Privacy issues confronting the sharing of justice information in an integrated justice environment

SEPTEMBER 2006

Introduction

The IIJIS Privacy Policy Subcommittee was created to develop privacy policy recommendations that will guide the sharing of justice information both among justice agencies and with the public. The group is composed of representatives from the traditional criminal justice system as well as individuals from the press, law schools, victim services groups, and private users of criminal history information.

The following issues represent this subcommittee's attempt to document the privacy concerns that should be addressed by agencies participating in or developing integrated justice information systems. This document is the result of several meetings with justice practitioners and subcommittee members as well as joint brainstorming sessions involving the group as a whole.

This document is continuing to evolve and issues will be added as the subcommittee moves forward with the development of privacy policy guidance for Illinois integrated justice information systems. This version includes privacy issues that arise with the sharing of traditional information as a case flows through the justice process. It also identifies issues concerning the enhanced collection, sharing, and dissemination of electronic police incident information – capabilities that are quickly being developed throughout the nation.

To our knowledge, no other state or agency has compiled a similar listing of privacy challenges that confront the enhanced sharing capabilities of integrated justice information systems. This document is being made available to the public so that entities attempting to integrate justice information systems can learn the types of questions they should be asking, even if the subcommittee has not yet addressed them.

Contents

I. General privacy policy considerations

(a) Public perceptions – The public's perceptions regarding the accessibility of justice information vary. This may be of concern because the public's acceptance of an integrated justice information system is related to its confidence that the government is taking measures to protect individuals' privacy interests.

- **(1)** There seems to be a need to educate the public as to what information about citizens is available in the justice system and what is available to the public.
- **(2)** Individuals should be informed of the following aspects of their criminal history record information:
  - **(A)** That any contact with the justice system results in a permanent record;
  - **(B)** How to expunge their juvenile record;
  - **(C)** Eligibility to seal or expunge their adult criminal records;
  - **(D)** How to obtain certificates of relief from licensing disabilities;
  - **(E)** How to exercise their rights to access and review under the Criminal Identification Act;
  - **(F)** That certain aspects of their criminal history will be available to employers and the public;
  - **(G)** Others?
- **(3)** What methods of educating the public will be most effective?
  - **(A)** A guide to understanding criminal background checks is available on the Illinois State Police website;
  - **(B)** The Illinois Appellate Defender maintains a website to inform people regarding the sealing and expunging of criminal records;
  - **(C)** Is a centralized location for this information preferable to individual agency public relations departments?
- **(4)** Are there any risks of informing the public about the limitations of criminal history record checks?

(b) Collection of records – The mere collection of information regarding individuals implicates privacy concerns. This is because the collection of information about individuals is usually premised upon some reasonable suspicion that they are acting unlawfully. Privacy issues are raised when the government collects information about individuals for investigatory purposes absent any suspicion of criminal wrongdoing. Developers of integrated justice information systems must be aware that the mere collection of personally identifiable victim and witness information raises genuine privacy concerns.

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

(c) Collection and maintenance of "non-relevant" information – The justice system collects information that may or may not be relevant to the prosecution of an offense; this is 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.

- **(1)** What is "relevant" information?
- **(2)** Who decides relevance?
  - **(A)** Police officers?
  - **(B)** Prosecutors?
- **(3)** Should information that is not immediately relevant be retained?
  - **(A)** If yes, for what purposes should such "non-relevant" information be retained?
    - **(i)** Presumably retaining information on cold cases in the hopes that they will be solved in the future is appropriate. But what about when the offense's statute of limitations lapses?
    - **(ii)** Is there a legitimate defense need for non-relevant information such as exhausted leads?

(d) Establish "ownership" of the data – Clearly establishing which entities have authority over and bear responsibility for the data contributed to the information system is of paramount importance. It is possible that the administrator of an integrated justice information system will have a substantial role to play in this regard.

- **(1)** Who will ultimately be responsible for fulfilling the following data management functions?
  - **(A)** Ensuring data is of proper quality;
  - **(B)** Identifying inaccurate data and correcting it;
  - **(C)** Ensuring that data is not misused;
  - **(D)** Establishing data retention periods;
  - **(E)** Enforcing laws, regulations, and policies concerning use of the data;
  - **(F)** Other functions?

(e) Identify authorized users – Currently, the integrated justice information systems across the country issue user logons to employees who work for law enforcement agencies that possess an Originating Agency Identifier (ORI) number. ORI numbers are unique identifiers assigned by the US Department of Justice for use with its National Crime Information Center (NCIC).

- **(1)** Should an agency, an individual, or both have to meet certain prerequisites before being authorized to access an integrated justice information system?
- **(2)** What should those requirements be?

(f) Appropriate uses of justice data – How government agencies use the data they collect is of significant concern to the public. A sound privacy policy should clearly identify appropriate uses of the information contained in the information system.

- **(1)** If an information system will be used for data mining purposes, appropriate checks and balances should be developed to ensure that the data mining is conducted within the proper scope and with appropriate authority.

(g) Dissemination of justice information when safety of community is at issue – Justice information can be used for many reasons unrelated to the operation of the justice system when the safety of the community is at issue.

- **(1)** What level of risk to the community is required before the justice information can be disseminated?
  - **(A)** Notification that a suspect is wanted for murder?
  - **(B)** Sex offender registrations?
  - **(C)** Terrorist threat?
- **(2)** Should a uniform set of criteria be established to help ensure that individuals' privacy interests are treated equally throughout the state?

(h) Secondary dissemination – Secondary dissemination of information maintained by the justice system is a concern. The sale of justice information to the private sector and the private sector's compiling and reselling of the information impacts the quality of justice information available to the public.

- **(1)** What secondary dissemination regulations are in place now?
- **(2)** What provisions should those regulations contain?
  - **(A)** Should there be a limit on the age of information that may be disseminated?
  - **(B)** Should private suppliers of criminal history record information be required to comply with the Illinois State Police's secondary dissemination requirements?
- **(3)** What types of information does the subcommittee need to draft effective regulations?
  - **(A)** Are examples of who is buying and re-selling justice information informative?
  - **(B)** Should we explore the extent to which investigative databases update their information?

(i) Data retention periods – In the past, paper files were purged largely due to storage constraints. As electronic storage becomes dominant, there is less of a physical need to purge information. As such, the retention of electronic law enforcement data in a data warehouse environment becomes a privacy issue that must be balanced with public safety (e.g., crime fighting) concerns. Furthermore, the fair information practices call for the destruction of personal information when it no longer serves the original processing purposes.

(1) How long should data entered into an integrated justice information system be stored? Is this determination different than the retention of public records for purposes of government oversight?

(2) What laws and regulations currently govern the retention and destruction of justice information?

(3) Retention standards may be appropriate to ensure that justice information does not become stale. Several factors may inform retention period standards:

(A) The level of trust that the public has that the justice system will maintain the confidentiality of the data and use it appropriately is a substantial factor. The lower the level of trust, the higher the public's desire may be to destroy the data.

(B) How the information will be used must also be considered. It is generally understood that justice information, especially criminal incident data, would be used to conduct various forms of crime analysis (e.g., analyzing similarities in crimes to connect them to a common offender, identifying who is associating with whom to commit crimes, etc.).

(C) Determining whether certain types of data become stale. Staleness is just one of several data quality factors that may weigh into this balancing test.

(D) The agency or administrator's ability to successfully maintain the confidentiality of justice information system data.

(4) If once a record becomes public it is forever public, why does it matter how long public records are retained?

(A) Are retention periods more applicable to non-public information?

(B) Are the sealing and expungement of conviction records data retention issues as well?

(5) How long should retention periods for justice information be?

(A) The Illinois Secretary of State's Archives Office has record retention periods; these might be helpful.

(B) The Illinois State Police also has retention periods for all of its records.

(C) Many privacy concerns are raised by the collection and maintenance of personally identifying victim information primarily because victims do not choose to participate in the justice system.

(6) Should retention include the ability to search the information with analytical tools or should data just be stored for limited purposes?

(j) Destruction of data – Some integrated justice information systems take "snapshots" of data from source systems. Frequent snapshots serve to keep the data contained in these systems current and accurate.

(1) Will old snapshots be destroyed or retained?

(A) These snapshots might themselves be state records under the State Records Act and subject to its conditions prior to destruction.

(k) Applicability – State-level justice information systems that are federally funded are required to comply with many federal laws and regulations. State laws also impact the

development and utilization of those state-level systems. However, these laws and regulations may not apply to agency-level systems that are not federally funded.

(1) Should the recommendations of the IIJIS Privacy Policy Subcommittee (which we expect will be based upon existing federal and state laws) be made to apply uniformly to all justice information systems operating in Illinois?

(2) What considerations are necessary to make this determination?

(A) How should access by public defenders be addressed by the policy since existing federal and state law does not specifically address them? See § III (B)(c).

(B) Are there agency-specific needs or missions that may be frustrated by the privacy policy?

(l) Interaction between the executive branch and the judiciary – Although justice information collected and maintained by the executive branch is often used in the course of criminal prosecutions that take place in the judicial branch, the executive branch is prohibited from imposing the privacy policy upon the judicial branch. The result, with few exceptions, is that information protected by the executive branch is made publicly available once it is used in court.

(1) How can we develop policy recommendations in cooperation with the judicial branch?

(m) Identify potential liabilities – The following areas have the potential to expose integrated justice information systems to public criticism and should be addressed preemptively.

(1) Identify any concerns with commingling fingerprint-based information with name-based records.

(2) Identify the nature of the harms that can potentially be caused by misuse of information contained in the system.

(3) Anticipate possible future abuses of data mining technology. Specifically consider its uses in background checks as opposed to criminal investigations. Today, time constraints limit these types of abuses.

(4) Learn from the mistakes MATRIX made.

II. Justice system access to justice information

A. Availability of officer safety information

(a) Officer safety information defined – It is a goal of the justice system to ensure that police officers have access to information that can help protect them in the field. However, there doesn't seem to be a uniform definition of officer safety information.

(1) What are the current types of information related to officer safety?

(A) LEADS caution fields

(B) CHRI

(C) Warrant information

(D) Gun ownership
(E) Domestic violence information (orders of protection)
(F) Gang information
(G) Mental patient status information?
(H) Others?

(2) How does a practitioner decide if a piece of information is related to officer safety? Or, stated differently, what factors influence the decision about whether a certain piece of information has an impact on officer safety?

(A) For instance, information gathered by probation and court services officers can sometimes improve officer safety. However, absent a court order, information maintained in probation files in Illinois is only available to the probation department and the court. Should such information be made available to law enforcement officers?

(i) Legislative history from the statute requiring probation records to remain private may be informative.

(ii) Note also that some information in the possession of probation officers may be protected by a different privacy regulation (HIPAA, Family Educational Rights and Privacy Act, etc.), thus impacting the secondary dissemination of the information.

(3) Should a set of criteria be established to help an agency decide whether information relates to officer safety or is it enough to designate specific types of information?

(A) Is setting "outer limits" of officer safety information a viable option?

(b) Stale officer safety information – LEADS Warning fields and caution files meant to provide officer safety information frequently contain old information.

(1) When do certain pieces of officer safety information become stale?

(2) What policies exist to ensure that information maintained in officer safety files is current?

(3) Are those policies sufficient? If not, what should those policies include?

(A) Is annual review of the information feasible?

(B) Who should review the information? The original officer?

B. Police contact cards

Contact Cards, also referred to as FI Cards,[1] document police officers' contacts with the public. They can include the officer's self-reported activities during a shift as well the name, date of birth, and address information of the citizens with whom the officer communicated. Contact card data can be used for several purposes, including as an officer management tool, as a method of collecting some minimal surveillance data for future investigative purposes, and as a potential method for recording racial profiling statistics.

[1] "FI" refers to, among other things, field investigation, field interview, and field interrogation.

(a) Contact cards as traditional justice information – Contact cards seem to be more analogous to traditional justice information and may not reach the level of intelligence information.

- **(1)** Should contact cards be addressed as an issue separate from intelligence data?
- **(2)** What information is contained on police contact cards?
  - **(A)** Contact cards contain the subject's name, data of birth, address, vehicle description, as well as the time and location where the person is stopped.
  - **(B)** Will the FBI's development of N-DEx impact the information collected by Illinois law enforcement officers?

(b) Regulation of contact cards – There is very little regulation of the collection, maintenance, dissemination, and use of contact card information.

- **(1)** How is the information contained in contact cards used?
- **(2)** Should contact cards be regulated in some manner?
  - **(A)** Should the data collected be standardized? Will N-DEx do this?
- **(3)** What issues should be covered by a policy intended to regulate the collection, maintenance, dissemination, and use of contact card information?
  - **(A)** Is the collection and combination of contact card information in danger of being perceived as a "dossier" of one's legal conduct?

(c) Reliability of information contained in contact cards – Reliance on contact card information to develop reasonable suspicion or probable cause may be a concern.

- **(1)** What factors are involved in determining whether contact card information is reliable?
  - **(A)** Does the age of contact card information affect its use as an investigative tool?
  - **(B)** What about the lack of fingerprint verification?
  - **(C)** The information is only as reliable as the people giving it to the officer.
- **(2)** Should there be a statewide policy regarding the reliability of contact card information?

(d) Sharing contact card information – Because of the mobile nature of society, sharing justice information, including relevant contact card data, is appropriate. Sharing contact card information between jurisdictions, however, may raise the stakes of these concerns.

- **(1)** Should policies be developed to regulate the sharing of contact card information specifically?
- **(2)** What should be included in such policies?

C. Availability of probation information

(a) Accessibility of probation conditions – It may be desirable to inform officers of an individual's probation status and conditions. While probation status and some conditions

are publicly available, some administrative sanctions that result in additional conditions of probation are not.

(1) What administrative sanctions or conditions are available?

(2) What does violation of an administrative sanction or condition mean for the probationer?

(3) Should those conditions be made available to police?

(A) Does this decision depend upon whether violation of the administrative conditions establishes probable cause to arrest or should officers have this information on the off chance that it may become important under certain, unknown circumstances?

(4) All of this presumes that ordinary conditions of probation are available to police officers. Is this really the case?

(A) Normally conditions imposed upon probationers are contained in the written order sentencing the offender to probation.

D. Availability of pre-sentence investigation reports

(a) Accessibility of PSI reports – The accessibility of pre-sentence investigations ("PSIs") is subject to local interpretations. Most jurisdictions keep PSIs sealed; however, some jurisdictions hold that once the report is used in open court, it becomes a public record.

(1) Should a uniform interpretation on the accessibility of pre-sentence investigations be recommended?

(2) What should that interpretation be?

(A) There seems to be significant public policy concerns that recommend keeping PSIs confidential even though they are used in open court. Is the development of a uniform sealing requirement a viable solution?

(B) How about allowing access to a witness's PSI subject to a protective order?

(3) How do we collaborate with the judiciary on this?

III. Public access to justice information

A. Generally

(a) Information accessible to the public – While several laws and regulations limit the release of justice information to the public, there is still uncertainty regarding what information can be released and when.

(1) Are there any perceived problems or uncertainties under existing law?

(2) What types of justice information should be shared with the public?

(A) Are warrants generally publicly accessible?

(i) Does the severity of the offense a person is wanted for determine the public accessibility of any warrant information (e.g., when the news reports an individual is wanted for murder)?

(B) Does it make sense for arrest information to be publicly available in the form of arrest blotters and newspaper reports (and thus publicly available forever) but not available from the criminal history repository?

(C) Are other types of non-conviction information available (perhaps inadvertently) to the public? Should they be?

(3) When should information be affirmatively provided to the public?

(A) What considerations should be made to ensure the defendant a fair trial?

(i) Illinois Rules of Professional Conduct 3.6 and 3.8(d) [concerning trial publicity and prosecutors' responsibilities] as well as Illinois Supreme Court Rule 415(c), (d) [regulating custody and protection orders for discovery materials] might be informative here.

(ii) Issues concerning the accessibility of victim and witness information are raised in Section V(A).

(b) Determine who might be responsible for responding to subpoenas or FOIA requests for integrated justice information system data – Under the Freedom of Information Act, a public body that maintains or possesses a requested state record must respond to the request within seven days. Illinois case law reveals that merely referring a requestor to the original source of the record does not relieve a public body of its obligation to respond to the FOIA request and that such a referral constitutes a denial under the act. There are several exemptions under which a public body can refuse to disclose a requested record. Several issues are implicated by this statute:

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

(2) Under the first exemption contained in FOIA, a public body does not need to disclose information that is protected from disclosure by law or administrative rule. Can a state agency (e.g., Illinois State Police, Illinois Criminal Justice Information Authority, Central Management Services) promulgate a rule that would exempt data contained in a statewide, integrated justice information system from disclosure under FOIA?

(3) There are times when copies of a single record are possessed by more than one agency. When this happens, one possessing agency may desire to withhold the requested report under an exemption while the other possessing agency may wish to disclose that same report or may not be eligible to invoke the exemption utilized by the first possessing agency. Some states' freedom of information acts address this circumstance by permitting or requiring the second possessing agency to invoke the first agency's exemption. Illinois' FOIA does not contain a similar provision. Should Illinois's FOIA be amended to include a similar provision? The

administrator of an integrated justice information system and participating agencies should enter into a written agreement to consult in these circumstances.

(4) Subpoenas are ordinarily served upon registered agents. Who will be the integrated justice information system's registered agent?

(5) Several statutory amendments may be necessary to meet Illinois's needs with regard to integrated justice information systems.

(c) Laws limiting public access to justice information – Several state laws impact the public availability of justice information.

(1) How do the provisions of the Uniform Conviction Information Act (UCIA), the Criminal Identification Act, the Freedom of Information Act, State Records Act, the Local Records Act, and Rule 3.6 of the Illinois Rules of Professional Conduct interact?

(2) What other laws might impact the public availability of justice information?

(A) Genetic Information Privacy Act, 410 ILCS 513/1-45;

(B) Right to Privacy in the Workplace Act, 820 ILCS 55/1-20;

(C) Communications Consumer Privacy Act, 720 ILCS 110/1-3;

(D) Alcoholism & Other Drug Abuse/Dependency Act, 20 ILCS 301/30-5(bb)(3);

(E) Mental Health and Developmental Disabilities Confidentiality Act, 740 ILCS 110/10;

(F) Others?

(3) Is there a need for a uniform policy? Should the IIJIS Privacy Policy be it?

(d) Arrest blotters – Traditionally, police departments maintain arrest blotters that are open to the public. However, the types of information contained in arrest blotters vary from department to department.

(1) Should police blotter information be made uniform in Illinois?

(A) Should the blotter carry a notation that persons are presumed innocent (in the spirit of Illinois Rules of Professional Conduct 3.6 (b)(6) and 3.8)?

(e) Training justice practitioners – Determining what justice information is accessible to the public and when is a complex task.

(1) Is there a need to educate criminal justice officials as to what information can and should be made available to the public?

(2) LEADS certification addresses some of these concerns; is it sufficient? Note also that not all justice practitioners are LEADS certified.

(f) Public accessibility of a compiled response – The goal of the IIJIS initiative is to eliminate barriers to the sharing of justice information within the justice system. Ultimately, when an individual has contact with the justice system, all the information necessary to make a decision regarding his case will be made available to the official in

the form of a compiled response. Presumably, it would be possible to strip any non-public information from that response and provide it to the public.

(1) Should IIJIS consider providing the public with a compiled response composed only of the publicly available justice information from multiple agencies?

(2) What issues are involved in making this recommendation?

(A) What information could lawfully be included in a publicly available compiled response? Is this even lawfully possible?

(B) Is there a legitimate need to provide this compiled information? Would it be helpful to members of the public?

(C) Would the release of compiled information be consistent with Illinois Rules of Professional Conduct 3.6 (b)(6)?

B. Criminal history records checks

There seems to be some confusion about the difference between a background check and a criminal history records check. A background check involves an investigation of an individual including a review of credit and employment references as well as past residences. A criminal history records check, however, is merely a search for criminal records.

(a) Illinois State Police as recommended data source – The Illinois State Police criminal history repository only contains Illinois criminal history data.

(1) Should the Illinois State Police be the state's recommended source of publicly available conviction information?

(A) Are the circuit court clerks a viable option?

(2) What information does the subcommittee need to make this recommendation?

(b) Ease of access to ISP conviction data – The Uniform Conviction Information Act provides that all conviction information collected and maintained by the Illinois State Police is available to the public.

(1) Should access to conviction information in Illinois be made more easily available in light of integration technologies?

(A) Is web-based accessibility of conviction information recommended?

(B) What about problems of ensuring that the wrong person is not improperly identified as the subject of the conviction information? (This does not inhibit private data sellers.)

(2) What issues should be discussed before recommending easier access to publicly available conviction information?

(A) Cost issues;

(B) Potential effects on jury pools if a defendant's prior criminal record is accessed and displayed in the media;

(C) Should web-based publicly accessible criminal history information be limited to convictions?

(i) We may want to examine the policy considerations underlying 20 ILCS 2635/3(F), which prohibits supervision and certain "First

Offender Drug Probation" dispositions from being listed as "convictions" in the criminal history repository.

(c) Public defender access to client, witness, and victim CHRI – Public defenders expressed an interest in access to the criminal history records of clients, witnesses, and victims. Currently, the court handles such requests during discovery.

(1) Are court oversight and the rules of evidence sufficient or should additional or alternative access be considered?

(A) Is this an efficiency issue or an access issue?

(B) See the Illinois Public Defender Association examples:

(i) A defendant is often appointed a Public Defender for his initial bond hearing. This is a fast-paced court proceeding and attorneys may not have the time to obtain the defendant's criminal history information from the prosecutor. A defendant's recollection of his criminal history is often inaccurate. Oftentimes defendants can't remember whether their prior felonies were Class 1, 2, 3 or 4 offenses and some lie to their attorneys about having prior convictions. If the Public Defender has immediate accurate information about a defendant's record, the Public Defender can assist the court in arriving at a reasonable bond in the first instance. Furthermore, the Public Defender will be able to advise his client on potential sentencing issues that are affected by prior convictions and other pending cases.

(ii) It can take nearly 30 days from the defendant's arrest for the court's discovery order to require disclosure of a witnesses' criminal history record. If a witness has a prior conviction, a defense attorney must order certified copies of those convictions (sometimes from multiple jurisdictions). This is the only way to ensure the admissibility of the witness's conviction at a hearing or trial. This often causes delay and costs the county money.

(C) There seems to be some misunderstanding between access to the information and the manner of access. Manner of access seems to impact response time from the Illinois State Police. *See also*, 725 ILCS 105/10 allowing State Appellate Defender capital litigation investigators access to LEADS data through the Illinois State Police for personal safety purposes only.

(2) If the response time on public inquiries were more timely (e.g., making publicly available conviction information readily available on the web), would there be a need to address public defender and private defense attorney access in particular?

(d) Municipal police department pre-employment checks – Municipal police departments are often requested by businesses and their city governments to conduct background and criminal history checks of potential employees. However, statutes and regulations prevent police departments from conducting such pre-employment checks.

(1) Should municipal police departments perform this function or should they refer the city government elsewhere?
- **(A)** What information would aid the subcommittee in making this recommendation?

(2) If referral is appropriate, to whom should municipal police departments refer such requests?
- **(A)** Illinois State Police?
- **(B)** Private data providers?
- **(C)** Illinois Association of Chiefs of Police are working on this issue.

(3) Are government "in-house" checks of their local databases a concern here?

(e) Reliability of private checks – There is some concern about the reliability of private criminal history records checks.

(1) Is there a need for regulation of private data providers?
- **(A)** What types of information are necessary to make this determination?
  - **(i)** Would creating a list of Illinois justice agencies that sell their data to the private sector be helpful?
  - **(ii)** Is anecdotal evidence enough?

(2) If so, what should those regulations include?
- **(A)** Will understanding the relevant provisions of the Drivers' Privacy Protection Act and the Fair Credit Reporting Act be beneficial to our efforts?
- **(B)** Should private data providers be required to expunge or seal their records as well?
- **(C)** Should vendors who fail to maintain complete and accurate information be precluded from purchasing agencies' data in bulk?

C. Open nature of justice information management practices

(a) Notice to those whose data is collected – The fair information practices state that agencies should provide notice about how they collect, maintain, and disseminate personal information.

(1) Specifically, this notice should:
- **(A)** Indicate the main purposes for the data's use;
- **(B)** Identify the person and office responsible for the data;
- **(C)** Identify those who may access or receive the data;
- **(D)** Explain whether the information is mandatory or voluntary and the consequences of failing to provide the information; and
- **(E)** Inform the data subject that he has a right to access the data and rectify errors.

(2) Should such a notice be provided to individuals whose information is collected by the justice system?
- **(A)** Would distribution of the privacy policy itself provide sufficient notice?
- **(B)** What are the resource implications of providing this notice? Is this administratively burdensome?

(C) How does this differ from Freedom of Information Act requirements?

(3) Where it would not compromise a pending investigation, case or court proceeding, should individuals be informed that they were the subject of an investigation in a manner similar to wiretaps?

(A) Is this better considered in a section focused on intelligence?

(b) Notification of secondary dissemination – The fair information practices also hold that agencies should communicate to affected individuals when their justice records are requested, sold, or released to third parties.

(1) Should agencies be required to comply with this requirement?

(2) Would compliance be unduly burdensome to the efficient administration of justice?

D. Transactional information generated by the justice system

(a) Accessibility of the justice system's transactional information – The operation of the justice system creates a significant amount of transactional information. 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 by both justice policy makers and the public.

(1) Do the provisions of the Freedom of Information Act provide enough regulation of this transactional information?

(A) FOIA allows for reasonable requests for information; if the integrated justice system makes these figures easily available are those provisions enough?

(2) If not, what policies should be developed for the sharing transactional information?

IV. Rights to access, review and challenge justice information

(a) Rights to access, review and challenge justice information other than CHRI – While the Department of Justice requires criminal history repositories to provide individuals with the right to review and challenge their criminal history transcripts, there are several types of justice information that do not provide such a right including state's attorney files and some IDOC records.

(1) Are other types of justice information, currently subject to access and review requirements?

(2) To what extent, if any, should individuals be afforded a right to review and challenge other types of justice information?
- **(A)** Should instances of identity theft impact an individual's access and review rights?
- **(B)** What about access to police and intelligence files?

(3) What factors would help to make this determination?
- **(A)** What other types of government information (justice and non-justice) are currently subject to access and review requirements? Can these be analogized?
- **(B)** Should instances of identity theft impact an individual's access and review rights (i.e., give the individual more access rights)?
- **(C)** Should the right extend to incidental references to an individual (e.g., the individual was named in a narrative as a possibly involved but is not formally described as a victim, suspect, or witness.)? Should the right be limited to only those individuals labeled by their government as suspects or offenders?
- **(D)** There would probably have to be a limitation on this right where it would interfere with a pending investigation.
- **(E)** Should the right to access and review, if granted, also include a listing of individuals and agencies to whom the information was previously disclosed?
- **(F)** The type and sensitivity of the data the individual is seeking access to is also a relevant factor.

(4) If additional types of information should be subject to access and review rights, what types of administrative procedures would need to be developed?
- **(A)** Could CHRI access and review provisions serve as a guide to access and review of other types of justice information?
- **(B)** Should a provision be considered that is similar to the section of the Fair Credit Reporting Act that permits the subject of the information to append a narrative to the record that explains his version of it?

(b) Access to how the information has been used – According to the fair information practices, the information reviewed by the data subject should include how the information is being used, whether it is being used, and to whom the information has been disclosed. The FIPs, however, were developed for the collection of consumer information.

(1) In the justice information context, should access and review policies provide individuals with information about:
- **(A)** How the information is being used?
- **(B)** Whether the information is being used?
  - **(i)** The U.S. Attorney's Office will frequently answer "target" letters (A person's defense attorney can ask the U.S. Attorney if they are a "target" of an investigation and the U.S. Attorney will frequently answer with a letter saying "yes").
- **(C)** To whom the information has been disclosed?

(i) Use of information in an attorney's work product is not readily revealed; this applies both to state's attorneys and public defenders.

V. Special considerations

A. Accessibility of victim and witness information

When an individual is victimized or witnesses a crime, the justice system collects personally identifiable information about that person. Many privacy concerns are raised by the collection and maintenance of information concerning victims and witnesses primarily because of the involuntary nature of their participation in the justice system.

(a) Accessibility of victim/witness information generally – People do not choose to become victims or witnesses; nonetheless, the justice system collects information about them anyway. Fear about who might have access to the information collected by the justice system in police reports, pre-sentence investigations, and the like may prevent victims and witnesses from calling the police or participating in a criminal prosecution.

- **(1)** Current practice is to limit the accessibility of victim/witness information outside of the justice system. Are existing limitations enough?
  - **(A)** Inconsistent sealing of pre-sentence investigations throughout the state was highlighted as an issue that might result in the publication of a victim's personal information.
  - **(B)** Are there other problems with existing practices designed to keep victim and witness information from the public?
  - **(C)** Note that a bill enacting the Crime Stoppers Program Act that would have allowed persons submitting information of a crime to remain anonymous did not pass the 93d Illinois General Assembly. Senate Amend. 1 to House Bill 1018.
  - **(D)** Is the mere allegation of victimization sufficient to obtain the protections provided to victims of crime or should those protections wait until after disposition?
- **(2)** There also seems to be a need to limit the accessibility of victim/witness information within the justice system.
  - **(A)** How much information is enough to identify a victim/witness?
  - **(B)** Collecting victim identifying information in a local records management system is different than contributing their identities to an integrated justice information system as part of an incident data sharing program.
    - **(i)** Should victim identities be available to all the systems users or should there be some limit to this information?
    - **(ii)** Is restricting access to the information on a need to know basis sufficient?
    - **(iii)** What qualifies as "needing" to know?
  - **(C)** How does the public availability of victim and witness information contained in the court records affect this issue?

(i) Illinois Supreme Court Rules 412 and 413 require "names and last known addresses" of witnesses to be disclosed; they are usually contained in the court file.

(ii) Where a witness's safety is at issue, protective orders are available to limit the public display of their address. Professional courtesy agreements between prosecutors and defense attorneys can also provide this protection.

(iii) Is there case law on how far a defendant's right to a "public trial" pertains to documents involved in the public trial?

(b) Access to a victim's location – In many cases, a victim's most fundamental need is for physical safety.

(1) Who should have access to the victim's or witness's location?

(A) Note that in *U.S. v. Carmichael*, 326 F.Supp.2d 1267 (M.D. Ala. 2004), the district court for the Middle District of Alabama held that a criminal defendant may maintain a website seeking information on named witnesses.

(B) Do justice practitioners other than law enforcement and state's attorney officials need access to this information? If so, why?

(c) Victim databases – Some justice agencies have developed databases that allow them to search victim and witness information. These databases can also link results in such a way that an individual's victimization history can be compiled.

(1) Current offenders might have been victims at an earlier point in their lives. Is there a possible need for the previous victimization history of a current offender?

(A) Currently, defense attorneys seek this information through a Motion for Supplemental Discovery directed to the prosecution.

(B) An offender's victimization history might serve to mitigate a sentence as in death penalty sentencing hearings.

(2) What purpose might this functionality serve?

(A) Both police and prosecutors need to know the background – good and bad – of witnesses and victims.

(B) There may be a legitimate defense need to investigate "prior false complaint" information as well as a confidential informant's background.

(3) Do the benefits of creating a victim database outweigh victims and witnesses' privacy interests and the policies surrounding those interests?

(d) Defense use of victim and witness information – Public defenders expressed an interest in the criminal history of victims and witnesses for use during trial.

(1) How does the defendant's right to a fair trial influence access to victim and witness information?

(A) Is the information used for purposes other than impeachment?

(2) Is court oversight sufficient or should additional policies be considered?

(A) Access to victim and witness information is already regulated through discovery rules and subpoena procedures. The prosecution is required to provide criminal history information for witnesses in felony cases but not in cases involving misdemeanor offenses.

(B) Delays in the subpoena process were discussed; is there a viable alternative?

(i) Is there a level of access to victim and witness information appropriate for purposes of a public defender's investigation of a case that is not above that provided to the public?

(ii) What about private defense attorneys?

(3) Illinois law does allow investigators employed by the Death Penalty Trial Assistance and Capital Litigation Division of the State Appellate Defender to access LEADS data through the Illinois State Police for personal safety purposes only. Investigators are not permitted to disclose the information they obtain through LEADS. *See* 725 ILCS 105/10.

(e) Victim and witness information in court files – Information concerning victims and witnesses is routinely kept in court files.

(1) Because of the sensitive nature of this information, should the information be protected by the court?

(A) Absent protection of the information, citizens might not participate in the justice system.

(2) How much of this protection is a result of local rules that vary from circuit to circuit?

(A) The 11th Judicial Circuit Court's local rules prevent the filing of discovery documents other than the compliance certification (this was largely a storage space issue). However, in Champaign County there is no such rule; the prosecutor there files copies of discovery in the public file.

(B) There is ongoing discussion about whether this conduct comports with Supreme Court Rule 415(c) (discovery to remain in attorney's exclusive custody). No consensus has been reached other than to specifically authorize defense counsel's experts to see the discovery materials.

B. Accessibility of Social Security numbers

(a) Accessibility of SSNs by the justice system and the public – There is concern regarding the availability of Social Security numbers contained in justice information systems. This concern is not limited to disclosure of the SSN to the public; it also includes the accessibility of Social Security numbers by members of the justice community.

(1) Within the justice system, who should have access to SSNs and when? In other words, how are Social Security numbers used by the justice system?

(A) Public defenders may need SSNs to obtain credit reports on clients who are suspected of lying on their affidavit of indigence to get a "free lawyer." *See* 725 ILCS 5/113-3(b).

(B) What are law enforcement needs with respect to SSNs?

(C) The recent debate over the proposed Social Security Number Privacy and Identity Theft Prevention Act and its potential to frustrate key legal functions such as locating witnesses and criminals may be informative.

(D) Illinois has a SSN Protection Task Force that may provide some input into this issue. *See* 20 ILCS 4040/10.

(2) Should the justice system ever release Social Security numbers to the public?

(A) Identity theft concerns may bear strongly on the resolution of this issue.

(i) Note that Illinois law was amended in July 2004 to prohibit insurance companies from using SSNs on insurance cards; might these policy concerns impact the release of SSNs by an IIJIS system?

(ii) Is limiting the display of the SSNs to the last four digits a reasonable solution?

C. Availability of offender and victim health information

(a) Health information in the justice context – 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.

(1) Do current laws and regulations sufficiently address how these types of information are collected and shared *by the justice system*?

(A) What about prisoner medical records maintained by IDOC?

(B) LEADS Caution fields?

(C) How does HIPAA impact the Illinois justice system's sharing of this information?

(2) If not, what policies should be developed to ensure the proper protection of health information contained in justice information systems?

VI. Justice system accountability for complying with the privacy policy

(a) Means of accountability; audits – There should be some means of ensuring that system administers, participating agencies, and individual users are complying with privacy policy provisions.

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

(2) Should individuals be able to challenge an agency's compliance with the privacy policy?

(A) If so, how and where should such a challenge proceed?

(B) How might frivolous challenges be avoided?

(C) Do existing models for filing a complaint about police service meet these needs?

(D) Should ensuring compliance with the privacy policy be left to state agency directors and managers instead?

(3) Would periodic and systematic audits by an independent agency suffice?
- **(A)** What sorts of compliance issues should be audited?
  - **(i)** These audits should examine the data itself as well as the dissemination of the data.
- **(B)** Can the CHRI audit model serve as a good starting point?

(b) Non-compliance penalties and remedies – Accountability provisions are included in many statutes and regulations that govern the release of justice information in Illinois and across the nation.

(1) What are some of the current accountability mechanisms in place in Illinois and across the nation?
- **(A)** Are civil lawsuit remedies available?
  - **(i)** Can attorney's fees be awarded?
- **(B)** What about criminal penalties?
- **(C)** Administrative penalties?
  - **(i)** LEADS penalties include loss of certification and use of the system.

(2) What, if any, penalties are currently imposed where an Illinois justice agency fails to comply with its information system policies?

VII. Quality of justice information

(a) Duty to ensure the accuracy, completeness, and timeliness of justice data – Data quality is an important concern of any integrated justice information system. Data quality takes on significant importance in the development of sound information sharing policies. For instance, if the data contained in an information system is of uncertain quality, it is likely that the sharing of that data will be more restrictive than if the data could be verified as accurate. Restricting the sharing of potentially inaccurate data limits the possibility that users will act upon erroneous information.

(1) To ensure that integrated justice information systems are valuable sources of data, data contributed to the system may need to be validated or verifiable. Will guidelines be developed to reduce the amount of inaccurate data contributed to the system?

(2) Data quality concerns are not limited to the mere contribution of the data. The quality of the association of the data is also an important factor to consider. This also goes to the public's and the user's trust in the system. Will guidelines or rules be developed that regulate how the data will be compiled/associated in response to a user's inquiry?

(b) Official information stores – It is common for justice agencies to share their data with other agencies either by sending it in hardcopy form or electronically. However, if such copies are not updated on a regular basis, they can quickly become stale.

(1) Instead of storing the same information in different systems, would it be preferable to require agencies to search or request the official information store for a particular type of information?

(A) This would require some sort of designation that certain types of information are available from certain official sources.

(B) This may prove difficult when that information is already maintained in two places; for instance CHRI is available from the state police but dispositions and charging decisions are also available from the county court files. A policy choice may need to be made here.

(2) Should a recommendation be made that justice decision makers rely upon information from a recent search of the official information store as opposed to an old copy of the data?

(A) Regulations like this already exist for some pieces of justice information such as 30 days for CHRI data.

(3) Is there a preferred or official store for all critical pieces of justice information? If not, should there be?

(c) Establish who is responsible for quality data – Decision-makers throughout the justice system rely upon the information collected and maintained by multiple agencies.

(1) Who is ultimately responsible for ensuring the quality of the information?

(A) the collecting agency?

(B) the maintaining agency?

(C) the agency relying on the information to make a decision?

(2) What factors go into deciding who is responsible?

VIII. Intelligence information

(a) Intelligence information defined – There is concern about the government collecting information and creating dossiers about people in the absence of probable cause.

(1) What qualifies as intelligence information in the Illinois justice system?

(A) Is intelligence data information collected on "bad guys" before they commit a crime or is it somehow related to information collected during the investigation of a crime that has already been committed?

(2) How is intelligence information different from surveillance information? Is there a distinction?

(3) Do the provisions of the Privacy Act and the Department of Justice's intelligence systems regulations sufficiently protect the privacy interests of the citizens of Illinois?

(A) The consent decree involving the Chicago Police Department's Red Squad as modified by 7th Cir. U.S. Court of Appeals may provide insight into this area as well.

(4) If not, what protections should be included in a policy designed to regulate the sharing of intelligence information throughout the Illinois justice system?

(b) Combination of government and commercial data – The combination of commercial data into government information systems is also a concern because it may act as a detailed biography of citizens.

- **(1)** Do policies regulating the collection and combination of government and commercial data exist?
- **(2)** What about the other way around?
  - **(A)** What about regulation of the information collection activities of private commercial data providers whether they collect the information first hand or acquire it from government databases?
- **(3)** Should policies be developed to regulate this collection and combination of information?
- **(4)** If so, what should be included is such a policies?

(c) Triggering mechanisms to the collection of intelligence information – It seems unclear what conditions, if any, must be met before law enforcement can legitimately begin to gather intelligence information about someone.

- **(1)** What policies exist that define a triggering mechanism before intelligence information can be gathered and analyzed?
  - **(A)** *See People v. Roberts*, 349 Ill.App.3d 972, (4th Dist. 2004) where justices argued over what constituted a triggering mechanism to a warrant check during a traffic stop.

(d) Sharing of intelligence information – The potential sharing of intelligence information raises the stakes of these concerns.

- **(1)** What policies exist that regulate the sharing of intelligence information with members of the justice system?
  - **(A)** Is 28 C.F.R. § 23 the only federal regulation on point?
  - **(B)** What impact does the PATRIOT Act have on local law enforcement?
  - **(C)** Should an agency need to have established reasonable suspicion before requesting or receiving intelligence data from another agency?

(e) Quality of intelligence information – Raw investigative as well as intelligence data may be fraught with inaccuracies until it is verified or crosschecked with other data.

- **(1)** In light of the justice enterprise's paradigm shift from responding to criminal or terrorist activity to preventing such acts, what types of data quality considerations should be addressed in the context of intelligence information?
  - **(A)** Would data quality provisions only come into effect if the investigative or intelligence data were shared?
  - **(B)** Should data quality really be left up to those who use the data in a prosecution? In other words, is it a responsibility of investigators as collectors or prosecutors as ultimate users?

IX. Juvenile justice information

(a) Uniform interpretation of juvenile justice information requirements – Even though the treatment of juvenile justice information is codified, it is subject to local interpretations.

- **(1)** Is a uniform interpretation of the sharing of juvenile justice information needed?
  - **(A)** Are there any readily identifiable problems now?
- **(2)** Is there a need to educate justice practitioners about what information regarding juveniles can be shared?
  - **(A)** Juvenile officers are already trained in the law.
- **(3)** What about educating school officials who have access to police records of their students?

(b) Sharing of juvenile data – Generally, the Juvenile Court Act limits the commingling of juvenile justice data with adult criminal justice data. Nevertheless, improving the sharing of juvenile justice data among law enforcement might actually support the implementation of formal and informal station adjustment laws.

- **(1)** Section 5-905(5) of the Juvenile Court Act requires the law enforcement records concerning juveniles to be maintained separate from the records of adults unless otherwise permitted by law. Juvenile records are maintained in the CHRI repository because Section 1-7(B)(2) of the Juvenile Court Act permits the commingling of CHRI records.
- **(2)** How will integrated justice information systems maintain juvenile records separately from adult records?
- **(3)** Illinois has some policies that protect juvenile offenders who do not recidivate as adults. How long should juvenile justice records be maintained as part of an integrated justice information system?

(c) Juvenile sex offender registration – Sex offender registration requirements also impact juvenile justice information sharing policies.

- **(1)** How do juvenile sex offender registration provisions affect the confidentiality of juvenile justice information?
  - **(A)** Juvenile sex offenders are now on the sex-offender website.
  - **(B)** Juvenile sex offender registration and community notification held constitutional by the Illinois Supreme Court.

X. Impact of orders sealing or expunging criminal records

Court orders that seal or expunge otherwise complete and accurate criminal history records essentially remove that information from consideration by some potential users of the information. Such orders generally allow individuals to assert that they have never been convicted of a criminal offense.

(a) Gaps in the coverage of expungement and sealing orders – Generally, entities that are not named in an order sealing or expunging a record are not bound by its terms. However, with the prevalence of information systems that store copies of arrest and conviction information, gaps exist in the coverage of expungement and sealing orders.

- **(1)** What are the gaps in the coverage of those orders?
- **(2)** Should current expungement and sealing provisions apply in those gaps?
  - **(A)** Is the phrase "arrest records" as used in § 5 of the Criminal Identification Act clearly defined or can it be used to potentially cover those gaps? (*See People v. Hansen*, 198 Ill.App.3d 160 (4th Dist. 1990))
- **(3)** Is there any way to control the conduct of private information providers who acquire and compile their information from publicly available sources?
- **(4)** Whether an individual can correct the privately compiled criminal history record information seems to be an issue of critical importance here.
  - **(A)** Is it enough that an individual could send providers certified copies of the expungement order or are there too many providers for that to be feasible?

(b) Public's perception of expungement and sealing orders – Expungement and sealing orders prevent the Illinois State Police from reporting an individual's "actual" criminal history record.

- **(1)** Does this impact the public's perception of the completeness of Illinois' criminal history repository?
- **(2)** Is a "clean" record no longer considered clean because a conviction might have been sealed?
- **(3)** Should the privacy policy even deal with this issue or is it better left to state law?
- **(4)** Would legislative debates regarding the "completeness" of criminal history records be informative in deciding whether the IIJIS Privacy Policy needs specific expungement or sealing provisions?
- **(5)** May an applicant with an expunged record reply "No" when asked if he or she has ever been convicted of a crime?

Selected glossary of acronyms

CHRI – Criminal History Record Information; the term means data identifiable to an individual and consisting of descriptions or notations of arrests, detentions, indictments, informations, pretrial proceedings, trials, or other formal events in the criminal justice system or descriptions or notations of criminal charges (including criminal violations of local municipal ordinances) and the nature of any disposition arising therefrom, including sentencing, court or correctional supervision, rehabilitation and release. The term does not apply to statistical records and reports in which individuals are not identified and from which their identities are not ascertainable, or to information that is for criminal investigative or intelligence purposes. 20 ILCS 2635/3(G).

FIPs – Fair Information Practices; it is a general term for a set of standards governing the collection and use of personal data and addressing issues of privacy and accuracy. The FIPs include the eight guiding principles:

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 that give effect to the principles stated above.

IDOC – Illinois Department of Corrections.

FOIA – Illinois Freedom of Information Act, 5 ILCS 140/1 -11.

LEADS – Law Enforcement Agencies Data System; The Illinois Law Enforcement Agencies Data System (LEADS) is a statewide, computerized, telecommunications system, maintained by the Illinois State Police, designed to provide the Illinois criminal justice community with access to computerized justice related information at both the state and national level. LEADS has a number of components. They

include the Computerized Hot File (CHF); the LEADS Informational file; and access to the National Crime Information Center (NCIC), the National Law Enforcement Telecommunications System (NLETS), and the files of the Illinois Secretary of State (SOS). LEADS also provides an administrative messaging component, which serves as the primary method for data communications among law enforcement agencies statewide. The Caution File is made up of computerized records containing information about individuals who have demonstrated that they are dangerous to themselves or others, or are suspected of being involved in activities that constitute a violation of the criminal laws of the State of Illinois or the national government. Individuals falling into one or more of the following three categories can be found in the file: (a) Parolees from the Illinois Department of Corrections; (b) Sex offenders as mandated by the Sex Offender Registration Act or the Child Sex Offender and Murderer Community Notification Law; and (c) Field Notification Program subjects involved in violent crime, organized crime, narcotics, gambling, and general criminal activity.

N-DEx – Federal Bureau of Information's National Data Exchange project; it is a developing system that is expected to provide a nationwide capability to exchange data derived from police incident and event reports. Data from incident and arrest reports -- name, address, and non-specific crime characteristics -- will be entered into a central repository to be queried against by future data submissions. The national scale of N-DEx will enable rapid coordination among all strata of law enforcement; it is an effort to electronically share police incident report information across the nation.

PSI – Pre-Sentence Investigation; it is a report drafted by a probation officer that advises the court before imposing a sentence. A PSI typically includes, among other things, a statement of: (a) the defendant's history of delinquency or criminality; (b) the defendant's physical and mental history and condition; (c) the defendant's family situation and background; (d) information about special resources within the community which might be available to assist the defendant's rehabilitation; (e) the effect the offense committed has had upon the victim or victims thereof; and (f) information concerning defendant's eligibility for alternative sentencing options. 730 ILCS 5/5-3-2.

UCIA – Uniform Conviction Information Act, 20 ILCS 2635/1 -24; permits conviction information to be disseminated to the public.