JusticePrivacy.com

January 22, 2007

Proposal:

Retention standards in an integrated justice environment

Although retention periods were once necessitated by physical storage constraints, electronic storage of records has made destruction of criminal justice information largely unnecessary. Thus, whether to retain a piece of information indefinitely is now a matter of policy that should take into consideration the justice system's need for the information as well as the public's reasonable expectations of privacy in the data.

This proposal contains recommendations concerning the retention of information in an integrated justice information system. Specifically, it presents a set of factors that agencies can use to establish their own retention periods. Although drafted with Illinois law in mind, it is hoped that these factors can be used to explain why a particular piece of information is retained in a criminal justice information system for a certain period of time.

Retention standards in an integrated justice environment

The goals of the criminal justice system strongly influence its records retention policies. For instance, in 1976, Illinois's Criminal Justice Information Standards called for the purging of conviction information ten years after the date of release from supervision for serious crimes and five years after the date of release for less serious offenses.[1] If the individual had any subsequent contact with the justice system within that time period, the information would not be purged from the computerized criminal history records. This policy ensured record retention for recidivists while acknowledging research findings that people are less likely to commit crimes as they grow older. As the goals of rehabilitation and reintegration gave way to punishment and deterrence, records retention policies favored more permanent retention of criminal history information.[2]

Although there are several reasons to retain official criminal history records for a substantial period of time, these reasons may not apply to every type of information collected and maintained as part of an integrated justice information system. Furthermore, the government's indefinite retention of justice records enhances certain information dissemination risks. The justice system is continuously collecting information about individuals. This continuous collection, combined with indefinite retention of that information, makes a vast amount of data available for potential misuse or accidental disclosure. Additionally, retaining certain types of information indefinitely can be a form of undesirable social control that can prevent people from engaging in activities that further their own self-development, and inhibit individuals from associating with others, which is sometimes critical for the promotion of free expression.

Nevertheless, justice practitioners and policy makers are hesitant to destroy records. The government's reluctance may be rooted in investigators' experience that seemingly irrelevant or untimely information may acquire new significance as an investigation brings new details to light.[3] Deleting or destroying information, justice practitioners argue, would impede investigations and potentially result in fewer cases being solved.

Even though agencies in Illinois are not required to dispose of their electronic records, some agencies may choose to remove data from their information systems as a means to address the public's privacy concerns or simply to reduce the costs of storing the numerous back-up tapes necessary to ensure a computer system can recover from an unforeseen disaster. The following factors are provided to assist agencies interested in setting retention periods for the personally identifying information contained in their integrated justice information systems.

---

[1] Criminal Justice Information Systems Standard 7.5 (3)(b) included in the State of Illinois Criminal History Record Information Plan submitted to the U.S. Department of Justice on March 16, 1976 on file with the Illinois Criminal Justice Information Authority.

[2] Those views are still dominant today. In 2003, a bill that called for the automatic sealing of arrest, conviction, and court records of misdemeanors three years after the completion of sentence, so long as the offender was not arrested during that period, failed to pass into law. H.B. 2391 93d Gen. Assembly (Ill. 2003).

[3] *See* 68 Fed. Reg. 14140 (2003).

There is no simple formula for determining how long the various types of information contained in an integrated justice information system should be retained. Rather, a process that evaluates the following six factors should aid agencies in setting reasonable retention standards. Although no relative weights are assigned to them, the factors are arranged in an approximate order of importance. Thus, the relevant statutes of limitation and potential future usefulness of the personally identifiable information at issue is to some extent more significant than the quality or sensitivity of the information and so on.

Additionally, the factors are interrelated. For example, the fact that a piece of information is extremely sensitive (e.g., the name of an 11-year-old rape victim) should not be considered alone. Instead, an agency also should take into account whether the information system containing that data employs strict access and use controls; if so, those controls can lessen the sensitivity factor's impact upon the determination of how long to retain the information. Each of the factors is explained in greater detail below.

These factors are not beyond criticism. The application of the factors is susceptible to multiple interpretations. Two agencies can review the same facts about a piece of personally identifiable information and come to different conclusions about how long it should appropriately be retained. This is the result of the many judgments that must take place during the course of the analysis.[4] Additionally, because of these numerous judgments and interpretations, system designers may find it difficult to incorporate this factor analysis into an integrated justice information system. Nevertheless, agencies can utilize these factors to better explain their reasons for retaining each type of information for as long as they do.

The following factors are proposed merely as a guide to agencies that want to set retention periods for the personally identifying information contained in their integrated justice information systems. They are an attempt to fill a gap in this area, which has historically relied heavily upon storage cost considerations, and to do so in the unique context of today's sophisticated and technologically advancing criminal justice system.

Factor 1. Statutes of limitation

Statutes of limitation exist to encourage prompt investigations and prevent stale prosecutions.[5] The Illinois Local Records Commission considers statutes of limitation when it sets minimum retention periods for justice records. More information about existing retention periods and their dependence on statutes of limitations can be found in *Table 2: Retention periods for justice information under the Local Records Act* located near the end of this proposal.

When personally identifiable information is associated with crimes not subject to a statute of limitations, the balance of factors tips in favor of a longer retention period. On the other hand, where personal information is collected during an investigation of a crime that is subject to a shorter statute of limitation, this balance shifts toward setting a shorter retention period.

[4] Such analyses are not uncommon in the law. *See*, among others, Wade, On the Nature of Strict Tort Liability for Products, 44 MISS.L.J. 825, 837- 38 (1973) (proposing a seven factor analysis useful in determining whether a product is defective) and 735 ILCS 5/2-801 (setting forth the factors necessary to sustain a class action in Illinois).

[5] Statutes of limitations for criminal offenses can be found in scattered provisions of the Criminal Code. *See* 720 ILCS 5/3-5 – /3-8(Illinois's general limitations periods); 35 ILCS 105/14 (3-year limitation period for violations of the Use Tax Act); 35 ILCS 505/15(7) (5-year limitation period for violations of Motor Fuel Tax Law); 740 ILCS 10/6(2) (4-year limitation period for violations of the Illinois Antitrust Act).

Nevertheless, certain characteristics of a criminal case may extend or toll statutes of limitation.[6] When a case contains any of the characteristics set forth in the following table, the balance of factors tips in favor of a longer retention period.

Extended limitations
STATUTES OF LIMITATION ARE EXTENDED IN THE FOLLOWING CIRCUMSTANCES.
❑ A theft that involves a breach of fiduciary duty owed to an individual with a legal disability
❑ Misconduct in office by a public officer or employee
❑ Any violation of the Environmental Protection Act
❑ Identity theft offenses
❑ Sex offenses where: • victim and defendant are family members or in a professional or fiduciary relationship; or • the victim reports the crime within 2 years of its commission
❑ Criminal sexual assault, predatory criminal asexual assault of a child, or aggravated criminal sexual abuse
❑ Child pornography or indecent solicitation of a child
Tolling periods
THE TIME PERIOD IN WHICH A PROSECUTION MUST TAKE PLACE DOES NOT INCLUDE THE FOLLOWING PERIODS.
❑ The defendant is not residing in Illinois
❑ Defendant is a public officer and the offense charged is theft of public funds while in office
❑ A material witness is on active military duty or leave
❑ Prosecution is pending against the defendant
❑ Proceedings relating to the quashing or enforcement of a grand jury subpoena are pending

The final statute of limitations consideration involves crimes based upon a series of acts performed at different times. Under Illinois law, the statute of limitations for these types of crimes begins to run when the last act is committed.[7] Such crimes typically include conspiracy[8] and thefts by deception that continue over a period of time.[9] The balance of factors tips in favor of a longer retention period when the information collected concerns a crime that may be one of a series of continuous acts.

Factor 2. Potential future usefulness of the information

Information collected as part of an investigation may have usefulness beyond the life of the case. Not only could information be part of a continuing series of acts as discussed in the statute of limitations factor, but information may be useful to generate leads for the investigation of subsequent crimes. For example, information collected as part of an investigation for misdemeanor trespass upon a power plant may be useful if that power plant is subsequently damaged due to an explosion. Additionally, the repetitive nature of domestic violence and its escalating pattern of abuse counsel a longer retention period for victims' reports of domestic violence, even where charges are not brought. This longer retention period allows the victim and prosecutor to establish a pattern of abuse, even if the first several instances of abuse were not

[6] 720 ILCS 5/3-6; -7.
[7] 720 ILCS 5/3-8.
[8] *People v. Konkowski*, 378 Ill. 616 (1941) (holding the period of limitation begins to run not from the time that the conspiracy was entered into, but from the commission of the last overt act in furtherance of the common design).
[9] *See People v. Blitstein*, 192 Ill. App. 3d 281 (1st Dist. 1989).

actionable. Thus, agencies should consider whether the type of victim and the type of crime committed warrant keeping the information for a period longer than the statute of limitations alone advises.

Agencies should also consider whether the information is appropriate for the forms of crime analysis used by the participants in the integrated justice information system. *Table 1: Categories of information most useful for traditional crime analysis* contains a listing of the types of information most commonly utilized to analyze similarities of different crimes to connect them to a common offender. Other types of information can assist justice agencies in the management of their resources. Data such as the number and types of calls-for-service received by a police department, the average amount of time spent responding to and investigating those calls, the number of hours devoted to non-patrol tasks, and the desired percentage of uncommitted time per unit per shift, can help a police agency assess how many officers it needs and how to deploy them.[10] The balance of factors weighs in favor of a longer retention period where the information is not personally identifiable and particularly useful for purposes of crime analysis.

Information collected as part of an investigation may also serve important officer safety needs. For example, it can be useful for responding officers to know that their department has responded to domestic violence calls at a particular location in the past. Information about a suspect's use of violence toward police officials can also keep officers safe. In general, the balance of factors tips in favor of a longer retention period when the information is likely to improve officer safety.

Some considerations that reduce the potential future usefulness of information might weigh in favor of shorter retention periods. First, retaining vast amounts of data for long periods may undermine the usefulness of an integrated justice information system over time. Depending upon its capabilities, the overall performance of an information system may decrease as the amount of data stored increases. Not only might it take longer for the system to search its vast repository of data, but the system might also return too much information for a user to sort through effectively. This factor cautions against overly broad interpretations and expectations of the potential future usefulness of a given type of information and tips the balance of retention factors toward a shorter period when the information isn't likely to generate a useful investigative lead, inform a crime analysis technique, or enhance officer safety.

Another consideration that might reduce the potential usefulness of information is lack of public support of the system and its information practices. The public's reasonable expectations of how a piece of information may be used in the future should be considered in the analysis of this factor. In most instances, the public's expectations likely are parallel to the justice system's practices; this is true especially in regard to generating future leads, informing crime analyses, and helping to ensure officer safety. Nevertheless, in some instances it may be necessary to inform the public of how a particular piece of information may be used by the justice system in the future. Upsetting reasonable expectations can subject an integrated justice information system to intense public scrutiny and lead to the public's refusal to report crimes or its failure to provide useful information to justice officials in the future. When taking the public's expectations into account, it might be useful to consider the availability of a substitute source of

[10] Steven Gottlieb, *et al.*, Crime Analysis: From First Report to Final Arrest 34-38 (1994).

information that would meet the same need but not contain the same risks of alienating the public's trust and confidence in the justice system.

Factor 3. Data quality

Several privacy groups have intentionally avoided the interaction of data quality with privacy issues. Some have started their discussions with the premise that the data contained in integrated justice information systems is timely, accurate, and complete. This premise is intended to ensure that recommendations are based solely upon genuine privacy concerns, and are not made more restrictive simply because the data at issue might be wrong. Other groups have acknowledged the interplay between data quality and privacy interests and will discuss these issues in significant detail at a future time so that national groups can take the lead and provide guidance to state and local justice entities.

Much is already known about the timeliness, accuracy, and completeness of the data maintained in the State's criminal history repository;[11] however, the same cannot be said about all the types of information that may be included in an integrated justice information system. Data quality encompasses several different dimensions that can affect how an agency considers this factor when developing retention periods. To ensure that integrated justice systems are valuable sources of information, data contributed to and compiled by these systems may need verification or validation. Additionally, data quality concerns are not limited to the mere contribution of data. The quality of the association of the information in response to a user inquiry is also a consideration in this factor.

For the limited purpose of expanding upon this retention factor, it is sufficient to explain that information of a higher caliber and reliability and that is accurately attributed to the right individuals should be retained longer than information that is of lesser quality or from a less reliable source that is inaccurately complied. The Global Privacy and Information Quality Working Group's current work will assist justice agencies in assessing and enhancing the quality of the data contained in integrated justice information systems.

Factor 4. Sensitivity of the information

Due to the nature of the justice system, a retention period based primarily upon the sensitivity of the information is not practicable. This is because sensitive information about offenders, victims, witnesses, and even jurors, is frequently necessary for justice practitioners to make sound public safety decisions and to enforce the criminal laws. For the purposes of setting an appropriate retention period for various types of justice data, the sensitivity of the information should be considered in relation to that information's potential future usefulness, the information system's technologically implemented policy controls, and the social desirability of the government's retaining the information.

The amount of protection that must be provided by these other factors will depend significantly upon the relative sensitivity of the information. The more sensitive a piece of information is, the more protection these other factors may need to provide in order to support a longer retention

[11] Since 1979, the Illinois Criminal Justice Information Authority has conducted fourteen audits of the state's official CHRI repository. The most recent audit was completed in 2006 and is available from the Authority website at: http://www.icjia.state.il.us/public/pdf/CHRI/2006CHRIAuditReport.pdf.

period. The public's perception that the justice system can adequately protect private information is important when establishing retention periods for sensitive data. The higher the public's confidence, the more receptive the public may be to a longer retention period. Conversely, if public confidence in the justice system's ability to maintain the confidentiality of information is low, the public may favor limiting the period of time that information is available to justice practitioners.

Examples of information that might be considered more sensitive include: (a) the identities of child and sexual assault victims; (b) the location of domestic violence victims; (c) individuals' Social Security numbers; and (d) individuals' medical information collected by the justice system. Less sensitive information includes publicly available information and may not require substantial protections from the other factors in order to tip the balance in favor of a longer retention period. Examples of less sensitive information include the identities of arrestees and convicted persons, conditions of supervised release and probation, and sex offender registration information.

Factor 5. Technologically implemented policy controls

This factor is included in the retention analysis to address the potential risks of harm associated with accidental and abusive disclosure of the information. It is related to the sensitivity factor because the more sensitive a piece of information, the more harm an individual may suffer if that information is improperly released. Agencies weighing this factor should assess their information system's ability to avoid or mitigate these risks through training and technological access restrictions on the data.

Using information technologies to implement sound policy controls is one way to promote the public's confidence in the justice system's ability to keep sensitive information confidential and limit authorized users' misuse of the data. As touched upon in the discussion of the sensitivity factor, the public's trust in the justice system is an important consideration when setting retention periods. If an agency has not reduced the risks of improper disclosure through the exercise of due care in the development and use of the information system, a shorter retention period may be appropriate. A shorter retention period reduces the amount of data in the information system available for inadvertent disclosure or purposeful misuse.

This factor tips in favor of a longer retention period, however, where an agency has reduced these risks by technologically implementing sound policy controls. Examples of privacy enhancing technologies include, but are not limited to:

- **(a) Rule-based processing functions** – Rule-based processing ensures that data provided by multiple sources and subject to various access rights can only be accessed under the proper conditions.[12] It permits access permissions to be developed based upon the user's role in the justice system and allows integrated justice information systems to directly incorporate privacy protections into the system's design.
- **(b) Selective revelation** – Selective revelation keeps sensitive data anonymous until a user certifies that he has a demonstrable need for the data subject's identity.[13] Methods of

[12] K.A. Taipale, *Data Mining and Domestic Security: Connecting the dots to make sense of data*, 5 COLUM. SCI. & TECH. L. REV. 2 (Dec. 2003).
[13] Latanya Sweeney, *Privacy-Preserving Surveillance using Selective Revelation* (October 2005). *Source*: http://privacy.cs.cmu.edu/dataprivacy/projects/selectiverevelation/pps.pdf.

certifying the user's need for the information will vary by agency, but once certified, the system reveals the sensitive information to the user.

(c) **Encryption** – Encryption adds another layer of protection to the data itself while still permitting the system to link data concerning individuals. Encrypting personally identifying information can keep the information anonymous until selective revelation rules apply. It also protects against accidental loss of the information; even if an unauthorized individual gains access to the system, the data will be useless to the intruder without a key to decode the data into a usable form.

(d) **Audit trails** – An audit trail is a record showing who has accessed a computer system and what operations the user performed during a given period of time. Strong audit functions document how users interact with the integrated justice information system and hold users responsible for improper use of the system's data.

Factor 6. Social desirability of the government retaining the information

The government's compilation and indefinite retention of information about individuals creates the risk that individuals will become more cautious in the exercise of their protected rights of expression, protest, association, and political participation. The social desirability factor is included in the retention analysis to address these potential chilling effects.

Although the social desirability factor has its roots in the public's exercise of First Amendment conduct, the factor is broader in scope. It is an acknowledgement that personally identifiable information brought together from various source systems has the potential to reveal an individual's beliefs or ideas concerning public or social policy, as well as political, educational, cultural, economic, philosophical, or religious matters. When establishing retention periods, agencies should consider the social consequences of the government's collection and indefinite retention of considerable quantities of personally identifiable information. Some of these potential consequences include:[14]

(a) Developing a prevailing climate of suspicion;

(b) Limiting police agencies' focus to easily detectable and provable offences;

(c) Limiting or denying individuals' due process protections when they are suspected of criminal conduct based upon analysis of data contained in the information system;

(d) Increasing individuals' desire to opt out of the official level of society to prevent information about them from being collected by the government; and

(e) Enhancing the repressive potential for a totalitarian government.

In order to limit these consequences, the social desirability factor requires agencies to consider the totality of the information contained in their integrated justice information systems when setting the retention period for a particular piece of data. These consequences can also be limited by considering the sensitivity of the data, the future uses of the data, and the information system's technologically implemented policy controls.

[14] Michael Froomkin, *The Death of Privacy?* 52 Stan. L. Rev. 1461, 1471-1472 (2000).

Figure 1. Factor analysis for retention periods

Factors supporting longer data retention	Factors supporting shorter data retention
STATUTE OF LIMITATIONS	
❑ The data is associated with crimes not subject to a statute of limitation.	❑ The data is associated with a crime that is subject to a short statute of limitation.
❑ Circumstances exist which extend the limitation period.	❑ No extension criteria exist.
❑ Circumstances exist that toll the operation of the statute of limitation.	❑ None of the statute of limitation tolling provisions applies.
❑ The data is associated with a crime based upon a series of acts performed at different times.	❑ The crime committed is based upon a single act.
POTENTIAL FUTURE USEFULNESS OF THE INFORMATION	
❑ The data is useful to generate future investigative leads.	❑ Based upon the type of victim and type of crime committed, the data is not likely to assist future investigations.
❑ The data is useful for crime analysis purposes.	❑ Retaining the data may reduce the overall performance of the information system.
❑ The data can by used to enhance officer safety.	❑ The public is unlikely to support the government's retention of this information and a substitute source of data exists that would meet the same need.
DATA QUALITY	
❑ The data is contributed from a reliable source.	❑ The accuracy or reliability of the data is unknown.
❑ The data is accurately attributed to the correct individual once it is included in the information system.	❑ It is unknown how accurate the information system's responses to user inquiries are.
SENSITIVITY AND TECHNOLOGICALLY IMPLEMENTED POLICY CONTROLS	
❑ The data is very sensitive but the information system incorporates several technologically implemented privacy protections.	❑ The data is very sensitive but the information system has not incorporated privacy protections into the information system's design and operation.
❑ The data is not of a personally identifiable or sensitive nature.	❑ The system is not regularly audited to ensure the technologically implemented policy controls are performing properly.
SOCIAL DESIRABILITY OF THE GOVERNMENT RETAINING THE INFORMATION	
❑ The data, when contributed to and analyzed with the rest of the information already contained in the information system, does not restrict or is incidental to the exercise of First Amendment rights.	❑ The data, when compiled with the rest of the information contained in the integrated system, has the potential to reveal individuals' thoughts or beliefs concerning public or social policy.

Table 1: Categories of information most useful for traditional crime analysis

Police agencies utilize crime analysis to prevent and suppress crime, apprehend offenders, and recover stolen property.[15] Crime analysis is usually conducted on offenses with discernable patterns and trends that can be prevented or reduced through the implementation of directed action plans.[16] A review of existing police crime analysis operations reveals that burglary, robbery, auto theft, larceny, fraud, sex crimes, aggravated assaults, and murder are the crimes most appropriate for crime analysis.[17] Experienced analysts have found that the factors listed below (the numbers in parentheses suggest the order in which the data should be searched) often help determine if a pattern exists.[18]

Residential Burglaries	Commercial Burglaries
❑ Geographic factors (1) ❑ Time factors (2) ❑ Property loss descriptors (2) ❑ Victim descriptors[19] (2) ❑ Physical evidence descriptors (2) ❑ Specific modus operandi factors[20] (2) ❑ Suspect vehicle descriptors (3) ❑ Suspect descriptors (3)	❑ Geographic factors (1) ❑ Victim descriptors (1) ❑ Specific modus operandi factors (1) ❑ Property loss descriptors (2) ❑ Physical evidence descriptors (2) ❑ Time factors (3) ❑ Suspect vehicle descriptors (3) ❑ Suspect descriptors (3)
Thefts From Vehicles	**Sexual Offenses**
❑ Geographic factors (1) ❑ Property loss descriptors (1) ❑ Suspect vehicle descriptors (1) ❑ Time factors (2) ❑ Victim descriptors[21] (2) ❑ Physical evidence descriptors (2) ❑ Specific modus operandi factors (2) ❑ Suspect descriptors (3)	❑ Time factors (1) ❑ Victim descriptors (1) ❑ Suspect descriptors (1) ❑ Victim-suspect relationship (1) ❑ Geographic factors (2) ❑ Physical evidence descriptors (2) ❑ Specific modus operandi factors[22] (2) ❑ Suspect vehicle descriptors (2)

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

Strong-Arm Robberies	Armed Robberies
❑ Geographic factors (1) ❑ Time factors (1) ❑ Victim descriptors[23] (1) ❑ Property loss descriptors (2) ❑ Physical evidence descriptors (2) ❑ Specific modus operandi factors[24] (2) ❑ Suspect descriptors (2) ❑ Suspect vehicle descriptors (3)	❑ Geographic factors (1) ❑ Time factors (1) ❑ Suspect descriptors (1) ❑ Victim descriptors (2) ❑ Specific modus operandi factors (2) ❑ Suspect vehicle descriptors (2) ❑ Property loss descriptors (3) ❑ Physical evidence descriptors (3)

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

Table 2: Retention periods for justice information under the Local Records Act

Nothing in Illinois law requires a local agency to destroy any of its records. Nevertheless, when an agency chooses to dispose of any of its records, it must follow the requirements set forth in the Local Records Act.[25] Specifically, the Act requires agencies to obtain the written approval of the appropriate Local Records Commission before disposing of public records.[26] To assist in this approval process, the Illinois Local Records Commission has established minimum retention periods for several types of justice agency documents.

When it set minimum retention periods for local justice agencies' police reports and records of investigations, the Local Records Commission took into consideration, among other factors, the type of crime being reported and its statute of limitations. Reports and investigatory records concerning crimes that are subject to the state's general statute of limitations (3 years for a felony and 6 months for a misdemeanor) must be preserved for at least 7 years.[27] This 7-year period is meant to provide for the extension and tolling provisions available under Illinois law.[28]

Some criminal conduct is not subject to a statute of limitations. Police incident reports, investigatory records, and case files concerning the following crimes must be retained for a period of not less than 80 years:[29]

(1) First degree murder;
(2) Attempt to commit first degree murder;
(3) Second degree murder;
(4) Involuntary manslaughter;
(5) Reckless homicide;
(6) Treason;
(7) Arson;
(8) Forgery;
(9) Thefts involving breach of a fiduciary obligation where the aggrieved party has been declared to have a legal disability; and

---

[25] 50 ILCS 205/1 -/17 implemented by ILL. ADMIN. CODE tit. 44 §§ 4000; 4500; *see also* 720 ILCS 5/32-8 (making it a Class 4 felony to destroy public records without lawful authority).

[26] 50 ILCS 205/7. Agencies must file an Application for Authority to Dispose of Local Records with the appropriate commission and submit a Local Records Disposal Certificate, which must be submitted sixty days in advance of the destruction of any records listed on the Disposal Certificate. Local agencies cannot dispose of records without first filing these documents. State agencies are subject to similar requirements under the State Records Act, 5 ILCS 160/1 -/26. Note that court records must be destroyed under the supervision of the Illinois Supreme Court and in accordance with the Supreme Court's General Administrative Order on Recordkeeping in the Circuit Courts. 50 ILCS 205/4.

[27] 720 ILCS 5/3-5(b). Illinois law currently lacks a precise statement regarding the start of the limitation period; this may create some ambiguity in the establishment of retention periods. *But see*, *People v. Mudd*, 154 Ill.App.3d 808, 814 (4th Dist. 1987) (applying the principle applied by most Illinois courts that "statutes of limitations normally begin to run only 'when the crime is complete[,]'...and the crime here was complete only upon the existence of the last element, the death of the victim" [internal citations omitted]).

[28] 720 ILCS 5/3-6; -7.

[29] *See* 720 ILCS 5/3-5(b).

(10) Sex offenses where the identity of the offender is unknown, but his DNA profile is obtained and entered into a DNA database.

Police incident reports and investigatory records concerning sex offenses where the victim is a minor must be retained for at least 22 years.[30]

The following table is provided to illustrate the numerous types of local police agency records, some of which might be included in an integrated justice information system, and their currently established minimum retention periods.[31]

Local police department record	Retention period
CRIMINAL INCIDENT REPORTS & INVESTIGATORY RECORDS	
❑ Incident reports / cards	Retention period is based upon the type of crime reported as discussed above – either 7, 22, or 80 years
❑ Criminal offense reports	
❑ Officers investigation and supplementary report	
❑ Investigative & follow-up reports	
❑ Detective files	
❑ Videotape of cases (e.g., tapes of crime scenes, traffic accident scenes, DUI arrests, etc.)	
❑ Adult case files / arrest jackets	
OTHER CRIMINAL REPORTS AND RECORDS	
❑ Child abuse case reports and letters from DCFS that state whether allegations were founded or unfounded	**Unfounded:** dispose of letter upon notification of official findings. **Indicated or undetermined:** records must be retained for 80 years.
❑ Tip sheets	Where the tip is regarding a crime not subject to a statute of limitations, retain the document permanently; otherwise, retain for 7 years.
❑ Crimestopper reports (i.e., documents providing tips, suspects, and information pertaining to crime)	1 year
❑ Neighborhood watch records	5 years
❑ Deceptive practice correspondence to police	7 years
❑ Gang member indices (names of reported gang members, address, etc.)	20 years
❑ Latent fingerprints from crime scenes	Where the latent print relates to a crime not subject to a statute of limitations, retain the print for 80 years; otherwise, retain for 7 years.
❑ Method of operation file cards	Permanently retained

[30] *See* 720 ILCS 5/3-6(c), (d), (e) (providing that certain sex offenses against children can be prosecuted up to 3 years after the victim reaches the age of 18).

[31] The following discussion includes guidelines used by the commission; agencies are cautioned that they do not have authority to destroy records without first complying with the requirements of the Local Records Act. *See* text accompanying *supra* note 26.

Local police department record	Retention period
❑ Voluntary statements	7 years, except for non-expiring statute of limitation cases which must be retained permanently
❑ Juvenile case files	**Cook County:** Until the earlier of the subject's 80th birthday or death; **Downstate:** One year after subject reaches legal age
❑ Field contacts	5 years, provided the files do not become part of an investigative or criminal history file; if so then dispose of with the file.
❑ Field interrogation cards	2 years after date of receipt of report
❑ Field interview report	1 year
❑ Vehicle theft case report	**Recovered:** 1 year **Not recovered:** 10 years
❑ Stolen vehicle reports (including supplemental reports, tow-in-theft recovery reports, vehicle impoundment, and inventory reports)	2 years
❑ Victim/witness program intake case files index	7 years after case is closed.
❑ Suicide reports	7 years where the cause of death has been ruled a suicide.
CRIMINAL HISTORY DOCUMENTS	
❑ Arrest cards (including mug shots, photographs, fingerprints, etc.,)	Retain until 1 year after death or until subject reaches his 80th birthday.
❑ Arrest booking forms	**Adult:** retain for 1 year, provided that information is transferred to arrest record. **Juvenile:** retain until 1 year after subject reaches legal age.
❑ Fingerprint files	Retain until 1 year after death or until subject reaches his 80th birthday.
❑ Rap sheets	May be disposed of once document has fulfilled its administrative use.
❑ Criminal history dissemination logs	2 years after date of last entry
❑ Nickname indices	Retain until 1 year after death or until subject reaches his 80th birthday.
❑ Police blotters	1 year
❑ Expungement orders	3 years
DOMESTIC VIOLENCE RECORDS	
❑ Domestic violence file (any court order or case file)	7 years
❑ Orders of protection	3 years following duration of the order **If extended:** 3 years from last expiration date
❑ Expired orders of protection	1 year after expiration
NON-CRIMINAL INCIDENT REPORTS & RECORDS	
❑ Community problem files (i.e., copies of complaints from citizens)	2 years
❑ Accident reports (traffic & non-traffic)	7 years
❑ Non-traffic complaints	3 years
❑ Lost or stolen drivers license or plates reports	2 years
❑ Unusual occurrence reports	2 years

Local police department record	Retention period
❑ Parking tickets	1 year
❑ Warning tickets/notices	60 days
❑ Miscellaneous incident reports (e.g., minor incidents, incidents not requiring a case report, non-criminal actions, etc.)	2 years
❑ Unfounded complaints against police officers	4 years after case is closed
ADMINISTRATIVE RECORDS & STATISTICAL INFORMATION	
❑ Case assignment books (i.e., ledger books that include lists of case numbers and the name of the detective assigned to each case)	2 years
❑ Officer's daily activity reports	2 years
❑ Shift commander daily activity report	2 years
❑ Requests for police reports	2 years
❑ Requests for traffic accident reports	1 year
❑ Overnight parking log	Retain until administrative use is complete.
❑ Police Information Management System (P.I.M.S.) statistical report	1 year, provided that information is audited and verified.
❑ Illinois Uniform Crime Reports (UCR) arrest/offense summaries	1 year, provided that information is audited and verified
COMPUTER & RADIO USAGE DOCUMENTS	
❑ Computer Aided Dispatch (C.A.D.) radio log	10 years
❑ Computer user logs	2 years
❑ Radio transmission logs	10 years
❑ Radio transmission tapes – Cook County	Retain tape recordings of phone calls, 911 calls, and radio transmissions for 30 days. Retain tapes related to pending litigation until 30 days after the case is closed. Retain handwritten radio logs of miscellaneous information for 1 year.
❑ Radio transmission tapes – Downstate	Retain tape recordings of phone calls, and radio transmissions for 30 days. Retain tapes related to pending litigation until 30 days after the case is closed.
MISCELLANEOUS RECORDS	
❑ State hospital escape list	1 year after cancellation
❑ Missing or wanted person reports	1 year after cancellation
❑ Firearms transaction records	Permanently retained
❑ Habitual Sex Offender Registration Act form	Permanently retained
❑ Sex offender registration	10 years
❑ Request for telephone tap	7 years
❑ Confidential source / information file	Until administrative use is complete
❑ Name index file (incidents, accidents, etc.)	Permanently retained
❑ Victim/suspect index cards	7 years
❑ Internal department investigations	5 years after case is closed

Local police department record	Retention period
PHOTOGRAPHS & VIDEOS	
❑ Mug shots	Retain until 1 year after death or until subject reaches his 80th birthday.
❑ Video tapes of bookings	Retain tapes for 7 days. Retain tapes related to pending litigation until 30 days after the case is closed.
❑ Wanted posters	1 year after apprehension
❑ Photographs of prisoner runaways and escapees	1 year after runaway/escapee is apprehended
WARRANT INFORMATION	
❑ Warrants	3 years following service
❑ Warrant information sheets	3 years following service
❑ Warrant index card file	3 years
❑ Warrant index (cancelled)	2 years
❑ Warrant recall (quash order)	4 years
PRISONER RECORDS	
❑ Prisoner phone logs	2 years
❑ Prisoner medication log	5 years
❑ Prisoner's medical records	5 years after release from custody
❑ Mittimus	2 years