging from a victim's HIV status to an offender's previous hospitalization in a mental institution. The privacy policy should address how these records concerning victims and offenders are collected and shared by the integrated justice system in order to ensure their appropriate use.

## G. COLLECTION, USE, & DISSEMINATION OF SOCIAL SECURITY NUMBERS

Information breeds information; although one's Social Security number does not in and of itself reveal much about an individual, it provides access to one's financial information, educational records, medical

records, and a whole host or other information. Social Security numbers are the currency of identity theft—one of the most rapidly escalating forms of crime. The privacy policy should address where in the justice process Social Security numbers are collected and disseminated by the integrated justice system to ensure their appropriate use.

## Step 5

The Privacy Committee Final Report

Briefly stated, Privacy Committee will create a final report that does four primary things. First, the report will convey a strong understanding of the current status of federal and state privacy law. This understanding will include the identification of all relevant statutes and regulations as well as an analysis of their accompanying case law.

Secondly, the report should include a summary of the research performed by committee staff as well as any policy research conducted by member agencies. Additionally, any significant policy deliberations transcribed during the course of the committee's meetings should also be included. Optimally, these legal discussions would be strategically positioned near the relevant portions of the privacy policy in order to provide context for the implementation of the privacy policy provisions.

Where appropriate, the final report should also include recommendations for amendments to current privacy statutes and regulations where the integrated justice information system operates outside the scope of their provisions but plainly shouldn't.

The privacy policy will be integrated into the final report so that the supplementary supporting documentation can provide direction on how local agencies should implement the policy in practice. This also allows the final report to more fully explain the policy decisions contained therein. Explaining the rationale for a particular policy decision is important because it can aid in the resolution of future privacy issues that may not have been foreseen during the privacy policy's development. An un-annotated version of the privacy policy would also be provided in an appendix to the final report.