Face Comparison

Policy

Draft – 10 Feb 2020

A. Purpose Statement

1. Face comparison technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons. The Chicago Police Department's Crime Prevention & Information Center (CPIC) utilizes face comparison programs to support the investigative efforts of law enforcement and public safety agencies both within and outside the City of Chicago.

2. It is the purpose of this policy to provide CPIC personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a face comparison (FC) program. This policy will ensure that all FC uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties (P/CRCL) of individuals.

Further, this policy will delineate the manner in which requests for face comparison are received, processed, catalogued, and responded to. The Fair Information Practice Principles (FIPPs) (See Appendix B for more information) form the core of the privacy framework for this policy.

This policy assists CPIC and its personnel in:

- Increasing public safety and improving state, local, tribal, territorial, and national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Fostering trust in the government by strengthening transparency, oversight, and accountability.
- Making the most effective use of public resources allocated to public safety entities.

3. All deployments of the face comparison system are for official use only/law enforcement sensitive (FOUO/LES). The provisions of this policy are provided to support the following authorized uses of face comparison information:

- An active or ongoing criminal or homeland security investigation.
- To mitigate an imminent threat to health or safety.
- A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity.
- To assist in the identification of a person who lacks capacity or is otherwise unable to identify him- or herself (such as an incapacitated, deceased, or otherwise at-risk person).
- To investigate and/or corroborate tips and leads.

- For comparison to determine whether an individual may have obtained one or more official state driver's licenses or identification cards that contain inaccurate, conflicting, or false information.
- To assist in the identification of victims of violent crime.
- To support law enforcement in critical incident responses and special events.

B. Policy Applicability and Legal Compliance

1. This policy was established to ensure that all images are lawfully obtained, including face comparison probe images obtained or received, accessed, used, disseminated, retained, and purged by the CPIC. This policy also applies to:
- Images contained in a known identity face image repository and its related identifying information.
- The face image searching process.
- Any results from face comparison searches that may be accessed, searched, used, evaluated, retained, disseminated, and purged by the CPIC
- Lawfully obtained probe images of unknown suspects that have been added to unsolved image files (refer to section L.3), pursuant to authorized criminal investigations.

2. All CPIC personnel, participating agency personnel, and authorized individuals working in direct support of CPIC personnel (such as interns), personnel providing information technology services to the CPIC, private contractors, and other authorized users will comply with the CPIC's face comparison policy and will be required to complete the training referenced in section N.2. . An outside agency, or investigators from an outside agency, may request face comparison searches to assist with investigations only if CPIC**:**
- The outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in section A. Purpose Statement, item 3. and the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number) and acknowledges an agreement with the following statement:

  The result of a face comparison search is provided by the CPIC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

3. The CPIC will provide a printed or electronic copy of this face comparison policy to all:
- CPIC and non-CPIC personnel who provide services
- Participating agencies
- Individual authorized users

The CPIC will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and its applicable provisions.

All CPIC personnel, participating agency personnel, and authorized individuals working in direct support of CPIC personnel (such as interns or volunteers), personnel providing information technology services to the CPIC, private contractors, agencies from which CPIC information originates, and other authorized users will comply with applicable laws and policies concerning P/CRCL, including, but not limited to the Illinois Biometric Information Privacy Act. (See Appendix C for a list of Federal Statutes and Appendix D for other Illinois Statutes.)

C. Governance and Oversight

1. Primary responsibility for the operation of the Chicago Police Department's justice information systems, face comparison program and system, operations, and the coordination of personnel; the receiving, seeking, retention, evaluation, data quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the Deputy Chief of the Bureau of Technology Services of the Chicago Police Department.

2. The Chicago Police Department's Deputy Chief of the Bureau of Technology Services will designate an administrator who will be responsible for the following:

- Overseeing and administering the face comparison program to ensure compliance with applicable laws, regulations, standards, and policy.
- Acting as the authorizing official for individual access to face comparison information.
- Ensuring that user accounts and authorities granted to personnel are maintained in a current and secure "need-to-know" status.

3. The CPIC has authorized access to and can perform face comparison searches utilizing face comparison software (i.e., DataWorks, etc.). The Chicago Police Department contracts with providers to provide system development services for the entity's face comparison system.

4. The CPIC is guided by a CPIC Face Comparison Oversight Committee that ensures that P/CRCL are not violated by this face comparison policy, on top of the CPIC Privacy Policy, (See Appendix E for CPIC Privacy Policy) and by the CPIC's face comparison information collection, receipt, access, use, dissemination, retention, and purging processes and procedures.

The committee will annually review and update the face comparison policy in response to changes in law and program implementation experience, including the results of audits and inspections.

5. The CPIC Privacy Officer will:

- Receive reports regarding alleged errors and violations of the provisions of this face comparison policy or applicable state law.
- Receive and coordinate complaint resolution under the CPIC's face comparison redress policy.
- Ensure that the provisions of this policy and P/CRCL protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies.
- Ensuring that protocols are followed to ensure that face comparison information (including probe images) is automatically purged in accordance with the entity's retention policy (refer to section L.1. Information Retention and Purging), unless determined to be of evidentiary value.
- Ensuring that random evaluations of user compliance with system requirements and the entity's face comparison policy and applicable law are conducted and documented (refer to section M.2. Accountability).
- Confirming, through random audits, that face comparison information is purged in accordance with this policy and to ensure compliance with applicable laws, regulations, standards, and policy.

- Ensuring and documenting that personnel (including investigators from external agencies who may make face comparison search requests) meet all prerequisites stated in this policy prior to being authorized to use the face comparison system.

The CPIC Privacy Officer may be contacted at the following address: cpicpo@chicagopolice.org, which is also posted on cpic.chicagopolice.org.

6. The Face Comparison Oversight Committee will ensure that enforcement procedures and sanctions outlined in Section M.3. Enforcement are adequate and enforced.

D. Definitions

1. For examples of primary terms and definitions used in this face comparison policy, refer to Appendix A.

E. Acquiring and Receiving Face Comparison Information

1. The CPIC face comparison system can access and perform face comparison searches utilizing the following entity-owned face image repositories:

- Mug-shot images from Chicago Police Department I-CLEAR system
- Open-source data services

In addition to above, the CPIC is authorized to submit requests for face comparison searches to be performed by external governmental entities that own and maintain face image repositories.

2. For the purpose of performing face comparison searches, the CPIC and authorized CPIC personnel will obtain probe images or accept probe images from authorized requesting or participating agencies only for the authorized uses identified in section A.2.

3. The CPIC will receive probe images only from other law enforcement agencies in accordance with this policy.

4. The CPIC and, if applicable, any authorized requesting or participating agencies will not violate the U.S. Constitution or laws of the United States, including the First, Fourth, and Fourteenth Amendments and will not perform or request face comparison searches about individuals or organizations based solely on their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.

5. The CPIC will contract only with commercial face comparison companies or subcontractors that provide assurances that their methods for collecting, receiving, accessing, disseminating, retaining, and purging face comparison information comply with applicable local, state, tribal, territorial, and federal laws, statutes, regulations, and policies and that these methods are not based on unfair or deceptive information collection practices.

F. Use of Face Comparison Information

1. Access to or disclosure of face comparison search results will be provided only *to individuals within the entity or in other governmental agencies* who are authorized to have access or have

completed applicable training outlined in section N. Training, and only for valid law enforcement purposes (e.g., enforcement, reactive investigations), and to IT personnel charged with the responsibility for system administration and maintenance. Authorized uses are described in A.3 of this policy.

2. The CPIC will prohibit access to and use of the face comparison system, including dissemination of face comparison search results, for the following purposes:
- Non-law enforcement (including but not limited to personal purposes).
- Any purpose that violates the U.S. Constitution or laws of the United States, including the protections of the First, Fourth, and Fourteenth Amendments.
- Prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute.
- Harassing and/or intimidating any individual or group.
- Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.
- Any purpose that violates the City of Chicago's Welcoming City Ordinance, Municipal Code of Chicago Chapter 2-173 (See Appendix D for more information)

3. The CPIC does not connect the face comparison system to any interface that performs live video surveillance, including surveillance cameras, drone footage, and body-worn cameras. The face comparison system will not be configured to conduct face comparison analysis on live or recorded video.

4. The CPIC will employ credentialed, role-based access criteria, as appropriate, to control:
- Categories of face comparison information to which a particular group or class of users may have access, based on the group or class.
- The assignment of roles (e.g., administrator, manager, operator, and user).
- The categories of face comparison information that a class of users are permitted to access, including information being utilized in specific investigations.
- Any administrative or functional access required to maintain, control, administer, audit, or otherwise manage the information or equipment.

5. The following describes the CPIC's manual and automated face comparison search procedure, which is conducted in accordance with a valid law enforcement purpose and this policy.
- Authorized CPIC personnel and/or authorized requesting agency personnel will submit a probe image of a subject of interest.
- Trained CPIC authorized examiners will initially run probe images without filters, using a filtered search as a secondary search, if needed. In some cases, enhancements may be considered after running an image as is against the image repository.
- In the automated search, most likely candidates are returned to the requestor.
- The resulting candidates, if any, are then manually compared with the probe images and examined by an authorized, trained examiner. Examiners shall conduct the comparison of images, biometric identifiers, and biometric information in accordance with their training.
    - If no likely candidates are found, the requesting entity will be informed of the negative results. In the case of a negative result, the images examined by the examiner will not be provided to the requesting entity.
-
- All results of most likely candidate images from the face comparison search must be approved by a supervisor prior to dissemination.

- All entities receiving the results of a face comparison search must be cautioned that the resulting candidate images do not provide positive identification of any subject, are considered advisory in nature as an investigative lead only, and do not establish probable cause, without further investigation, to obtain an arrest warrant without further investigation.
- The following statement will accompany the released most likely candidate image(s) and any related records:

The result of a face comparison search is provided by the CPIC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

6. At no time is the use of force permitted to capture a subject's image.

G. Sharing and Disseminating Face Comparison Information

1. External law enforcement agencies who request face comparison searches will comply with CPIC policies with regards to Face Comparison searches. External agencies must comply with the laws and rules governing it, including applicable federal and state laws. Each request must be accompanied by a complaint number or case number and all requests must be for official use only/law enforcement sensitive (FOUO/LES).

2. The CPIC's face comparison search information will not be:
- Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by the CPIC's agreement with the commercial vendor.
- Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication. However, the CPIC and the originating agency may agree in writing in advance that the CPIC will disclose face comparison search information as part of its normal operations, including disclosure to an external auditor of the face comparison search information.
- Disclosed on a discretionary basis unless the originating agency has provided prior written approval or unless such disclosure is otherwise authorized by the MOU or agreement between the CPIC and the originating agency.
- Disclosed to unauthorized individuals or for unauthorized purposes.

3. The CPIC will not confirm the existence or nonexistence of face comparison information to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

H. Data Quality Assurance

1. Original probe images will not be altered, changed, or modified in order to protect the integrity of the image. Any enhancements made to a probe image will be made on a copy, saved as a separate image, and documented to indicate what enhancements were made, including the date and time of change.

2. CPIC examiners will analyze, review, and evaluate the quality and suitability of probe images, to include factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a probe image prior to performing a face comparison search.

3. The CPIC considers the results, if any, of a face comparison search to be advisory in nature as an investigative lead only. Face comparison search results are not considered positive identification of a subject and do not, on their own, establish probable cause, without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.

4. The Chicago Police Department's Bureau of Technology will make every reasonable effort to perform routine maintenance, upgrades and enhancements, testing, of the face comparison system to ensure proper performance.

5. The Commanding Officer of the CPIC, or designee, will ensure the following:
   - Designated, trained personnel shall assess the face comparison system on a regular basis to ensure performance and accuracy.
   - Malfunctions or deficiencies of the system will be reported to the Chicago Police Department's Deputy Chief of the Bureau of Technology Services as soon as possible and without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures.

6. The integrity of information depends on quality control and correction of recognized errors which is key to mitigating the potential risk of misidentification or inclusion of individuals in a possible identification. The CPIC will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face comparison information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The CPIC will correct the information or advise the process for obtaining correction of the information.

I. Disclosure Requests

1. Face comparison information will be disclosed, if appropriate, to the public in accordance with applicable Federal and state laws, including the Illinois Freedom of Information laws (See Appendix D for more information). A record will be kept of all requests and of what information is disclosed to an individual.

J. Redress

J.1 Complaints

1. If an individual has a complaint with regard to face comparison information that is exempt from disclosure, is held by the CPIC, and allegedly has resulted in demonstrable harm to the complainant, the CPIC Privacy Officer will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the entity's CPIC's Privacy Officer at the following address: cpicpo@chicagopolice.org which is also posted on cpic.chicagopolice.org. The CPIC Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law.

   If the face comparison information did not originate with the entity, the CPIC Privacy Officer will notify the originating agency within 30 days in writing or electronically and, upon request, assist such agency to correct any identified data/record deficiencies in the information or verify that the record is accurate.

All face comparison information held by the entity that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged or out-of-date information. If there is no resolution within 30 days, the entity will not share the information until such time as the complaint has been resolved. A record will be kept by the entity of all complaints and the resulting action taken in response to them.

J.2 Requests for Corrections

1. If, in accordance with state law, an individual requests correction of face comparison information *originating with the* CPIC that has been disclosed, the CPIC's Privacy Officer will inform the individual of the procedure for requesting a correction. The CPIC will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face comparison information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The CPIC will correct the information or advise the process for obtaining correction of the information. A record will be kept of all requests and the CPIC's response.

J.3 Appeals

1. The individual who has requested disclosure or to whom face comparison information has been disclosed will be informed of the reason(s) why the CPIC or originating agency denied the request for disclosure or correction. The individual will also be informed of the procedure for appeal when the CPIC or originating agency has cited an exemption for the type of information requested or has declined to correct challenged face comparison information to the satisfaction of the individual to whom the information relates.

K. Security and Maintenance

1. The entity will comply with generally accepted industry or other applicable standards for security, in accordance with Fair Information Practice Principles (FIPPS) (See Appendix B for more information) to protect data at rest, in motion, or in use. Security safeguards will cover any type of medium (printed or electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related CPIC activity.

   All results produced by the CPIC as a result of a face comparison search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee.

2. All individuals with access to CPIC's information or information systems will report a suspected or confirmed breach to both the Chicago Police Department's Deputy Chief of the Bureau of Technology Services and the CPIC Privacy Officer as soon as possible and without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, and electronic.

   Following assessment of the suspected or confirmed breach and as soon as practicable, the CPIC will notify the originating agency from which the entity received face comparison information of the nature and scope of a suspected or confirmed breach of such information.

The CPIC adheres to the Illinois Personal Information Protection Act (See Appendix D for more information). The CPIC will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

3. All face comparison equipment and face comparison software and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.

4. The CPIC will store face comparison information in a manner that ensures that it cannot be modified, accessed, or purged except by personnel authorized to take such actions.

5. Authorized access to the CPIC's face comparison system will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check and the training referenced in section N. Training.

6. Usernames and passwords to the face comparison system are not transferrable, must not be shared by CPIC personnel, and must be kept confidential.

7. The system administrator will ensure that all manufacturer-generated default passwords are replaced with secure passwords before web-based interfaces of the system become operational. User passwords must meet the following standards such as no English words and a combination of upper and lowercase letters, numbers, and at least one special character. Authorized users are not permitted to use the same password over time and are required to change their password semi-annually.

8. Queries made to the CPIC's face comparison system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.

9. The CPIC will maintain an audit trail of requested, accessed, searched, or disseminated CPIC-held face comparison information. An audit trail will be kept for a minimum of 12 months of requests, access, and searches of face comparison information for specific purposes and of what face comparison information is disseminated to each individual in response to the request.

Audit logs may include:

- The name, agency, and contact information of the law enforcement user
- The date and time of access
- Case number
- Probe images (refer to section L.5)
- The modification or deletion, if any, of the face comparison information
- The authorized law enforcement or public safety justification for access (criminal investigation, criminal intelligence, imminent threat, or identification), including a relevant case number

L. Information Retention and Purging

1. The CPIC maintains or operates a Chicago Police Department owned image repository

   All images are contained within the CPD's mug-shot repository located within the Chicago Police Department's ICLEAR system. No comparison photos are added to

this system during the face comparison process. Refer to section K. Security and Maintenance, item 9, regarding face comparison information stored in audit logs.

2. The CPIC has authorized access to and can perform face comparison searches utilizing image repositories not owned by the entity, but are available thru open-source.

   Images accessed by the CPIC for face comparison searches, in accordance with section E.1, are not maintained or owned by the CPIC and are subject to the policies of the entities who maintain those images.

3. The CPIC is authorized to request that face comparison searches be performed by an external governmental entities that operates a face comparison program.

   The CPIC is authorized to submit face comparison search requests, in accordance with section E.1, to external agencies that own and maintain face image repositories. The images searched are subject to the retention policies of the respective external governmental agencies that maintain or own the face image repositories.

Once a face comparison image is downloaded by CPIC personnel and incorporated into a criminal intelligence record or an investigative case file, the face comparison information is then considered criminal intelligence or investigative information and the laws, regulations, and policies applicable to that type of information or criminal intelligence govern its use.

Any images that do not originate with the CPIC will remain in the custody and control of the originating agency and will not otherwise be transferred to any other entity without authorization from the originating agency.

Probe images are not enrolled (stored) in the image repository. Retention of probe images will be the same as for the type of file (criminal case file, criminal intelligence file), whether paper or electronic, in which the information is stored.

A lawfully obtained probe image of an unknown suspect *may* be added to an unsolved image file pursuant to an authorized criminal investigation. Images in an unsolved image file are periodically compared with those in an image repository (of known persons). If a most likely candidate meets a minimum threshold of computer-evaluated similarity results, the contributor of the probe image is notified and requested to validate the continued need to store the image or determine whether the image can be purged. Images enrolled in an unsolved image file will be validated on a periodic basis, at least every 12 months, with the contributors to ensure that the criminal investigation remains active and that the image remains relevant to the investigation. If, in accordance with this policy, the contributor has not validated the need to retain the image in the unsolved file, the image will be purged.

The list of most likely candidate images is not enrolled (stored) in the image repository. For CPIC investigations, the case agent will maintain the list of most likely candidates from a face comparison search within the case file.

Probe images and face comparison search results are saved within the entity's system audit log, for audit purposes only. The audit log is available only to members of the Face Comparison Oversight Committee and will be purged within 12 months. The audit log is not searchable and face comparison searches cannot be performed using the audit log.

M. Accountability and Enforcement

M.1 Transparency

1. The CPIC will be open with the public with regard to face comparison information collection, receipt, access, use, dissemination, retention, and purging practices. The CPIC's face comparison policy will be made available in printed copy upon request and posted prominently on the CPIC's website or Chicago Police Department's website at cpic.chicagopolice.org.

2. The CPIC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about the entity's use of the face comparison system, as well as complaints regarding incorrect information or P/CRCL protections in the image repository maintained and face comparison system accessed by the CPIC. The CPIC Privacy Officer may be contacted at cpicpo@chicagopolice.org.

M.2 Accountability

1. The CPIC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with the face comparison system requirements and with the provisions of this policy and applicable law. This will include logging access to face comparison information, and will entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least annually, and a record of the audits will be maintained by the CPIC Privacy Officer of the CPIC pursuant to the retention policy. Audits may be completed by an independent third party or a designated representative of the Chicago Police Department.

   Appropriate elements of this audit process and key audit outcomes will be compiled into a report and may be provided to command staff and oversight entities or governance boards.[1]

2. The CPIC's personnel or other authorized users shall report errors, malfunctions, or deficiencies of face comparison information and suspected or confirmed violations of the CPIC's face comparison policy to the CPIC's Commanding Officer.

3. The CPIC Privacy Officer will review and update the provisions contained in this face comparison policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the face comparison system; the audit review; and public expectations.

M.3 Enforcement

1. If CPIC personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging, the Commanding Officer of the CPIC will:
   - Suspend or discontinue access to information by the CPIC entity personnel, the participating agency, or the authorized user.

[1] *Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component*, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component.

- Apply appropriate disciplinary or administrative actions or sanctions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. The CPIC reserves the right to establish the qualifications and number of personnel having access to the CPIC's face comparison system and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this face comparison policy.

N. Training

1. Before access to the CPIC's face comparison system is authorized, the CPIC will require the following individuals to participate in training regarding implementation of and adherence to this face comparison policy:
- All authorized CPIC personnel, including examiners
- All authorized personnel providing information technology services to the CPIC

2. The CPIC's face comparison policy training program will cover both:

a. Elements of the operation of the face comparison program, including:
- Purpose and provisions of the face comparison policy.
- Substance and intent of the provisions of this face comparison policy and any revisions thereto relating to collection, receipt, access, use, dissemination, retention, and purging of the CPIC's face comparison information.
- Policies and procedures that mitigate the risk of profiling.
- How to implement the face comparison policy in the day-to-day work of the user, whether a paper or systems user.
- Security awareness training.
- How to identify, report, and respond to a suspected or confirmed breach.
- Implicit Bias training.

b. Elements related to the results generated by the face comparison system, including:
- Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.
- The P/CRCL protections on the use of the technology and the information collected or received, including constitutional protections, and applicable state, local, and federal laws.
- Face comparison system functions, limitations, and interpretation of results.
- Mechanisms for reporting violations of CPIC face comparison policy provisions.
- The nature and possible penalties for face comparison policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

3. Investigators from outside agencies are permitted to request face comparison searches from the CPIC only if prior to making requests:

The outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in section A. Purpose Statement, item 3. And the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number), and acknowledges an agreement with the following statement:

The result of a face comparison search is provided by the CPIC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVEI IDENTIFICATION OF ANY SUBJECT. Any

possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

Appendix A—Glossary of Terms and Definitions

The following is a list of terms and definitions used within the policy or provided for the purpose of enhancing the reader's understanding of the topics discussed.

Access—Information access is being able to get to particular information on a computer (usually requiring permission to use). Web access means having a connection to the internet through an access provider or an online service provider.

Access Control—The mechanisms for limiting access to certain information, based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role- or user-based.

Acquisition—The means by which an entity obtains face comparison information through the exercise of its authorities.

Agency—See Participating Agency.

Algorithm—An algorithm is a procedure or formula for solving a problem, based on conducting a sequence of specified actions. A computer program can be viewed as an elaborate algorithm. Algorithms can perform calculation, data processing, and automated reasoning tasks and are widely used throughout all areas of information technology.

Analysis—Refer to Image Analysis.

Attributes—Physical characteristics, such as gender, race, age, hair color, etc. that can be applied to a face comparison search.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail, such as what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security and used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication—The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provides a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

Authorization—The process of granting a person, a computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, a computer process, or a device requesting access that is verified through authentication. See Authentication.

Automated Face Comparison (AFC)—Automated face comparison (AFC) software compares patterns within the field of computer vision. Such approaches do not rely upon intrinsic models of what a face is, how it should appear, or what it may represent. In other words, the matching is not based on biological or anatomical models of what a face–or the features that make up a face—look like. Instead, the algorithm performance is entirely dependent upon the patterns which the algorithm developer finds to be most useful for finding similarities. The patterns used in AFR algorithms do not correlate to obvious anatomical features such as the eyes, nose or mouth in a one-to-one manner, although they are affected by these features.

Biometric Template—A biometric template is a set of biometric measurement data [or features] prepared by

a face comparison system from a face image.[2] The prepared set can be compared to a probe image. An enrolled image, on its own, is not a biometric template. See Features.

Biometrics—A general term used alternatively to describe (1) a characteristic or (2) a process—(1) a measureable biological (anatomical and physiological) and behavioral characteristic that can be used for automated comparison or (2) automated methods of recognizing an individual based on measureable biological (anatomical and physiological) and behavioral characteristics.[3]

Candidates—See Candidate Images.

Candidate Images—The possible results of a face comparison search. When face comparison software compares a probe image against the images contained in a repository (See Repository.), the result is a list of most likely candidate images that were determined by the software to be sufficiently similar to or most likely resemble the probe image to warrant further analysis. A candidate image is an investigative lead only and does not establish probable cause to obtain an arrest warrant without further investigation.

Candidate List—One or more most likely candidate images resulting from a face comparison search. See Candidate Images.

Center—See Fusion Center.

Civil Liberties—According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term "civil liberties" refers to fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals.[4] They are the freedoms that are guaranteed by the Bill of Rights—the first 10 amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Civil Rights—The term "civil rights" refers to those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights means that government entities will take action to ensure that individuals are not discriminated against on the basis of any federal- or state- protected characteristic. For example, a state may have constitutional or statutory language regarding parental status. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.[5]

Collect—For purposes of this document, "gather" and "collect" mean the same thing.

Comparison—The observation of two or more faces to determine the existence of discrepancies, dissimilarities, or similarities.[6] See Face Comparison.

Computer Security—The protection of information technology assets through the use of technology, processes, and training.

Confidentiality—Refers to the obligations of individuals and institutions to appropriately use information and data under their control once they have been disclosed to them and in accordance with applicable data security laws and policies. See Privacy.

Consent—In general use, consent means compliance in or approval of what is done or proposed by another; specifically, the voluntary agreement or acquiescence by a person of age or with requisite mental capacity who is not under duress or coercion and usually who has knowledge or understanding. Related to mobile

[2] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.
[3] Ibid.
[4] *Civil Rights and Civil Liberties Protections Guidance*, at 4 (August 2008), https://www.dni.gov/files/ISE/documents/DocumentLibrary/Privacy/CR-CL_Guidance_08112008.pdf.
[5] The definition of "civil rights" is a modified version of the definition contained in the *National Criminal Intelligence Sharing Plan* (NCISP), at pp. 5–6. *Civil Rights and Civil Liberties Protections Guidance* (August 2008), https://www.dni.gov/files/ISE/documents/DocumentLibrary/Privacy/CR-CL_Guidance_08112008.pdf.
[6] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

face comparison, consent means an individual agrees to have his or her image taken by a law enforcement officer for purposes of identification. See Revocation.

Continuous Monitoring—A system security process that comprises ongoing situational awareness of information security, vulnerabilities, threats, and incidents for each user level to support entity risk management decisions.

Credentials—Information that includes identification and proof of identification that are used to gain access to local and network resources. Examples of credentials are usernames, passwords, smart cards, and certificates.

Criminal Activity—A behavior, an action, or an omission that is punishable by criminal law.

Criminal Case Support—Administrative or analytic activities that provide relevant information to law enforcement personnel regarding the investigation of specific criminal activities or trends or specific subject(s) of criminal investigations.

Criminal Intelligence Information—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

Data—Inert symbols, signs, descriptions, or measures; elements of information.

Data Breach—The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information (PII) or (2) an authorized user accesses or potentially accesses PII for a purpose other than authorized purposes. An entity's response to a data breach may be addressed in state law or agency policy. This may include incidents such as:

- Theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted.
- Posting such information on the internet.
- Unauthorized employee access to certain information.
- Moving information to a computer otherwise accessible from the internet without proper information security precautions.
- Intentional or unintentional transfer of information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail.
- Transfer of information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

Data Quality—Refers to various aspects of the information, such as the accuracy and validity of the actual values of the data, information structure, and database/information repository design. Traditionally, the basic elements of data quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, data quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy. This concept is also addressed as one of the Fair Information Practice Principles (FIPPs), Data Quality/Integrity. See Appendix B for a full set of FIPPs.

Direct Face Comparison Collection—The entity is owner of the face comparison equipment that captures face comparison information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of PII in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Dissemination—See Disclosure.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, compact disc optical media, or cloud technologies.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as movement of information from one location to another by magnetic or optical media, or transmission over the internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Enhancement—Image enhancement is the process of adjusting digital images so that the results are more suitable for display or further image analysis. For example, removing noise, sharpening or brightening an image may make it easier to identify key features.

Enroll—The process of storing and maintaining information. Specifically in the face comparison context, biometric enrollment is capturing a face image, creating a biometric template from the image, and entering the template into a face comparison repository.[7] See Biometric Template and Repository.

Enrolled Image—An image that is loaded to, and may be stored in, an image repository (see Repository) and used as a reference image for face comparison comparisons (searches). Enrolled images do not include probe images. Some images of individuals may not be enrolled because they do not meet established criteria.

Enrollment—See Enroll.

Entity—The **CPIC,** which is the subject and owner of the face comparison policy.

Evaluation—Refer to Image Evaluation.

Examiner—An individual who has received advanced training in the face comparison system and its features. Examiners have at least a working knowledge of the limitations of face comparison and the ability to use image editing software. They are qualified to assess image quality and appropriateness for face comparison searches and to perform one-to-many and one-to-one face image comparisons.

Examiners determine if probe images are suitable for face comparison searches, and may enhance images for the purpose of conducting a face comparison search. Though enhancements to the probe image are permissible, the examiner does not base any conclusions on a comparison between an enhanced probe image and a potential candidate photo. Examiners shall evaluate search results by comparing the original unknown probe image with the potential candidate photo.

Expression—Face aspects resulting from muscle movement or position.[8]

Face Comparison—The manual examination of the differences and similarities between two face images or a live subject and a face image (one-to-one) for the purpose of determining if they represent the same or different persons.[9] See Face Comparison, One-to-One Face Image Comparison, and Verification.

Face Detection—Automated determination of the locations and sizes of human faces in digital images.[10]

Face Examiner—See Examiner.

Face Comparison—The automated searching for a reference image in an image repository (see Repository) by comparing the face features of a probe image with the features of images contained in an image repository (one-to-many search). A face comparison search will typically result in one or more most likely candidates—or candidate images—ranked by computer-evaluated similarity or will return a negative result. See Candidate Images.

Face Comparison Program—An entity's face comparison initiative that includes the management of human components (management, analysts, examiners, authorized users), ownership and management of the face comparison system (technical components), and the establishment and enforcement of entity-wide processes, policies, and procedures. See Face Comparison System.

Face Comparison Software/Technology—Third-party software that uses specific proprietary algorithms to compare face features from one specific picture—a probe image—to many others (one-to-many) that are stored in an image repository (see Repository) to determine most likely candidates for further investigation. See Candidate Images.

Face Comparison System—The technical components of a face comparison program, such as hardware, software, interfaces, image repositories,

[7] Ibid.
[8] Ibid.
[9] Ibid.
[10] Ibid.

biometric templates, autogenerated candidate lists, etc. While some entities own such a system, others may only have authorized access to another entity's face comparison system. See Face Comparison Program.

Face Comparison—See Face Comparison.

Fair Information Practice Principles—The Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies both within government and the private sector. Although specific articulations of FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into information privacy laws, policies, and governance documents around the world. They provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal use that needs to be done with regard to privacy in integrated justice systems. Because of operational necessity, it may not always be possible to apply all of the principles equally. For example, the Individual Participation Principle (#8) may be of limited applicability in intelligence operations, as entities do not generally engage with individuals and under federal law, the Privacy Act of 1974 contains exemptions in the law enforcement context. That said, law enforcement entities and all other integrated justice systems should endeavor to apply FIPPs where practicable and ensure compliance with applicable law.

The eight principles are:
1. Purpose Specification
2. Data Quality/Integrity (See definition.)
3. Collection Limitation/Data Minimization
4. Use Limitation
5. Security Safeguards (See definition.)
6. Accountability/Audit
7. Openness/Transparency
8. Individual Participation

See Appendix B for one description of how the U.S. Department of Homeland Security applies these principles.

Features—Observable class or individual characteristics. The components of biometric templates. [11]

Filtering—In the face comparison context, filtering uses relevant physical face attributes such as eye color, nose shape, eyebrow position, hairline, and other attributes to compare, select, and narrow results. See Attributes.

Firewall—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

Frontal Pose—A face image captured from directly in front of the subject with the focal plane approximately parallel to the plane of the subject's face.[12]

Fusion Center—A fusion center is a collaborative effort of two or more federal, state, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity.[13] State and major urban area fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between federal and SLTT government agencies and private-sector partners.

Holistic Comparison—The process of comparing faces by looking at the face as a whole and not the component parts in isolation.[14]

Identity—Within a biometric system, the collective set of biographic data, images, and biometric templates assigned to one person.[15] See Face Comparison.

Image—See Probe Image and Repository.

Image Analysis—The assessment of an image to determine suitability for comparison, including the ability to discriminate significant features.[16]

Image Enhancement—See Enhancement.

[11] Ibid.
[12] Ibid.
[13] ISE-SAR Functional Standard, version 1.5.5. Source: Section 511 of the 9/11 Commission Act.
[14] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.
[15] Ibid.
[16] Ibid.

Image Evaluation—Ascertaining the value of dissimilarities and similarities between two face images, where an examiner assesses the value of the details observed during the analysis and comparison steps and reaches a conclusion.[17]

Image Repository—See Repository.

Individual Characteristics—Characteristics allowing one to differentiate between individuals having the same class of characteristics (e.g., freckles, moles, and scars).[18]

Individual Responsibility—Because a privacy notice is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the notice.

Individualization—The determination by an examiner that there is sufficient agreement in the quality and quantity of detail to conclude that two images depict the same person.[19] Such results are generally referred for peer and supervisory reviews and approval before any dissemination of results is made.

Information—Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into three general areas: general data, including investigative information; tips and leads data, including suspicious activity reports; and criminal intelligence information.

Information Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

Information Quality (IQ)—Refer to Data Quality.

Information Sharing Environment (ISE)—In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the Information Sharing Environment (ISE) is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of SLTT agencies, federal agencies, and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

Intelligence—See Criminal Intelligence Information.

Invasion of Privacy— Intrusion on an individual's solitude or into an individual's private affairs, public disclosure of embarrassing private information, publicity that puts an individual in a false light to the public, or appropriation of an individual's name or picture for personal or commercial advantage. See also Right to Privacy.

Investigative Lead—Any information which could potentially aid in the successful resolution of an investigation, but does not imply positive identification of a subject or that the subject is guilty of a criminal act.

Known Image—The image of an individual associated with a known or claimed identity and recorded electronically or by other medium (also known as exemplars).[20] Known images are enrolled and stored in an image repository. See Repository.

Law—As used by this policy, law includes any local, state, or federal constitution, statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement (LE) Agency—An organizational unit, or subunit, of a local, state, federal, or tribal government with the principal functions of prevention, detection, and investigation of crime, apprehension of alleged offenders, and enforcement of laws. LE agencies further investigations of criminal behavior based on prior identification of specific criminal activity with a statutory ability to perform arrest functions.

Law Enforcement Information—For purposes of the ISE (see Information Sharing Environment), law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including, but not limited to, information pertaining to an actual or potential criminal, civil, or administrative investigation or a

[17] Ibid.
[18] Ibid.
[19] Ibid.
[20] Ibid.

foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident—A foreign national who has been granted the privilege of permanently living and working in the United States.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

Logs—A necessary part of an adequate security system which ensures that information is properly tracked and that only authorized individuals are getting access to the data. See also Audit Trail.

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases or repositories) and nonelectronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Manual Face Examination—Comparison and evaluations of the probe image and the candidate images by a trained biometric images specialist.

Match/Matching—For the purposes of face comparison, see Candidate Images.

Morphological Comparison—The direct comparison of class and individual face characteristics without explicit measurement.[21] See Comparison and Manual Face Examination.

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information to perform or assist in a law enforcement, homeland security, or counterterrorism activity or other lawful and authorized government activity, such as to further an investigation or meet another law enforcement requirement.

Nodal Points—Measurements of distinctive face characteristics, including, but not limited to, the distance between the eyes, width of the nose, and the depth of the eye sockets. Nodal points are extracted from the face image and are transformed through the use of algorithms into a unique file called a biometric template. See Biometric Template.

No Match—A negative result from a face comparison search in which the probe image was determined not to be sufficiently similar to or resemble any of the reference images contained in an image repository.

Non-Criminal Justice Agency—An entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

One-to-Many Face Image Comparison—The process whereby a probe image from one subject is compared with the features of reference images contained in an image repository, generally resulting in a list of most likely candidate images (one-to-many). See Candidate Images.

One-to-One Face Image Comparison—The process whereby a probe image from one subject is compared with a most likely candidate image that is also from one subject (one-to-one). See Comparison, Face Comparison, and Verification.

Participating Agency—An organizational entity that is authorized to contribute images and/or biometric information to a face comparison system and/or is authorized to access or receive, request, or use face comparison information from the **CPIC**'s face

[21] Ibid.

comparison system for lawful purposes through its authorized individual users.

Peer Review—An additional layer of verification of face comparison results in a face comparison search process. Examiners submit face comparison search results to other authorized and trained examiners—or peers—for an independent review and cross-verification of the probe and most likely candidate images. If verified by peer(s), this step is generally followed by a supervisor's review and approval prior to dissemination. Refer to Verification.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, a directory, or a printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personally Identifiable Information (PII)—
Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information, that is linked or linkable to a specific individual." [22]

Pose—The orientation of the face with respect to the camera, consisting of pitch, roll, and yaw. Common poses are frontal and profile.[23]

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of PII. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); and to avoid being seen or overheard in particular contexts.

Privacy Policy—Short term for a privacy, civil rights, and civil liberties (P/CRCL) policy which is a printed, published statement that articulates the policy position of an organization on how it handles the PII that it gathers or receives and uses in the normal course of business. The policy should include information relating to the processes of information collection, receipt, access, use, dissemination, retention, and purging. It is likely to be informed by the FIPPs. The purpose of the P/CRCL policy is to articulate that the entity will adhere to those legal requirements and entity policy determinations that enable collection, receipt, access, use, dissemination, retention, and purging of information to occur in a manner that protects personal privacy interests. A well-developed P/CRCL policy uses justice entity resources wisely and effectively; protects the entity, the individual, and the public; and promotes public trust.

Probe Image—Any face image used by face comparison software for comparison with the face images contained within a face image repository. See Repository.

A front-facing image of an individual lawfully obtained pursuant to an authorized criminal investigation. Examples of probe images include:

- Face images captured from closed circuit TV cameras
- Face images captured from an ATM camera
- Face images provided by a victim or witness of a crime
- Face images gained from evidence (fraudulent bank card or photograph ID)
- Face sketches (for example, police artist drawings)

Protected Information—For the nonintelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States.

For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, policy, or other similar instrument.

For state, local, tribal, and territorial governments, protected information may include information about individuals and organizations that is subject to

[22] For further information about the breadth of PII and how to perform an assessment of the specific risk that an individual can be identified using the information, see Revision of Office of Management and Budget Circular A-130: Managing Information as a Strategic Resource, July 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf.

[23] Ibid.

information privacy or other legal protections by law, including the U.S. Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, tribal, and territorial laws, ordinances, and codes. Protection may be extended to other individuals and organizations by a law enforcement entity or other state, local, tribal, or territorial agency policy or regulation.

Public—Includes:

- Any individual and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the entity's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit and without distinction as to the nature or intent of those requesting information from the entity or participating entity.

Public does not include:

- Any employees of the entity or participating entity.
- People or entities, private or governmental, who assist the entity in the operation of the justice information system.
- Public entities whose authority to access information collected or received and retained by the entity is specified in law.

Public Access—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

Purge—A term that is commonly used to describe methods that render data unrecoverable in a storage space or destroy data in a manner that it cannot be reconstituted. There are many different strategies and techniques for data purging, which is often contrasted with data deletion (e.g., made inaccessible except to system administrators or other privileged users).

Recognition—See Face Comparison.

Record—Any item, collection, or grouping of information that includes PII and is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting agency or organization.

Redress—Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding *protected information* about them which is under the entity's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

Protected information includes personal information about individuals that is subject to information privacy or other legal protections by law. Protection may also be extended to organizations by entity policy or state, local, tribal, or territorial law.

Relative Frequency—How often face features or combinations thereof occur in a given population.[24]

Repository—A location where a group of images of known individuals and biometric templates are stored and managed. An image repository is searched during a face comparison search process whereby a probe image is used by face comparison software for comparison with the images (or features within images) contained in the image repository.

Request—A request received by the **CPIC** to utilize face comparison in support of a criminal investigation. Submissions will not contain original evidence. Images received in a request or submission will not be stored as enrolled images within the face comparison system.

Retention—See Storage.

Revocation—In general use, revocation is the act of recall or annulment. It is the reversal of an act, the recalling of a grant or privilege, or the making void of some deed previously existing. As it relates to the revocation of consent to be photographed or the individual's image captured by a law enforcement officer to perform a mobile face comparison search for purposes of identification, once consent to capture an individual's image is given, an individual may withdraw consent with an unequivocal act or statement of withdrawal. Consent may be withdrawn by

[24] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

statements, actions, or a combination of statements and actions. However, the revocation of consent must clearly be a statement revoking consent; an expression of impatience or dislike is not sufficient to terminate consent.

Revoke—See Revocation.

Right to Information Privacy—The right to be left alone, in the absence of some reasonable public interest in collecting, accessing, retaining, and disseminating information about an individual's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the individual or entity violating an individual's privacy.

Right to Know—A requirement for access to specific information to perform or assist in a lawful and authorized government function. Right to know is determined by the mission and functions of a law enforcement, homeland security, counterterrorism, or other lawful and authorized government activity, or the roles and responsibilities of particular personnel in the course of their official duties.

Role-Based Access—A type of access authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

Search—For the purposes of face comparison, the act of comparing a probe image against an image repository.[25] See Repository.

Search Filters—See Filtering.

Search Result Set—The candidate list returned from a face comparison search.[26] See Candidate Images.

Security—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of information for the legitimate user set, as well as promoting failure resistance in the electronic systems overall. Security safeguarding of information is a Fair Information Practice Principle (FIPP). See Appendix B.

Source Entity—Refers to the entity or organizational entity that originates face comparison information.

Storage—In a computer, storage is the place where data is held in electromagnetic or optical form for access by a computer processor. There are two general usages:

- Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This is probably the most common meaning in the IT industry.
- In more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called "random access memory," or RAM) and other built-in devices, such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations. Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

Submission—See Request.

System Bias—Errors repeatedly introduced through automation (e.g., errors in biometric template generation or comparison). Errors repeatedly introduced through operational practices in an organization or unit (e.g., improper lighting or camera position guidance).[27]

Template—See Biometric Template.

Uncontrolled Image—An image for which the subject did not pose (e.g., security camera images, cell phone photograph taken by a witness).

Unsolved Image File—A lawfully obtained probe image of an unknown suspect *may* be added by authorized law enforcement users to an unsolved image file pursuant to an authorized criminal investigation and if a search has produced no

[25] Ibid.
[26] Ibid.
[27] Ibid.

candidates and the subject remains unknown. Images in an unsolved image file are periodically compared with the known images in an image repository. Images enrolled in an unsolved image file should be required to be validated periodically by the contributors to ensure that the criminal investigation remains active and that the image remains relevant to the investigation.

User—An **CPIC** employee or an individual representing a participating agency who is authorized and trained to access and use, or receive results from, an entity's face comparison system for lawful purposes.

Valid Law Enforcement Purpose—A purpose for information/intelligence gathering, development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, protection of public or private structures and property, furthering officer safety (including situational awareness), and homeland and national security, while adhering to law and agency policy designed to protect the P/CRCL of Americans.[28] Similar terms include "reasonable law enforcement purpose,"[29] "legitimate law enforcement purpose," and "authorized law enforcement activity."[30]

Verification—In a biometric system, the process of conducting a one-to-one comparison. A task where the face comparison system attempts to confirm an individual's claimed identity by comparing the biometric template generated from a submitted face image with a specific known template generated from a previously enrolled face image.

A review and independent analysis of the conclusion of another examiner.[31]

[28] See *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*, Global, BJA, OJP, DOJ, February 2013, https://it.ojp.gov/GIST/132/Developing-a-Policy-on-the-Use-of-Social-Media-in-Intelligence-and-Investigative-Activities--Guidance-and-Recommendations- and also in the *Real-Time and Open Source Analysis (ROSA) Resource Guide*, Criminal Intelligence Coordinating Council (CICC), Global, BJA, OJP, DOJ, July 2017, https://it.ojp.gov/GIST/1200/Real-Time-and-Open-Source-Analysis--ROSA--Resource-Guide (using "valid law enforcement purpose").

[29] *Recommendations for First Amendment-Protected Events for State and Local Law enforcement Agencies*, CICC, Global, OJP, DOJ, and DHS, December 2011, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.

[30] The term "authorized law enforcement activity" is used, for example, in *The Attorney General's Guidelines For Domestic FBI Operations*, as provided in sections 509, 510, 533, and 534 of title 28, United States Code, and Executive Order 12333, September 29, 2008.

[31] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

Appendix B—Fair Information Practice Principles (FIPPs)

The Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies within both government and the private sector.

Although specific articulations of FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into data privacy laws, policies, and governance documents around the world. For example, FIPPs are:

- At the core of the Privacy Act of 1974, which applies these principles to U.S. federal agencies.[32]
- Internationally influential, especially as articulated by the Organisation for Economic Co-operation and Development.
- Mirrored in many states' laws and in law enforcement entities' and fusion centers' privacy policies.
- Used by numerous foreign countries and international organizations.

The following formulation of FIPPs is used and implemented for the Information Sharing Environment (ISE) by the U.S. Department of Homeland Security (DHS).[33] For a definition of the Information Sharing Environment, refer to Appendix A, Glossary of Terms and Definitions. Note, however, that under certain circumstances, FIPPs may be superseded by authorities paralleling those provided in the federal Privacy Act; state, local, tribal, or territorial law; or entity policy.

1. **Purpose Specification—**Agencies should specifically articulate the authority that permits the collection of personally identifiable information (PII). The purpose(s) for which PII is collected should be specified at the time of data collection. Subsequent use of this data should be limited to the original purpose for which the PII was collected (or other purposes *compatible* with the original collection purpose).

   Implementing the Purpose Specification Principle—Agencies are bound by specific constitutional and statutory authorities that circumscribe their ability to collect PII. The following are examples of ways agencies may implement this principle:

   - Ensure that a valid lawful purpose exists and is documented for all collection of PII.
   - Include the source and authority for the data so that access restrictions can be applied.
   - Upon receipt of data containing PII from third parties, if possible, identify the purpose for which it was collected initially and limit agency use to only those uses compatible with the original purpose supporting collection.
   - Ensure that metadata or other tags are associated with the data as it is shared.

[32] 5 U.S.C. § 552a.
[33] 6 U.S.C. § 142.

- Institute a two-individual review and approval process to consider any Privacy Act or other legal or policy limitation before permitting use or sharing of data for purposes other than that for which it was collected.

2. **Data Quality/Integrity—**PII collected should be relevant to the purposes identified for its use and should be accurate, complete, and up to date.

   Implementing the Data Quality/Integrity Principle—One important way to minimize potential downstream privacy and civil liberties concerns is to ensure that any information collected, stored, and disseminated is accurate. This includes ensuring that the information provides sufficient context for any PII. Possible approaches include:
   - Properly labeling PII.
   - Determining a policy for safeguarding PII if there are "mixed" databases (i.e., those databases with personal information on U.S. individuals and others, regardless of nationality).
   - Instituting a source verification procedure to ensure that reporting is based only on authorized data.
   - Reconciling and updating PII whenever new relevant information is collected.
   - Developing a protocol for ensuring that data corrections are passed to those entities with which information has been shared.
   - Creating a documented process for identifying and addressing situations in which data has been erroneously received, is inaccurate, or has been expunged.

3. **Collection Limitation/Data Minimization—**PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose. PII should be obtained by lawful and fair means and retained only as long as is necessary to fulfill the specified purpose.

   Implementing the Collection Limitation/Data Minimization Principle—Collection limitation may be implemented by:
   - Designing a data storage system to pull data for review and then, if appropriate, automatically purging data after the specified retention period has been reached.
   - Limiting data field elements to only those that are relevant.
   - Ensuring that all distributed reports and products contain only that personal information that is relevant and necessary (nothing extraneous or superfluous).
   - Ensuring that all shared information with PII meets the required thresholds for sharing, such as reasonable suspicion.

4. **Use Limitation—**PII should not be disclosed, made available, or otherwise used for purposes other than those specified except (a) with the consent of the individual or (b) by authority of the law.

   Implementing the Use Limitation Principle—Sharing information should be tempered by adherence to key principles, such as "authorized access." Use limitation may be implemented by:
   - Limiting users of data to those with credential-based access.
   - Requiring that justifications be entered and logs maintained for all queries with sensitive PII and that an internal review process of those logs takes place at specified intervals.
   - Requiring senior analysts to review all reports that use PII before dissemination to ensure (a) that PII is relevant and necessary and (b) that the recipient is authorized to receive the information in the performance of an authorized activity.
   - Prior to sharing information, verify that partners have a lawful purpose for requesting information.
   - Creating multiple use-based distribution lists and restricting distribution to those authorized to receive the information.

5. **Security/Safeguards—**Agencies should institute reasonable security safeguards to protect PII against loss, unauthorized access, destruction, misuse, modification, or disclosure.

   Implementing the Security/Safeguards Principle—This principle can be implemented by:
   - Maintaining up-to-date technology for network security.
   - Ensuring that access to data systems requires that users meet certain training and/or vetting standards and that such access is documented and auditable.
   - Ensuring that physical security measures are in place, such as requiring an identification card, credentials, and/or passcode for data access; disabling computers' USB ports; and implementing firewalls to prevent access to commercial e-mail or messaging services.

- Implementing a protocol with technical and manual safeguards to ensure the accuracy and completeness of data system purges when records are deleted at the end of their retention period.
- Ensuring that data system purge protocols include complete record deletion on all backup systems.
- Transitioning older repositories into more modern systems to improve access controls.
- Masking data so that it is viewable only to authorized users.
- Maintaining an audit log to record when information is accessed and by whom for review by senior staff at specified intervals.
- Requiring authorized users to sign nondisclosure agreements.

6. **Accountability/Audit—**Agency personnel and contractors are accountable for complying with measures implementing FIPPs, for providing training to all employees and contractors who use PII, and for auditing the actual use and storage of PII.

   Implementing the Accountability/Audit Principle—Strong policies must not only be in place but also be effectively implemented. Accountability can be demonstrated by:

   - Ensuring that upon entry for duty, all staff members take an oath to adhere to the privacy and civil liberties protections articulated in the entity's or host agency's mission, core values statements, other key documents, and/or the U.S. Constitution.
   - Conducting effective orientation and periodic refresher training, including privacy, civil rights, and civil liberties (P/CRCL) protections, for all individuals handling PII.
   - Tailoring training to specific job functions, database access, or data source/storage requirements.
   - Conducting regular audits of all systems in which records are kept to ensure compliance with P/CRCL policies and all legal requirements.
   - Following a privacy incident, establishing a handling procedure for any data breaches or policy violations.
   - Denying database access to individuals until they have completed mandatory systems access training (including training for handling of PII), show a mission need for access, and have any necessary clearances.
   - Developing targeted and consistent corrective actions whenever noncompliance is found.

7. **Openness/Transparency—**To the extent feasible, agencies should be open about developments, practices, and policies with respect to the collection, use, dissemination, and maintenance of PII. Agencies should publish information about policies in this area, including the P/CRCL policy, and contact information for data corrections and complaints.

   Implementing the Openness/Transparency Principle—Agencies can implement the Openness/Transparency principle by:

   - Providing reports to an internal or external oversight body concerned with P/CRCL issues, including P/CRCL audit results.
   - Publishing the P/CRCL policy and redress procedures.
   - Meeting with community groups through initiatives or other opportunities to explain the agency's mission and P/CRCL protections.
   - Responding in the fullest way possible to freedom of information and/or sunshine requests and fully explaining any denial of information requests from the public.
   - Conducting and publishing Privacy Impact Assessments and Privacy Impact Analysis in advance of implementing any new technologies that affect PII, thereby demonstrating that P/CRCL issues have been considered and addressed.

8. **Individual Participation—**To the extent practicable, involve the individual in the process of using PII and seek individual consent for the collection, use, dissemination, and maintenance of PII. Agencies should also provide mechanisms for appropriate access, correction, and redress regarding the agency's use of PII.

   Implementing the Individual Participation Principle—To the extent appropriate, agencies can implement the Individual Participation principle by:

   - Collecting information directly from the individual, to the extent possible and practical.
   - Providing the individual with the ability to find out whether an agency maintains a record relating to him or her and, if not (i.e., access and/or correction is denied), then providing the individual with notice as to why the denial was made and how to challenge such a denial.

- Putting in place a mechanism by which an individual is able to prevent information about him or her that was obtained for one purpose from being used for other purposes without his or her knowledge.

(This Page Intentionally Left Blank)

Appendix C—Listing of Federal Laws

The U.S. Constitution is known as the primary authority that applies to federal as well as state, local, tribal, and territorial (SLTT) entities. State constitutions cannot provide a lower level of privacy and other civil liberties protection than that established by the U.S. Constitution, but states may broaden constitutional rights guaranteed by their own constitutions.

Civil liberties protections are primarily founded in the Bill of Rights. They include the basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc. Statutory civil rights protections in the U.S. Constitution may, in addition, directly govern state action. These include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act of 1990; Title VIII of the Civil Rights Act of 1968 (Fair Housing Act); the Voting Rights Act of 1965; and the Civil Rights of Institutionalized Individuals Act.

While in general, SLTT entities may not be bound directly by most statutory federal privacy and other civil liberties protection laws in the face comparison information collection sharing context, compliance may be required **indirectly** by funding conditions (e.g., Title VI of the Civil Rights Act of 1964), operation of the Commerce Clause of the U.S. Constitution, or a binding agreement between a federal agency and an SLTT entity (e.g., a memorandum of agreement or a memorandum of understanding).

The following are synopses of primary federal laws that an entity should review and, where appropriate, consider citing in a face comparison policy to protect face comparison data and any personally identifiable information later associated with the face comparison information. As face comparison information may be incorporated as one piece of information into a larger case file, the following federal laws may be applicable. The list is arranged in alphabetical order by popular name.

1. **Applicants and Recipients of Immigration Relief Under the Violence Against Women Act of 1994 (VAWA), Public Law 103-322, September 13, 1994, and the Victims of Trafficking and Violence Prevention Act of 2000 (T and U nonimmigrant status for victims of trafficking and other serious crimes), Public Law 106-386, Oct. 28, 2000, 8 U.S.C. § 1367, Penalties for Disclosure of Information—**The governing statute prohibits the unauthorized disclosure of information about VAWA, T, and U cases to anyone other than an officer or employee of the U.S. Department of Homeland Security, the U.S. Department of Justice, the U.S. Department of State, or parties covered by exception when there is a need to know. This confidentiality provision is commonly referred to as "Section 384" because it originally became law under Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) of 1996, which protects the confidentiality of victims of domestic violence, trafficking, and other crimes who have filed for or have been granted immigration relief. 8 U.S.C. § 1367 Information is defined as any information relating to aliens who are seeking or have been approved for nonimmigrant or immigrant status as (1) battered spouses, children, or parents under provisions of VAWA; (2) victims of a severe form of human trafficking who generally are cooperating with law enforcement authorities (T nonimmigrant status); or (3) aliens who have suffered substantial physical

or mental abuse as the result of qualifying criminal activity and have been, are being, or are likely to be helpful in the investigation or prosecution of that activity (U nonimmigrant status). This includes information pertaining to qualifying family members who receive derivative T, U, or VAWA status. Because 8 U.S.C. § 1367 applies to any information about a protected individual, this includes records or other information that do not specifically identify the individual as an applicant for or a beneficiary of T nonimmigrant status, U nonimmigrant status, or relief under VAWA.

2. **Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23**—This is a guideline for law enforcement agencies that operate federally funded multijurisdictional criminal intelligence systems. The operating principles of 28 CFR Part 23 provide guidance to law enforcement regarding how to operate criminal intelligence information systems effectively while safeguarding privacy, civil rights, and civil liberties (P/CRCL) during the collection, storage, and dissemination of criminal intelligence information. The regulation governs the intelligence information systems' process, which includes information submission or collection, secure storage, inquiry and search capability, controlled dissemination, and review and purge processes.

3. **Driver's Privacy Protection Act (DPPA) of 1994, 18 U.S.C. 2721 and 2725—18 U.S.C. 2725 (4)** defines "highly restricted personal information" as **an individual's photograph or image**, social security number, medical or disability information. 18 U.S.C. 2721(b)(1) states that personal information (as described in 18 U.S.C. 2725(4), above) may be disclosed for use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a federal, state, or local agency in carrying out its functions. § 2721-2725 restricts access and prohibits the release of personal information from state motor vehicle records to ensure the privacy of persons whose records have been obtained by that department in connection with a motor vehicle record unless certain criteria are met.

4. **E-Government Act of 2002, Public Law 107–347, 208, 116 Stat. 2899 (2002)—**Office of Management and Budget (OMB) (03-22, OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002)**—**OMB implementing guidance for this act requires federal agencies to perform privacy impact assessments (PIAs) for new information technologies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make significant changes to existing information technology that manages information in identifiable form. A PIA is an evaluation of how information in identifiable form is collected, stored, protected, shared, and managed. The purpose of a PIA is to demonstrate that system owners and developers have incorporated P/CRCL protections throughout the entire life cycle of a system. The act requires an agency to make PIAs publicly available, except when an agency, in its discretion, determines that publication of the PIA would raise security concerns or reveal classified (i.e., national security) or sensitive information. Although this act does not apply to SLTT partners, this tool is useful for identifying and mitigating privacy risks and for notifying the public what PII the SLTT agency is collecting, why PII is being collected, and how the PII will be collected, used, accessed, shared, safeguarded, and stored.

5. **Enhanced Border Security and Visa Reform Act of 2002, H.R. 3525**—In the Enhanced Border Security and Visa Entry Reform Act of 2002, the U.S. Congress mandated the use of biometrics in U.S. visas. This law requires that U.S. embassies and consulates abroad must issue to international visitors, "only machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers." Additionally, the Homeland Security Council decided that the U.S. standard for biometric screening is 10 fingerprint scans collected at all U.S. embassies and consulates for visa applicants seeking to come to the United States.

6. **Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99**—FERPA governs the disclosure of students' biometric information, to the extent that it is contained in student records. A student's biometric record is included in the definition of personally identifiable information, and is a type of information that may be included in students' education records. As such, FERPA prohibits schools from releasing students' biometric information without parental consent, to the extent that it is contained

in students' education records, with some limited exceptions.[34]

7. **Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983—**This is a federal statute that allows an individual to sue public officials in federal court for violations of the individual's civil rights. Civil rights include such things as the Fourth Amendment's prohibitions against unreasonable search and seizure, violations of privacy rights, and violations of the right to freedom of religion, free speech, and free association. It serves as a deterrent to unlawful collection, use, or sharing of information rather than providing specific authority or a prohibition to the collection, use, or sharing of information.

8. **Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301**—This chapter contains the laws governing disposal of records made or received by a federal agency in the normal course of business. It discusses procedures and notices, if required, and the role of the federal archivist. The law applies only to federal agencies, but there may be similar state or local laws applicable to state and local agencies.

9. **Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552—**The federal FOIA, enacted in 1966, provides access to federal agency records or information. It does not, however, allow access to state or local government records. Nearly all states have their own public access statutes that provide access to state- and local-agency records. The interaction of federal and state FOIA laws can create complex issues. Federal statutes, in essence, provide a baseline of legal protections for individuals. While state legislatures may pass laws to supplement these federal guidelines, state laws that interfere with or are contrary to a federal law are preempted. By virtue of the Supremacy Clause of the U.S. Constitution (Article VI, Clause 2), federal law may restrict access to records otherwise available pursuant to a state's FOIA by requiring that certain information be kept confidential. Thus, federal confidentiality requirements may supersede a state FOIA statute mandating public disclosure of a record, but only when there is a specific federal statute (other than the federal FOIA) that mandates the records be kept confidential. In short, records may be available under one FOIA statute but not pursuant to another.

10. **Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191**—HIPAA was enacted to improve the Medicare and Medicaid programs and the efficiency and effectiveness of the nation's health care system by encouraging the development of a national health information system through the establishment of standards and requirements for the electronic transmission of health information. To that end, Congress directed the U.S. Department of Health and Human Services (HHS) to issue safeguards to protect the security and confidentiality of health information. To implement HIPAA's privacy requirements, HHS promulgated regulations setting national privacy standards for health information: the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule")—42 U.S.C. §1320d-2; 45 CFR Parts 160, 164 (2003).

11. **HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, Code of Federal Regulations, Title 45, Parts 160 and 164**—This "Privacy Rule" sets forth national standards for the privacy and security of individually identifiable health information (45 CFR Part 164, Subpart E (2003)). This rule has been described as providing a "federal floor" of safeguards to protect the confidentiality of medical information. State laws that provide stronger privacy protection will continue to apply over and above the federal privacy protection. The general rule under these standards states that a covered entity may not use or disclose protected health information except as permitted or required by the rules (45 CFR Part 164.502(a) and §164.103 [defining protected health information and use]). The Privacy Rule applies to the following covered entities: (1) a health plan, (2) a health care clearinghouse, and (3) a health care provider who transmits any health information in electronic form in connection with certain transactions (42 U.S.C. §1320d-1(a) (2003); 45 CFR Part 160.102 (2003). Since the Privacy Rule applies only to a covered entity, a governmental body begins its inquiry by

[34] *Developing Laws Address Flourishing Commercial Use of Biometric Information,* Claypoole, Ted, and Stoll, Cameron, Business Law Today, American Bar Association, May 2016, https://www.americanbar.org/publications/blt/2016/05/08_claypoole.html.

first determining whether it is a covered entity under the Privacy Rule (45 CFR Part 160.103 (2003) [defining health plan, health care clearinghouse, health care provider]). If it is a covered entity, it then looks to the Privacy Rule for a permitted or required disclosure.

Section 164.510(b)(3) permits (but does not require) a health care provider, when a patient is not present or is unable to agree or object to a disclosure due to incapacity or emergency circumstances, to determine whether disclosing a patient's information to the patient's family, friends, or other persons involved in the patient's care, is in the best interests of the patient. Where a provider determines that such a disclosure is in the patient's best interests, the provider would be permitted to disclose only the protected health information (PHI) that is directly relevant to the person's involvement in the patient's care.

This permission clearly applies where a patient is unconscious. However, there may be additional situations in which a health care provider believes, based on professional judgment, that the patient does not have the capacity to agree or object to the sharing of PHI at a particular time and that sharing the information is in the best interests of the patient at that time. These may include circumstances in which a patient is suffering from temporary psychosis or is under the influence of drugs or alcohol.

12. **Indian Civil Rights Act of 1968, 25 U.S.C. § 1301 et seq., United States Code, Title 25, Chapter 15, Subchapter I—**This act contains definitions of relevant terms and extends certain constitutional rights to Indian tribes exercising powers of self-government.

13. **National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490—**In each state, an authorized criminal justice agency of the state shall report child abuse crime information to or index child abuse crime information in the national criminal history background check system. A criminal justice agency can satisfy the requirement by reporting or indexing all felony and serious misdemeanor arrests and dispositions. The U.S. Attorney General (AG) is required to publish an annual statistical summary of child abuse crimes. The act requires that 80 percent of final dispositions be entered in the state databases by December 1998, with steps being taken toward 100 percent entry.

    A 1994 amendment required that the AG—in consultation with federal, state, and local officials, including officials responsible for criminal history record systems, and representatives of public and private care organizations and health, legal, and social welfare organizations—shall develop guidelines for the adoption of appropriate safeguards by care providers and by the state for protecting children, the elderly, and individuals with disabilities from abuse.

14. **NIST Special Publication 800-53 (Appendix J) *Security and Privacy Controls for Federal Information Systems and Organizations*—** Federal agencies are required to ensure that privacy protections are incorporated into information security planning. To that end, SP 800-53 Rev. 4 features eight families of privacy controls that are based on FIPPs. The proliferation of social media, Smart Grid, mobile, and cloud computing as well as the transition from structured to unstructured information and metadata environments have added significant complexities and challenges for federal organizations in safeguarding privacy. These challenges extend well beyond the traditional information technology security view of protecting privacy, which focused primarily on ensuring confidentiality. The use of these standardized privacy controls will provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance with those requirements. Like their federal partners, SLTT agencies may use the privacy controls when evaluating their systems, processes, and programs.

15. **Preparing for and Responding to a Breach of Personally Identifiable Information, OMB Memorandum M-17-12 (January 2017)**—This Memorandum sets forth the policy for federal agencies to prepare for and respond to a breach of PII. It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals. This memorandum is intended to promote consistency in the way agencies prepare for and respond to a breach by requiring common standards and processes.

16. **Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a—**The Privacy Act establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal

agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act prohibits the disclosure of a record about an individual from a system of records without the written consent of the individual, unless the disclosure is pursuant to one of 12 statutory exceptions. The act also provides individuals with a means by which to seek access to and amendment of their records and sets agency record-keeping requirements. In addition, the Privacy Act requires that agencies give the public notice of their systems of records by publication in the *Federal Register*.

17. **Protection of Sensitive Agency Information, Office of Management and Budget Memorandum M-06-16 (June 2006)—**This memorandum provides a security checklist from the National Institute of Standards and Technology (NIST) to protect remote information removed from or accessed from outside an agency's physical location specific to personally identifiable information (PII). The NIST checklist requires that agencies verify PII in need of protection, confirm the adequacy of organization policy surrounding PII protection, and implement any necessary protections for PII transported or stored off-site or accessed remotely. In addition to the NIST checklist, the memorandum recommends implementing information encryption on all mobile devices, allowing remote access only with two-factor authentication, using timeout functions on devices, and logging all computer-readable information extracts from databases with sensitive information, while verifying that each extract has either been erased within 90 days or its use is still required.

18. **REAL ID Act of 2005, Public Law 109–13, Division B, 119 Statute 302, enacted May 11, 2005—**The REAL ID Act requires states to issue driver's licenses and identification cards that comply with standards established by the U.S. Department of Homeland Security if those identifying documents will be used to gain access to federal facilities, board federally regulated commercial aircraft, or enter nuclear power plants. Of particular note, the REAL ID Act requires that a face image be captured for each person ***applying*** for a driver's license or identification card versus existing practices in most states that only capture face images that are ultimately ***issued*** a card. While all states capture face images as part of the routine issuance process for driver's licenses and identification cards, laws in 32 states grant exceptions to the photograph requirement for individuals, including religious objectors, overseas military personnel, and persons unable to visit a service center due to physical disabilities. The REAL ID act further requires departments of motor vehicles to make reasonable efforts to ensure that an applicant does not have more than one driver's license or identification card already issued by that state under a different identity. Many states are already complying with this requirement through the use of face comparison systems. It not only requires the collection of face images but implicitly authorizes the creation of biometric templates used by face comparison systems.

19. **Section 210401 of the Violent Crime Control and Law Enforcement Act of 1994, 42 U.S.C. § 14141—**This is a federal statute that provides that it shall be unlawful for any governmental authority or its agent to engage in a pattern or practice of conduct by law enforcement officers that violates the Constitution or laws of the United States. It authorizes the Attorney General to bring civil actions to obtain injunctive or declaratory relief to eliminate the unlawful or unconstitutional pattern or practice.

20. **U.S. Constitution, First, Fourth, Fifth, Sixth, and Fourteenth Amendments—**The Bill of Rights establishes minimum standards for the protection of the civil rights and civil liberties of persons within the United States. The First Amendment protects religious freedom, speech, the press, the right to peaceably assemble, and the right to petition the government for a redress of grievances. The Fourth Amendment protects the people from unreasonable searches and seizures and requires that warrants be issued only upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the individual or things to be seized. The Sixth Amendment establishes the right of an accused individual to a speedy and public trial by an impartial jury, to be informed of the nature and cause of the charges, to confront witnesses, to have compulsory process to obtain witnesses, and to have the assistance of legal counsel. The Fourteenth Amendment addresses citizenship rights and equal protection of the laws. Although the equal protection clause applies explicitly only to state governments, equal protection requirements apply to the federal government through the Fifth Amendment Due Process Clause.

Appendix D—Listing of Illinois Laws & Chicago Municipal Code

Freedom of Information Act (5 ILCS 140/)

(5 ILCS 140/1) (from Ch. 116, par. 201)

Sec. 1. Pursuant to the fundamental philosophy of the American constitutional form of government, it is declared to be the public policy of the State of Illinois that all persons are entitled to full and complete information regarding the affairs of government and the official acts and policies of those who represent them as public officials and public employees consistent with the terms of this Act. Such access is necessary to enable the people to fulfill their duties of discussing public issues fully and freely, making informed political judgments and monitoring government to ensure that it is being conducted in the public interest.

The General Assembly hereby declares that it is the public policy of the State of Illinois that access by all persons to public records promotes the transparency and accountability of public bodies at all levels of government. It is a fundamental obligation of government to operate openly and provide public records as expediently and efficiently as possible in compliance with this Act.

This Act is not intended to cause an unwarranted invasion of personal privacy, nor to allow the requests of a commercial enterprise to unduly burden public resources, or to disrupt the duly-undertaken work of any public body independent of the fulfillment of any of the fore-mentioned rights of the people to access to information.

This Act is not intended to create an obligation on the part of any public body to maintain or prepare any public record which was not maintained or prepared by such public body at the time when this Act becomes effective, except as otherwise required by applicable local, State or federal law.

Restraints on access to information, to the extent permitted by this Act, are limited exceptions to the principle that the people of this State have a right to full disclosure of information relating to the decisions, policies, procedures, rules, standards, and other aspects of government activity that affect the conduct of government and the lives of any or all of the people. The provisions of this Act shall be construed in accordance with this principle. This Act shall be construed to require disclosure of

requested information as expediently and efficiently as possible and adherence to the deadlines established in this Act.

The General Assembly recognizes that this Act imposes fiscal obligations on public bodies to provide adequate staff and equipment to comply with its requirements. The General Assembly declares that providing records in compliance with the requirements of this Act is a primary duty of public bodies to the people of this State, and this Act should be construed to this end, fiscal obligations notwithstanding.

The General Assembly further recognizes that technology may advance at a rate that outpaces its ability to address those advances legislatively. To the extent that this Act may not expressly apply to those technological advances, this Act should nonetheless be interpreted to further the declared policy of this Act that public records shall be made available upon request except when denial of access furthers the public policy underlying a specific exemption.

This Act shall be the exclusive State statute on freedom of information, except to the extent that other State statutes might create additional restrictions on disclosure of information or other laws in Illinois might create additional obligations for disclosure of information to the public.
(Source: P.A. 96-542, eff. 1-1-10.)

(5 ILCS 140/1.1) (from Ch. 116, par. 201.1)

Sec. 1.1. This Act may be cited as the Freedom of Information Act.
(Source: P.A. 86-1475.)

(5 ILCS 140/1.2)

Sec. 1.2. Presumption. All records in the custody or possession of a public body are presumed to be open to inspection or copying. Any public body that asserts that a record is exempt from disclosure has the burden of proving by clear and convincing evidence that it is exempt.
(Source: P.A. 96-542, eff. 1-1-10.)

(5 ILCS 140/2) (from Ch. 116, par. 202)

Sec. 2. Definitions. As used in this Act:

(a) "Public body" means all legislative, executive, administrative, or advisory bodies of the State, state universities and colleges, counties, townships, cities, villages, incorporated towns, school districts and all other municipal corporations, boards, bureaus, committees, or commissions of this State, any subsidiary bodies of any of the foregoing including but not limited to committees and subcommittees thereof, and a School Finance Authority created under Article 1E of the School Code. "Public body" does not include a child death review team or the Illinois Child Death Review Teams Executive Council established under the Child Death Review Team Act, or a regional youth advisory board or the Statewide Youth Advisory Board established under the Department of Children and Family Services Statewide Youth Advisory Board Act.

(b) "Person" means any individual, corporation, partnership, firm, organization or association, acting individually or as a group.

(c) "Public records" means all records, reports, forms, writings, letters, memoranda, books, papers, maps, photographs, microfilms, cards, tapes, recordings, electronic data processing records, electronic communications, recorded information and all other documentary materials pertaining to the transaction of public business, regardless of physical form or characteristics, having been prepared by or for, or having been or being used by, received by, in the possession of, or under the control of any public body.

(c-5) "Private information" means unique identifiers, including a person's social security number, driver's license number, employee identification number, biometric identifiers, personal financial information, passwords or other access codes, medical records, home or personal telephone numbers, and personal email addresses. Private information also includes home address and personal license plates, except as otherwise provided by law or when compiled without possibility of attribution to any person.

(c-10) "Commercial purpose" means the use of any part of a public record or records, or information derived from public records, in any form for sale, resale, or solicitation or advertisement for sales or services. For purposes of this definition, requests made by news media and non-profit, scientific, or academic organizations shall not be considered to be made for a "commercial purpose" when the principal purpose of the request is (i) to access and disseminate information concerning news and current or passing events, (ii) for articles of opinion or features of interest to the public, or (iii) for the purpose of academic, scientific, or public research or education.

(d) "Copying" means the reproduction of any public record by means of any photographic, electronic, mechanical or other process, device or means now known or hereafter developed and available to the public body.

(e) "Head of the public body" means the president, mayor, chairman, presiding officer, director, superintendent, manager, supervisor or individual otherwise holding primary executive and administrative authority for the public body, or such person's duly authorized designee.

(f) "News media" means a newspaper or other periodical issued at regular intervals whether in print or electronic format, a news service whether in print or electronic format, a radio station, a television station, a television network, a community antenna television service, or a person or corporation engaged in making news reels or other motion picture news for public showing.

(g) "Recurrent requester", as used in Section 3.2 of this Act, means a person that, in the 12 months immediately preceding the request, has submitted to the same public body (i) a minimum of 50 requests for records, (ii) a minimum of 15 requests for records within a 30-day period, or (iii) a minimum of 7 requests for records within a 7-day period. For purposes of this definition, requests made by news media and non-profit, scientific, or academic organizations shall not be considered in calculating the number of requests made in the time periods in this definition when the principal purpose of the requests is (i) to access and disseminate information concerning news and current or passing events, (ii) for articles of opinion or features of interest to the public, or (iii) for the purpose of academic, scientific, or public research or education.

For the purposes of this subsection (g), "request" means a written document (or oral request, if the public body chooses to honor oral requests) that is submitted to a public body via personal delivery, mail, telefax, electronic mail, or other means available to the public body and that identifies the particular public record the requester seeks. One request may identify multiple records to be inspected or copied.

(h) "Voluminous request" means a request that: (i) includes more than 5 individual requests for more than 5 different categories of records or a combination of individual requests that total requests for more than 5 different categories of records in a period of 20 business days; or (ii) requires the compilation of more than 500 letter or legal-sized pages of public records unless a single requested record exceeds 500 pages. "Single requested record" may include, but is not limited to, one report, form, e-mail, letter, memorandum, book, map, microfilm, tape, or recording.

"Voluminous request" does not include a request made by news media and non-profit, scientific, or academic organizations if the principal purpose of the request is: (1) to access and disseminate information concerning news and current or passing events; (2) for articles of opinion or features of interest to the public; or (3) for the

purpose of academic, scientific, or public research or education.

For the purposes of this subsection (h), "request" means a written document, or oral request, if the public body chooses to honor oral requests, that is submitted to a public body via personal delivery, mail, telefax, electronic mail, or other means available to the public body and that identifies the particular public record or records the requester seeks. One request may identify multiple individual records to be inspected or copied.

(i) "Severance agreement" means a mutual agreement between any public body and its employee for the employee's resignation in exchange for payment by the public body.

(Source: P.A. 98-806, eff. 1-1-15; 98-1129, eff. 12-3-14; 99-78, eff. 7-20-15; 99-478, eff. 6-1-16.)

(5 ILCS 140/2.5)

Sec. 2.5. Records of funds. All records relating to the obligation, receipt, and use of public funds of the State, units of local government, and school districts are public records subject to inspection and copying by the public.

(Source: P.A. 96-542, eff. 1-1-10.)

(5 ILCS 140/2.10)

Sec. 2.10. Payrolls. Certified payroll records submitted to a public body under Section 5(a)(2) of the Prevailing Wage Act are public records subject to inspection and copying in accordance with the provisions of this Act; except that contractors' employees' addresses, telephone numbers, and social security numbers must be redacted by the public body prior to disclosure.

(Source: P.A. 96-542, eff. 1-1-10.)

(5 ILCS 140/2.15)

Sec. 2.15. Arrest reports and criminal history records.

(a) Arrest reports. The following chronologically maintained arrest and criminal history information maintained by State or local criminal justice agencies shall be furnished as soon as practical, but in no event later than 72 hours after the arrest, notwithstanding the time limits otherwise provided for in Section 3 of this Act: (i) information that identifies the individual, including the name, age, address, and photograph, when and if available; (ii) information detailing any charges relating to the arrest; (iii) the time and location of the arrest; (iv) the name of the investigating or arresting law enforcement agency; (v) if the individual is incarcerated, the amount of any bail or bond; and (vi) if the individual is incarcerated, the time and date that the individual was received into, discharged from, or transferred from the arresting agency's custody.

(b) Criminal history records. The following documents maintained by a public body pertaining to criminal history record information are public records subject to inspection and copying by the public pursuant to this Act: (i) court records that are public; (ii) records that are otherwise available under State or local law; and (iii) records in which the requesting party is the individual identified, except as provided under Section 7(1)(d)(vi).

(c) Information described in items (iii) through (vi) of subsection (a) may be withheld if it is determined that disclosure would: (i) interfere with pending or actually and reasonably contemplated law enforcement proceedings conducted by any law enforcement agency; (ii) endanger the life or physical safety of law enforcement or correctional personnel or any other person; or (iii) compromise the security of any correctional facility.

(d) The provisions of this Section do not supersede the confidentiality provisions

for law enforcement or arrest records of the Juvenile Court Act of 1987.

(e) Notwithstanding the requirements of subsection (a), a law enforcement agency may not publish booking photographs, commonly known as "mugshots", on its social networking website in connection with civil offenses, petty offenses, business offenses, Class C misdemeanors, and Class B misdemeanors unless the booking photograph is posted to the social networking website to assist in the search for a missing person or to assist in the search for a fugitive, person of interest, or individual wanted in relation to a crime other than a petty offense, business offense, Class C misdemeanor, or Class B misdemeanor. As used in this subsection, "social networking website" has the meaning provided in Section 10 of the Right to Privacy in the Workplace Act.

(Source: P.A. 100-927, eff. 1-1-19; 101-433, eff. 8-20-19.)

(5 ILCS 140/2.20)

Sec. 2.20. Settlement and severance agreements. All settlement and severance agreements entered into by or on behalf of a public body are public records subject to inspection and copying by the public, provided that information exempt from disclosure under Section 7 of this Act may be redacted.

(Source: P.A. 99-478, eff. 6-1-16.)

(5 ILCS 140/3) (from Ch. 116, par. 203)

Sec. 3. (a) Each public body shall make available to any person for inspection or copying all public records, except as otherwise provided in Sections 7 and 8.5 of this Act. Notwithstanding any other law, a public body may not grant to any person or entity, whether by contract, license, or otherwise, the exclusive right to access and disseminate any public record as defined in this Act.

(b) Subject to the fee provisions of Section 6 of this Act, each public body shall promptly provide, to any person who submits a request, a copy of any public record required to be disclosed by subsection (a) of this Section and shall certify such copy if so requested.

(c) Requests for inspection or copies shall be made in writing and directed to the public body. Written requests may be submitted to a public body via personal delivery, mail, telefax, or other means available to the public body. A public body may honor oral requests for inspection or copying. A public body may not require that a request be submitted on a standard form or require the requester to specify the purpose for a request, except to determine whether the records are requested for a commercial purpose or whether to grant a request for a fee waiver. All requests for inspection and copying received by a public body shall immediately be forwarded to its Freedom of Information officer or designee.

(d) Each public body shall, promptly, either comply with or deny a request for public records within 5 business days after its receipt of the request, unless the time for response is properly extended under subsection (e) of this Section. Denial shall be in writing as provided in Section 9 of this Act. Failure to comply with a written request, extend the time for response, or deny a request within 5 business days after its receipt shall be considered a denial of the request. A public body that fails to respond to a request within the requisite periods in this Section but thereafter provides the requester with copies of the requested public records may not impose a fee for such copies. A public body that fails to respond to a request received may not treat the request as unduly burdensome under subsection (g).

(e) The time for response under this Section may be extended by the public body for not more than 5 business days from the original due date for any of the following reasons:

(i) the requested records are stored in whole or in part at other locations than the office having charge of the requested records;

(ii) the request requires the collection of a substantial number of specified records;

(iii) the request is couched in categorical terms and requires an extensive search for the records responsive to it;

(iv) the requested records have not been located in the course of routine search and additional efforts are being made to locate them;

(v) the requested records require examination and evaluation by personnel having the necessary competence and discretion to determine if they are exempt from disclosure under Section 7 of this Act or should be revealed only with appropriate deletions;

(vi) the request for records cannot be complied with by the public body within the time limits prescribed by subsection (d) of this Section without unduly burdening or interfering with the operations of the public body;

(vii) there is a need for consultation, which shall be conducted with all practicable speed, with another public body or among 2 or more components of a public body having a substantial interest in the determination or in the subject matter of the request.

The person making a request and the public body may agree in writing to extend the time for compliance for a period to be determined by the parties. If the requester and the public body agree to extend the period for compliance, a failure by the public body to comply with any previous deadlines shall not be treated as a denial of the request for the records.

(f) When additional time is required for any of the above reasons, the public body shall, within 5 business days after receipt of the request, notify the person making the request of the reasons for the extension and the date by which the response will be forthcoming. Failure to respond within the time permitted for extension shall be considered a denial of the request. A public body that fails to respond to a request within the time permitted for extension but thereafter provides the requester with copies of the requested public records may not impose a fee for those copies. A public body that requests an extension and subsequently fails to respond to the request may not treat the request as unduly burdensome under subsection (g).

(g) Requests calling for all records falling within a category shall be complied with unless compliance with the request would be unduly burdensome for the complying public body and there is no way to narrow the request and the burden on the public body outweighs the public interest in the information. Before invoking this exemption, the public body shall extend to the person making the request an opportunity to confer with it in an attempt to reduce the request to manageable proportions. If any public body responds to a categorical request by stating that compliance would unduly burden its operation and the conditions described above are met, it shall do so in writing, specifying the reasons why it would be unduly burdensome and the extent to which compliance will so burden the operations of the public body. Such a response shall be treated as a denial of the request for information.

Repeated requests from the same person for the same records that are unchanged or identical to records previously provided or properly denied under this Act shall be deemed unduly burdensome under this provision.

(h) Each public body may promulgate rules and regulations in conformity with the provisions of this Section pertaining to the availability of records and procedures to be followed, including:

(i) the times and places where such records will be made available, and

(ii) the persons from whom such records may be obtained.

(i) The time periods for compliance or denial of a request to inspect or copy records set out in this Section shall not apply to requests for records made for a commercial purpose, requests by a recurrent requester, or voluminous requests.

Such requests shall be subject to the provisions of Sections 3.1, 3.2, and 3.6 of this Act, as applicable.
(Source: P.A. 101-81, eff. 7-12-19.)

(5 ILCS 140/3.1)
Sec. 3.1. Requests for commercial purposes.
(a) A public body shall respond to a request for records to be used for a commercial purpose within 21 working days after receipt. The response shall (i) provide to the requester an estimate of the time required by the public body to provide the records requested and an estimate of the fees to be charged, which the public body may require the person to pay in full before copying the requested documents, (ii) deny the request pursuant to one or more of the exemptions set out in this Act, (iii) notify the requester that the request is unduly burdensome and extend an opportunity to the requester to attempt to reduce the request to manageable proportions, or (iv) provide the records requested.
(b) Unless the records are exempt from disclosure, a public body shall comply with a request within a reasonable period considering the size and complexity of the request, and giving priority to records requested for non-commercial purposes.
(c) It is a violation of this Act for a person to knowingly obtain a public record for a commercial purpose without disclosing that it is for a commercial purpose, if requested to do so by the public body.
(Source: P.A. 96-542, eff. 1-1-10.)

(5 ILCS 140/3.2)
Sec. 3.2. Recurrent requesters.
(a) Notwithstanding any provision of this Act to the contrary, a public body shall respond to a request from a recurrent requester, as defined in subsection (g) of Section 2, within 21 business days after receipt. The response shall (i) provide to the requester an estimate of the time required by the public body to provide the records requested and an estimate of the fees to be charged, which the public body may require the person to pay in full before copying the requested documents, (ii) deny the request pursuant to one or more of the exemptions set out in this Act, (iii) notify the requester that the request is unduly burdensome and extend an opportunity to the requester to attempt to reduce the request to manageable proportions, or (iv) provide the records requested.
(b) Within 5 business days after receiving a request from a recurrent requester, as defined in subsection (g) of Section 2, the public body shall notify the requester (i) that the public body is treating the request as a request under subsection (g) of Section 2, (ii) of the reasons why the public body is treating the request as a request under subsection (g) of Section 2, and (iii) that the public body will send an initial response within 21 business days after receipt in accordance with subsection (a) of this Section. The public body shall also notify the requester of the proposed responses that can be asserted pursuant to subsection (a) of this Section.
(c) Unless the records are exempt from disclosure, a public body shall comply with a request within a reasonable period considering the size and complexity of the request.
(Source: P.A. 97-579, eff. 8-26-11; 98-756, eff. 7-16-14.)

(5 ILCS 140/3.3)
Sec. 3.3. This Act is not intended to compel public bodies to interpret or advise requesters as to the meaning or significance of the public records.
(Source: P.A. 96-542, eff. 1-1-10.)

(5 ILCS 140/3.5)

Sec. 3.5. Freedom of Information officers.

(a) Each public body shall designate one or more officials or employees to act as its Freedom of Information officer or officers. Except in instances when records are furnished immediately, Freedom of Information officers, or their designees, shall receive requests submitted to the public body under this Act, ensure that the public body responds to requests in a timely fashion, and issue responses under this Act. Freedom of Information officers shall develop a list of documents or categories of records that the public body shall immediately disclose upon request.

Upon receiving a request for a public record, the Freedom of Information officer shall:

(1) note the date the public body receives the written request;

(2) compute the day on which the period for response will expire and make a notation of that date on the written request;

(3) maintain an electronic or paper copy of a written request, including all documents submitted with the request until the request has been complied with or denied; and

(4) create a file for the retention of the original request, a copy of the response, a record of written communications with the requester, and a copy of other communications.

(b) All Freedom of Information officers shall, within 6 months after the effective date of this amendatory Act of the 96th General Assembly, successfully complete an electronic training curriculum to be developed by the Public Access Counselor and thereafter successfully complete an annual training program. Thereafter, whenever a new Freedom of Information officer is designated by a public body, that person shall successfully complete the electronic training curriculum within 30 days after assuming the position. Successful completion of the required training curriculum within the periods provided shall be a prerequisite to continue serving as a Freedom of Information officer.

(Source: P.A. 96-542, eff. 1-1-10.)

(5 ILCS 140/3.6)

Sec. 3.6. Voluminous requests.

(a) Notwithstanding any provision of this Act to the contrary, a public body shall respond to a voluminous request within 5 business days after receipt. The response shall notify the requester: (i) that the public body is treating the request as a voluminous request; (ii) the reasons why the public body is treating the request as a voluminous request; (iii) that the requester must respond to the public body within 10 business days after the public body's response was sent and specify whether the requester would like to amend the request in such a way that the public body will no longer treat the request as a voluminous request; (iv) that if the requester does not respond within 10 business days or if the request continues to be a voluminous request following the requester's response, the public body will respond to the request and assess any fees the public body charges pursuant to Section 6 of this Act; (v) that the public body has 5 business days after receipt of the requester's response or 5 business days from the last day for the requester to amend his or her request, whichever is sooner, to respond to the request; (vi) that the public body may request an additional 10 business days to comply with the request; (vii) of the requester's right to review of the public body's determination by the Public Access Counselor and provide the address and phone number for the Public Access Counselor; and (viii) that if the requester fails to accept or collect the responsive records, the public body may still charge the requester for its response pursuant to

Section 6 of this Act and the requester's failure to pay will be considered a debt due and owing to the public body and may be collected in accordance with applicable law.

(b) A public body shall provide a person making a voluminous request 10 business days from the date the public body's response pursuant to subsection (a) of this Section is sent to amend the request in such a way that the public body will no longer treat the request as a voluminous request.

(c) If a request continues to be a voluminous request following the requester's response under subsection (b) of this Section or the requester fails to respond, the public body shall respond within the earlier of 5 business days after it receives the response from the requester or 5 business days after the final day for the requester to respond to the public body's notification under this subsection. The response shall: (i) provide an estimate of the fees to be charged, which the public body may require the person to pay in full before copying the requested documents; (ii) deny the request pursuant to one or more of the exemptions set out in this Act; (iii) notify the requester that the request is unduly burdensome and extend an opportunity to the requester to attempt to reduce the request to manageable proportions; or (iv) provide the records requested.

(d) The time for response by the public body under subsection (c) of this Section may be extended by the public body for not more than 10 business days from the final day for the requester to respond to the public body's notification under subsection (c) of this Section for any of the reasons provided in subsection (e) of Section 3 of this Act.

The person making a request and the public body may agree in writing to extend the time for compliance for a period to be determined by the parties. If the requester and the public body agree to extend the period for compliance, a failure by the public body to comply with any previous deadlines shall not be treated as a denial of the request for the records.

(e) If a requester does not pay a fee charged pursuant to Section 6 of this Act for a voluminous request, the debt shall be considered a debt due and owing to the public body and may be collected in accordance with applicable law. This fee may be charged by the public body even if the requester fails to accept or collect records the public body has prepared in response to a voluminous request.
(Source: P.A. 98-1129, eff. 12-3-14.)

(5 ILCS 140/4) (from Ch. 116, par. 204)

Sec. 4. Each public body shall prominently display at each of its administrative or regional offices, make available for inspection and copying, and send through the mail if requested, each of the following:

(a) A brief description of itself, which will include, but not be limited to, a short summary of its purpose, a block diagram giving its functional subdivisions, the total amount of its operating budget, the number and location of all of its separate offices, the approximate number of full and part-time employees, and the identification and membership of any board, commission, committee, or council which operates in an advisory capacity relative to the operation of the public body, or which exercises control over its policies or procedures, or to which the public body is required to report and be answerable for its operations; and

(b) A brief description of the methods whereby the public may request information and public records, a directory designating the Freedom of Information officer or officers, the address where requests for public records should be directed, and any fees allowable under Section 6 of this Act.

A public body that maintains a website shall also post this information on its website.
(Source: P.A. 96-542, eff. 1-1-10; 96-1000, eff. 7-2-10.)

(5 ILCS 140/5) (from Ch. 116, par. 205)

Sec. 5. As to public records prepared or received after the effective date of this Act, each public body shall maintain and make available for inspection and copying a reasonably current list of all types or categories of records under its control. The list shall be reasonably detailed in order to aid persons in obtaining access to public records pursuant to this Act. Each public body shall furnish upon request a description of the manner in which public records stored by means of electronic data processing may be obtained in a form comprehensible to persons lacking knowledge of computer language or printout format.
(Source: P.A. 83-1013.)

(5 ILCS 140/6) (from Ch. 116, par. 206)

Sec. 6. Authority to charge fees.

(a) When a person requests a copy of a record maintained in an electronic format, the public body shall furnish it in the electronic format specified by the requester, if feasible. If it is not feasible to furnish the public records in the specified electronic format, then the public body shall furnish it in the format in which it is maintained by the public body, or in paper format at the option of the requester. A public body may charge the requester for the actual cost of purchasing the recording medium, whether disc, diskette, tape, or other medium. If a request is not a request for a commercial purpose or a voluminous request, a public body may not charge the requester for the costs of any search for and review of the records or other personnel costs associated with reproducing the records. Except to the extent that the General Assembly expressly provides, statutory fees applicable to copies of public records when furnished in a paper format shall not be applicable to those records when furnished in an electronic format.

(a-5) If a voluminous request is for electronic records and those records are not in a portable document format (PDF), the public body may charge up to $20 for not more than 2 megabytes of data, up to $40 for more than 2 but not more than 4 megabytes of data, and up to $100 for more than 4 megabytes of data. If a voluminous request is for electronic records and those records are in a portable document format, the public body may charge up to $20 for not more than 80 megabytes of data, up to $40 for more than 80 megabytes but not more than 160 megabytes of data, and up to $100 for more than 160 megabytes of data. If the responsive electronic records are in both a portable document format and not in a portable document format, the public body may separate the fees and charge the requester under both fee scales.

If a public body imposes a fee pursuant to this subsection (a-5), it must provide the requester with an accounting of all fees, costs, and personnel hours in connection with the request for public records.

(b) Except when a fee is otherwise fixed by statute, each public body may charge fees reasonably calculated to reimburse its actual cost for reproducing and certifying public records and for the use, by any person, of the equipment of the public body to copy records. No fees shall be charged for the first 50 pages of black and white, letter or legal sized copies requested by a requester. The fee for black and white, letter or legal sized copies shall not exceed 15 cents per page. If a public body provides copies in color or in a size other than letter or legal, the public body may not charge more than its actual cost for reproducing the records. In calculating its actual cost for reproducing records or for the use of the equipment of the public body to reproduce records, a public body shall not include the costs of any search for and review of the records or other personnel costs associated with reproducing the records, except for commercial requests as provided in subsection (f) of this Section. Such fees shall be imposed according to a standard scale of fees, established and

made public by the body imposing them. The cost for certifying a record shall not exceed $1.

(c) Documents shall be furnished without charge or at a reduced charge, as determined by the public body, if the person requesting the documents states the specific purpose for the request and indicates that a waiver or reduction of the fee is in the public interest. Waiver or reduction of the fee is in the public interest if the principal purpose of the request is to access and disseminate information regarding the health, safety and welfare or the legal rights of the general public and is not for the principal purpose of personal or commercial benefit. For purposes of this subsection, "commercial benefit" shall not apply to requests made by news media when the principal purpose of the request is to access and disseminate information regarding the health, safety, and welfare or the legal rights of the general public. In setting the amount of the waiver or reduction, the public body may take into consideration the amount of materials requested and the cost of copying them.

(d) The imposition of a fee not consistent with subsections (6)(a) and (b) of this Act constitutes a denial of access to public records for the purposes of judicial review.

(e) The fee for each abstract of a driver's record shall be as provided in Section 6-118 of "The Illinois Vehicle Code", approved September 29, 1969, as amended, whether furnished as a paper copy or as an electronic copy.

(f) A public body may charge up to $10 for each hour spent by personnel in searching for and retrieving a requested record or examining the record for necessary redactions. No fees shall be charged for the first 8 hours spent by personnel in searching for or retrieving a requested record. A public body may charge the actual cost of retrieving and transporting public records from an off-site storage facility when the public records are maintained by a third-party storage company under contract with the public body. If a public body imposes a fee pursuant to this subsection (f), it must provide the requester with an accounting of all fees, costs, and personnel hours in connection with the request for public records. The provisions of this subsection (f) apply only to commercial requests.
(Source: P.A. 97-579, eff. 8-26-11; 98-1129, eff. 12-3-14.)

(5 ILCS 140/7) (from Ch. 116, par. 207)
(Text of Section from P.A. 101-434)
Sec. 7. Exemptions.

(1) When a request is made to inspect or copy a public record that contains information that is exempt from disclosure under this Section, but also contains information that is not exempt from disclosure, the public body may elect to redact the information that is exempt. The public body shall make the remaining information available for inspection and copying. Subject to this requirement, the following shall be exempt from inspection and copying:

(a) Information specifically prohibited from disclosure by federal or State law or rules and regulations implementing federal or State law.

(b) Private information, unless disclosure is required by another provision of this Act, a State or federal law or a court order.

(b-5) Files, documents, and other data or databases maintained by one or more law enforcement agencies and specifically designed to provide information to one or more law enforcement agencies regarding the physical or mental status of one or more individual subjects.

(c) Personal information contained within public records, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, unless the disclosure is consented to in writing by the individual subjects of the information. "Unwarranted invasion of personal privacy" means the disclosure of information that is highly personal or objectionable to a reasonable

person and in which the subject's right to privacy outweighs any legitimate public interest in obtaining the information. The disclosure of information that bears on the public duties of public employees and officials shall not be considered an invasion of personal privacy.

(d) Records in the possession of any public body created in the course of administrative enforcement proceedings, and any law enforcement or correctional agency for law enforcement purposes, but only to the extent that disclosure would:

(i) interfere with pending or actually and reasonably contemplated law enforcement proceedings conducted by any law enforcement or correctional agency that is the recipient of the request;

(ii) interfere with active administrative enforcement proceedings conducted by the public body that is the recipient of the request;

(iii) create a substantial likelihood that a person will be deprived of a fair trial or an impartial hearing;

(iv) unavoidably disclose the identity of a confidential source, confidential information furnished only by the confidential source, or persons who file complaints with or provide information to administrative, investigative, law enforcement, or penal agencies; except that the identities of witnesses to traffic accidents, traffic accident reports, and rescue reports shall be provided by agencies of local government, except when disclosure would interfere with an active criminal investigation conducted by the agency that is the recipient of the request;

(v) disclose unique or specialized investigative techniques other than those generally used and known or disclose internal documents of correctional agencies related to detection, observation or investigation of incidents of crime or misconduct, and disclosure would result in demonstrable harm to the agency or public body that is the recipient of the request;

(vi) endanger the life or physical safety of law enforcement personnel or any other person; or

(vii) obstruct an ongoing criminal investigation by the agency that is the recipient of the request.

(d-5) A law enforcement record created for law enforcement purposes and contained in a shared electronic record management system if the law enforcement agency that is the recipient of the request did not create the record, did not participate in or have a role in any of the events which are the subject of the record, and only has access to the record through the shared electronic record management system.

(e) Records that relate to or affect the security of correctional institutions and detention facilities.

(e-5) Records requested by persons committed to the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail if those materials are available in the library of the correctional institution or facility or jail where the inmate is confined.

(e-6) Records requested by persons committed to the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail if those materials include records from staff members' personnel files, staff rosters, or other staffing assignment information.

(e-7) Records requested by persons committed to the Department of Corrections or Department of Human Services Division of Mental Health if those materials are available through an administrative request to the Department of Corrections or Department of Human Services Division of Mental Health.

(e-8) Records requested by a person committed to

the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail, the disclosure of which would result in the risk of harm to any person or the risk of an escape from a jail or correctional institution or facility.

(e-9) Records requested by a person in a county jail or committed to the Department of Corrections or Department of Human Services Division of Mental Health, containing personal information pertaining to the person's victim or the victim's family, including, but not limited to, a victim's home address, home telephone number, work or school address, work telephone number, social security number, or any other identifying information, except as may be relevant to a requester's current or potential case or claim.

(e-10) Law enforcement records of other persons requested by a person committed to the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail, including, but not limited to, arrest and booking records, mug shots, and crime scene photographs, except as these records may be relevant to the requester's current or potential case or claim.

(f) Preliminary drafts, notes, recommendations, memoranda and other records in which opinions are expressed, or policies or actions are formulated, except that a specific record or relevant portion of a record shall not be exempt when the record is publicly cited and identified by the head of the public body. The exemption provided in this paragraph (f) extends to all those records of officers and agencies of the General Assembly that pertain to the preparation of legislative documents.

(g) Trade secrets and commercial or financial information obtained from a person or business where the trade secrets or commercial or financial information are furnished under a claim that they are proprietary, privileged or confidential, and that disclosure of the trade secrets or commercial or financial information would cause competitive harm to the person or business, and only insofar as the claim directly applies to the records requested.

The information included under this exemption includes all trade secrets and commercial or financial information obtained by a public body, including a public pension fund, from a private equity fund or a privately held company within the investment portfolio of a private equity fund as a result of either investing or evaluating a potential investment of public funds in a private equity fund. The exemption contained in this item does not apply to the aggregate financial performance information of a private equity fund, nor to the identity of the fund's managers or general partners. The exemption contained in this item does not apply to the identity of a privately held company within the investment portfolio of a private equity fund, unless the disclosure of the identity of a privately held company may cause competitive harm.

Nothing contained in this paragraph (g) shall be construed to prevent a person or business from consenting to disclosure.

(h) Proposals and bids for any contract, grant, or agreement, including information which if it were disclosed would frustrate procurement or give an advantage to any person proposing to enter into a contractor agreement with the body, until an award or final selection is made. Information prepared by or for the body in preparation of a bid solicitation shall be exempt until an award or final selection is made.

(i) Valuable formulae, computer geographic systems, designs, drawings and research data obtained or produced by any public body when disclosure could reasonably be expected to produce private gain or public loss. The exemption for "computer geographic systems" provided in this paragraph (i) does not extend to requests made by news media as defined in Section 2 of this Act when the requested information is not otherwise exempt and

the only purpose of the request is to access and disseminate information regarding the health, safety, welfare, or legal rights of the general public.

(j) The following information pertaining to educational matters:

(i) test questions, scoring keys and other examination data used to administer an academic examination;

(ii) information received by a primary or secondary school, college, or university under its procedures for the evaluation of faculty members by their academic peers;

(iii) information concerning a school or university's adjudication of student disciplinary cases, but only to the extent that disclosure would unavoidably reveal the identity of the student; and

(iv) course materials or research materials used by faculty members.

(k) Architects' plans, engineers' technical submissions, and other construction related technical documents for projects not constructed or developed in whole or in part with public funds and the same for projects constructed or developed with public funds, including but not limited to power generating and distribution stations and other transmission and distribution facilities, water treatment facilities, airport facilities, sport stadiums, convention centers, and all government owned, operated, or occupied buildings, but only to the extent that disclosure would compromise security.

(l) Minutes of meetings of public bodies closed to the public as provided in the Open Meetings Act until the public body makes the minutes available to the public under Section 2.06 of the Open Meetings Act.

(m) Communications between a public body and an attorney or auditor representing the public body that would not be subject to discovery in litigation, and materials prepared or compiled by or for a public body in anticipation of a criminal, civil or administrative proceeding upon the request of an attorney advising the public body, and materials prepared or compiled with respect to internal audits of public bodies.

(n) Records relating to a public body's adjudication of employee grievances or disciplinary cases; however, this exemption shall not extend to the final outcome of cases in which discipline is imposed.

(o) Administrative or technical information associated with automated data processing operations, including but not limited to software, operating protocols, computer program abstracts, file layouts, source listings, object modules, load modules, user guides, documentation pertaining to all logical and physical design of computerized systems, employee manuals, and any other information that, if disclosed, would jeopardize the security of the system or its data or the security of materials exempt under this Section.

(p) Records relating to collective negotiating matters between public bodies and their employees or representatives, except that any final contract or agreement shall be subject to inspection and copying.

(q) Test questions, scoring keys, and other examination data used to determine the qualifications of an applicant for a license or employment.

(r) The records, documents, and information relating to real estate purchase negotiations until those negotiations have been completed or otherwise terminated. With regard to a parcel involved in a pending or actually and reasonably contemplated eminent domain proceeding under the Eminent Domain Act, records, documents and information relating to that parcel shall be exempt except as may be allowed under discovery rules adopted by the Illinois Supreme Court. The records, documents and information relating to a real estate sale shall be exempt until a sale is consummated.

(s) Any and all proprietary information and records

related to the operation of an intergovernmental risk management association or self-insurance pool or jointly self-administered health and accident cooperative or pool. Insurance or self insurance (including any intergovernmental risk management association or self insurance pool) claims, loss or risk management information, records, data, advice or communications.

(t) Information contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of a public body responsible for the regulation or supervision of financial institutions or insurance companies, unless disclosure is otherwise required by State law.

(u) Information that would disclose or might lead to the disclosure of secret or confidential information, codes, algorithms, programs, or private keys intended to be used to create electronic or digital signatures under the Electronic Commerce Security Act.

(v) Vulnerability assessments, security measures, and response policies or plans that are designed to identify, prevent, or respond to potential attacks upon a community's population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community, but only to the extent that disclosure could reasonably be expected to jeopardize the effectiveness of the measures or the safety of the personnel who implement them or the public. Information exempt under this item may include such things as details pertaining to the mobilization or deployment of personnel or equipment, to the operation of communication systems or protocols, or to tactical operations.

(w) (Blank).

(x) Maps and other records regarding the location or security of generation, transmission, distribution, storage, gathering, treatment, or switching facilities owned by a utility, by a power generator, or by the Illinois Power Agency.

(y) Information contained in or related to proposals, bids, or negotiations related to electric power procurement under Section 1-75 of the Illinois Power Agency Act and Section 16-111.5 of the Public Utilities Act that is determined to be confidential and proprietary by the Illinois Power Agency or by the Illinois Commerce Commission.

(z) Information about students exempted from disclosure under Sections 10-20.38 or 34-18.29 of the School Code, and information about undergraduate students enrolled at an institution of higher education exempted from disclosure under Section 25 of the Illinois Credit Card Marketing Act of 2009.

(aa) Information the disclosure of which is exempted under the Viatical Settlements Act of 2009.

(bb) Records and information provided to a mortality review team and records maintained by a mortality review team appointed under the Department of Juvenile Justice Mortality Review Team Act.

(cc) Information regarding interments, entombments, or inurnments of human remains that are submitted to the Cemetery Oversight Database under the Cemetery Care Act or the Cemetery Oversight Act, whichever is applicable.

(dd) Correspondence and records (i) that may not be disclosed under Section 11-9 of the Illinois Public Aid Code or (ii) that pertain to appeals under Section 11-8 of the Illinois Public Aid Code.

(ee) The names, addresses, or other personal information of persons who are minors and are also participants and registrants in programs of park districts, forest preserve districts, conservation districts, recreation agencies, and special recreation associations.

(ff) The names, addresses, or other personal

information of participants and registrants in programs of park districts, forest preserve districts, conservation districts, recreation agencies, and special recreation associations where such programs are targeted primarily to minors.

(gg) Confidential information described in Section 1-100 of the Illinois Independent Tax Tribunal Act of 2012.

(hh) The report submitted to the State Board of Education by the School Security and Standards Task Force under item (8) of subsection (d) of Section 2-3.160 of the School Code and any information contained in that report.

(ii) Records requested by persons committed to or detained by the Department of Human Services under the Sexually Violent Persons Commitment Act or committed to the Department of Corrections under the Sexually Dangerous Persons Act if those materials: (i) are available in the library of the facility where the individual is confined; (ii) include records from staff members' personnel files, staff rosters, or other staffing assignment information; or (iii) are available through an administrative request to the Department of Human Services or the Department of Corrections.

(jj) Confidential information described in Section 5-535 of the Civil Administrative Code of Illinois.

(kk) The public body's credit card numbers, debit card numbers, bank account numbers, Federal Employer Identification Number, security code numbers, passwords, and similar account information, the disclosure of which could result in identity theft or impression or defrauding of a governmental entity or a person.

(1.5) Any information exempt from disclosure under the Judicial Privacy Act shall be redacted from public records prior to disclosure under this Act.

(2) A public record that is not in the possession of a public body but is in the possession of a party with whom the agency has contracted to perform a governmental function on behalf of the public body, and that directly relates to the governmental function and is not otherwise exempt under this Act, shall be considered a public record of the public body, for purposes of this Act.

(3) This Section does not authorize withholding of information or limit the availability of records to the public, except as stated in this Section or otherwise provided in this Act.

(Source: P.A. 100-26, eff. 8-4-17; 100-201, eff. 8-18-17; 100-732, eff. 8-3-18; 101-434, eff. 1-1-20.)

(Text of Section from P.A. 101-452)

Sec. 7. Exemptions.

(1) When a request is made to inspect or copy a public record that contains information that is exempt from disclosure under this Section, but also contains information that is not exempt from disclosure, the public body may elect to redact the information that is exempt. The public body shall make the remaining information available for inspection and copying. Subject to this requirement, the following shall be exempt from inspection and copying:

(a) Information specifically prohibited from disclosure by federal or State law or rules and regulations implementing federal or State law.

(b) Private information, unless disclosure is required by another provision of this Act, a State or federal law or a court order.

(b-5) Files, documents, and other data or databases maintained by one or more law enforcement agencies and specifically designed to provide information to one or more law enforcement agencies regarding the physical or mental status of one or more individual subjects.

(c) Personal information contained within public

records, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, unless the disclosure is consented to in writing by the individual subjects of the information. "Unwarranted invasion of personal privacy" means the disclosure of information that is highly personal or objectionable to a reasonable person and in which the subject's right to privacy outweighs any legitimate public interest in obtaining the information. The disclosure of information that bears on the public duties of public employees and officials shall not be considered an invasion of personal privacy.

(d) Records in the possession of any public body created in the course of administrative enforcement proceedings, and any law enforcement or correctional agency for law enforcement purposes, but only to the extent that disclosure would:

(i) interfere with pending or actually and reasonably contemplated law enforcement proceedings conducted by any law enforcement or correctional agency that is the recipient of the request;

(ii) interfere with active administrative enforcement proceedings conducted by the public body that is the recipient of the request;

(iii) create a substantial likelihood that a person will be deprived of a fair trial or an impartial hearing;

(iv) unavoidably disclose the identity of a confidential source, confidential information furnished only by the confidential source, or persons who file complaints with or provide information to administrative, investigative, law enforcement, or penal agencies; except that the identities of witnesses to traffic accidents, traffic accident reports, and rescue reports shall be provided by agencies of local government, except when disclosure would interfere with an active criminal investigation conducted by the agency that is the recipient of the request;

(v) disclose unique or specialized investigative techniques other than those generally used and known or disclose internal documents of correctional agencies related to detection, observation or investigation of incidents of crime or misconduct, and disclosure would result in demonstrable harm to the agency or public body that is the recipient of the request;

(vi) endanger the life or physical safety of law enforcement personnel or any other person; or

(vii) obstruct an ongoing criminal investigation by the agency that is the recipient of the request.

(d-5) A law enforcement record created for law enforcement purposes and contained in a shared electronic record management system if the law enforcement agency that is the recipient of the request did not create the record, did not participate in or have a role in any of the events which are the subject of the record, and only has access to the record through the shared electronic record management system.

(e) Records that relate to or affect the security of correctional institutions and detention facilities.

(e-5) Records requested by persons committed to the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail if those materials are available in the library of the correctional institution or facility or jail where the inmate is confined.

(e-6) Records requested by persons committed to the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail if those materials include records from staff members' personnel files, staff rosters, or other staffing assignment information.

(e-7) Records requested by persons committed to the

Department of Corrections or Department of Human Services Division of Mental Health if those materials are available through an administrative request to the Department of Corrections or Department of Human Services Division of Mental Health.

(e-8) Records requested by a person committed to the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail, the disclosure of which would result in the risk of harm to any person or the risk of an escape from a jail or correctional institution or facility.

(e-9) Records requested by a person in a county jail or committed to the Department of Corrections or Department of Human Services Division of Mental Health, containing personal information pertaining to the person's victim or the victim's family, including, but not limited to, a victim's home address, home telephone number, work or school address, work telephone number, social security number, or any other identifying information, except as may be relevant to a requester's current or potential case or claim.

(e-10) Law enforcement records of other persons requested by a person committed to the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail, including, but not limited to, arrest and booking records, mug shots, and crime scene photographs, except as these records may be relevant to the requester's current or potential case or claim.

(f) Preliminary drafts, notes, recommendations, memoranda and other records in which opinions are expressed, or policies or actions are formulated, except that a specific record or relevant portion of a record shall not be exempt when the record is publicly cited and identified by the head of the public body. The exemption provided in this paragraph (f) extends to all those records of officers and agencies of the General Assembly that pertain to the preparation of legislative documents.

(g) Trade secrets and commercial or financial information obtained from a person or business where the trade secrets or commercial or financial information are furnished under a claim that they are proprietary, privileged or confidential, and that disclosure of the trade secrets or commercial or financial information would cause competitive harm to the person or business, and only insofar as the claim directly applies to the records requested.

The information included under this exemption includes all trade secrets and commercial or financial information obtained by a public body, including a public pension fund, from a private equity fund or a privately held company within the investment portfolio of a private equity fund as a result of either investing or evaluating a potential investment of public funds in a private equity fund. The exemption contained in this item does not apply to the aggregate financial performance information of a private equity fund, nor to the identity of the fund's managers or general partners. The exemption contained in this item does not apply to the identity of a privately held company within the investment portfolio of a private equity fund, unless the disclosure of the identity of a privately held company may cause competitive harm.

Nothing contained in this paragraph (g) shall be construed to prevent a person or business from consenting to disclosure.

(h) Proposals and bids for any contract, grant, or agreement, including information which if it were disclosed would frustrate procurement or give an advantage to any person proposing to enter into a contractor agreement with the body, until an award or final selection is made. Information prepared by or for the body in preparation of a bid solicitation shall be exempt until an award or final selection is made.

(i) Valuable formulae, computer geographic systems,

designs, drawings and research data obtained or produced by any public body when disclosure could reasonably be expected to produce private gain or public loss. The exemption for "computer geographic systems" provided in this paragraph (i) does not extend to requests made by news media as defined in Section 2 of this Act when the requested information is not otherwise exempt and the only purpose of the request is to access and disseminate information regarding the health, safety, welfare, or legal rights of the general public.

(j) The following information pertaining to educational matters:

(i) test questions, scoring keys and other examination data used to administer an academic examination;

(ii) information received by a primary or secondary school, college, or university under its procedures for the evaluation of faculty members by their academic peers;

(iii) information concerning a school or university's adjudication of student disciplinary cases, but only to the extent that disclosure would unavoidably reveal the identity of the student; and

(iv) course materials or research materials used by faculty members.

(k) Architects' plans, engineers' technical submissions, and other construction related technical documents for projects not constructed or developed in whole or in part with public funds and the same for projects constructed or developed with public funds, including but not limited to power generating and distribution stations and other transmission and distribution facilities, water treatment facilities, airport facilities, sport stadiums, convention centers, and all government owned, operated, or occupied buildings, but only to the extent that disclosure would compromise security.

(l) Minutes of meetings of public bodies closed to the public as provided in the Open Meetings Act until the public body makes the minutes available to the public under Section 2.06 of the Open Meetings Act.

(m) Communications between a public body and an attorney or auditor representing the public body that would not be subject to discovery in litigation, and materials prepared or compiled by or for a public body in anticipation of a criminal, civil or administrative proceeding upon the request of an attorney advising the public body, and materials prepared or compiled with respect to internal audits of public bodies.

(n) Records relating to a public body's adjudication of employee grievances or disciplinary cases; however, this exemption shall not extend to the final outcome of cases in which discipline is imposed.

(o) Administrative or technical information associated with automated data processing operations, including but not limited to software, operating protocols, computer program abstracts, file layouts, source listings, object modules, load modules, user guides, documentation pertaining to all logical and physical design of computerized systems, employee manuals, and any other information that, if disclosed, would jeopardize the security of the system or its data or the security of materials exempt under this Section.

(p) Records relating to collective negotiating matters between public bodies and their employees or representatives, except that any final contract or agreement shall be subject to inspection and copying.

(q) Test questions, scoring keys, and other examination data used to determine the qualifications of an applicant for a license or employment.

(r) The records, documents, and information relating to real estate purchase negotiations until those negotiations have been completed or otherwise terminated. With regard to a parcel involved in a pending or actually and reasonably contemplated eminent domain proceeding under the Eminent

Domain Act, records, documents and information relating to that parcel shall be exempt except as may be allowed under discovery rules adopted by the Illinois Supreme Court. The records, documents and information relating to a real estate sale shall be exempt until a sale is consummated.

(s) Any and all proprietary information and records related to the operation of an intergovernmental risk management association or self-insurance pool or jointly self-administered health and accident cooperative or pool. Insurance or self insurance (including any intergovernmental risk management association or self insurance pool) claims, loss or risk management information, records, data, advice or communications.

(t) Information contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of a public body responsible for the regulation or supervision of financial institutions, insurance companies, or pharmacy benefit managers, unless disclosure is otherwise required by State law.

(u) Information that would disclose or might lead to the disclosure of secret or confidential information, codes, algorithms, programs, or private keys intended to be used to create electronic or digital signatures under the Electronic Commerce Security Act.

(v) Vulnerability assessments, security measures, and response policies or plans that are designed to identify, prevent, or respond to potential attacks upon a community's population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community, but only to the extent that disclosure could reasonably be expected to jeopardize the effectiveness of the measures or the safety of the personnel who implement them or the public. Information exempt under this item may include such things as details pertaining to the mobilization or deployment of personnel or equipment, to the operation of communication systems or protocols, or to tactical operations.

(w) (Blank).

(x) Maps and other records regarding the location or security of generation, transmission, distribution, storage, gathering, treatment, or switching facilities owned by a utility, by a power generator, or by the Illinois Power Agency.

(y) Information contained in or related to proposals, bids, or negotiations related to electric power procurement under Section 1-75 of the Illinois Power Agency Act and Section 16-111.5 of the Public Utilities Act that is determined to be confidential and proprietary by the Illinois Power Agency or by the Illinois Commerce Commission.

(z) Information about students exempted from disclosure under Sections 10-20.38 or 34-18.29 of the School Code, and information about undergraduate students enrolled at an institution of higher education exempted from disclosure under Section 25 of the Illinois Credit Card Marketing Act of 2009.

(aa) Information the disclosure of which is exempted under the Viatical Settlements Act of 2009.

(bb) Records and information provided to a mortality review team and records maintained by a mortality review team appointed under the Department of Juvenile Justice Mortality Review Team Act.

(cc) Information regarding interments, entombments, or inurnments of human remains that are submitted to the Cemetery Oversight Database under the Cemetery Care Act or the Cemetery Oversight Act, whichever is applicable.

(dd) Correspondence and records (i) that may not be disclosed under Section 11-9 of the Illinois Public Aid Code or (ii) that pertain to appeals under Section 11-8 of the Illinois Public Aid Code.

(ee) The names, addresses, or other personal information of persons who are minors and are also participants and registrants in programs of park districts, forest preserve districts, conservation districts, recreation agencies, and special recreation associations.

(ff) The names, addresses, or other personal information of participants and registrants in programs of park districts, forest preserve districts, conservation districts, recreation agencies, and special recreation associations where such programs are targeted primarily to minors.

(gg) Confidential information described in Section 1-100 of the Illinois Independent Tax Tribunal Act of 2012.

(hh) The report submitted to the State Board of Education by the School Security and Standards Task Force under item (8) of subsection (d) of Section 2-3.160 of the School Code and any information contained in that report.

(ii) Records requested by persons committed to or detained by the Department of Human Services under the Sexually Violent Persons Commitment Act or committed to the Department of Corrections under the Sexually Dangerous Persons Act if those materials: (i) are available in the library of the facility where the individual is confined; (ii) include records from staff members' personnel files, staff rosters, or other staffing assignment information; or (iii) are available through an administrative request to the Department of Human Services or the Department of Corrections.

(jj) Confidential information described in Section 5-535 of the Civil Administrative Code of Illinois.

(1.5) Any information exempt from disclosure under the Judicial Privacy Act shall be redacted from public records prior to disclosure under this Act.

(2) A public record that is not in the possession of a public body but is in the possession of a party with whom the agency has contracted to perform a governmental function on behalf of the public body, and that directly relates to the governmental function and is not otherwise exempt under this Act, shall be considered a public record of the public body, for purposes of this Act.

(3) This Section does not authorize withholding of information or limit the availability of records to the public, except as stated in this Section or otherwise provided in this Act.

(Source: P.A. 100-26, eff. 8-4-17; 100-201, eff. 8-18-17; 100-732, eff. 8-3-18; 101-452, eff. 1-1-20.)

(Text of Section from P.A. 101-455)

Sec. 7. Exemptions.

(1) When a request is made to inspect or copy a public record that contains information that is exempt from disclosure under this Section, but also contains information that is not exempt from disclosure, the public body may elect to redact the information that is exempt. The public body shall make the remaining information available for inspection and copying. Subject to this requirement, the following shall be exempt from inspection and copying:

(a) Information specifically prohibited from disclosure by federal or State law or rules and regulations implementing federal or State law.

(b) Private information, unless disclosure is required by another provision of this Act, a State or federal law or a court order.

(b-5) Files, documents, and other data or databases maintained by one or more law enforcement agencies and specifically designed to provide information to one or more law enforcement agencies regarding the physical or mental status of one or more individual subjects.

(c) Personal information contained within public

records, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, unless the disclosure is consented to in writing by the individual subjects of the information. "Unwarranted invasion of personal privacy" means the disclosure of information that is highly personal or objectionable to a reasonable person and in which the subject's right to privacy outweighs any legitimate public interest in obtaining the information. The disclosure of information that bears on the public duties of public employees and officials shall not be considered an invasion of personal privacy.

(d) Records in the possession of any public body created in the course of administrative enforcement proceedings, and any law enforcement or correctional agency for law enforcement purposes, but only to the extent that disclosure would:

(i) interfere with pending or actually and reasonably contemplated law enforcement proceedings conducted by any law enforcement or correctional agency that is the recipient of the request;

(ii) interfere with active administrative enforcement proceedings conducted by the public body that is the recipient of the request;

(iii) create a substantial likelihood that a person will be deprived of a fair trial or an impartial hearing;

(iv) unavoidably disclose the identity of a confidential source, confidential information furnished only by the confidential source, or persons who file complaints with or provide information to administrative, investigative, law enforcement, or penal agencies; except that the identities of witnesses to traffic accidents, traffic accident reports, and rescue reports shall be provided by agencies of local government, except when disclosure would interfere with an active criminal investigation conducted by the agency that is the recipient of the request;

(v) disclose unique or specialized investigative techniques other than those generally used and known or disclose internal documents of correctional agencies related to detection, observation or investigation of incidents of crime or misconduct, and disclosure would result in demonstrable harm to the agency or public body that is the recipient of the request;

(vi) endanger the life or physical safety of law enforcement personnel or any other person; or

(vii) obstruct an ongoing criminal investigation by the agency that is the recipient of the request.

(d-5) A law enforcement record created for law enforcement purposes and contained in a shared electronic record management system if the law enforcement agency that is the recipient of the request did not create the record, did not participate in or have a role in any of the events which are the subject of the record, and only has access to the record through the shared electronic record management system.

(e) Records that relate to or affect the security of correctional institutions and detention facilities.

(e-5) Records requested by persons committed to the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail if those materials are available in the library of the correctional institution or facility or jail where the inmate is confined.

(e-6) Records requested by persons committed to the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail if those materials include records from staff members' personnel files, staff rosters, or other staffing assignment information.

(e-7) Records requested by persons committed to the

Department of Corrections or Department of Human Services Division of Mental Health if those materials are available through an administrative request to the Department of Corrections or Department of Human Services Division of Mental Health.

(e-8) Records requested by a person committed to the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail, the disclosure of which would result in the risk of harm to any person or the risk of an escape from a jail or correctional institution or facility.

(e-9) Records requested by a person in a county jail or committed to the Department of Corrections or Department of Human Services Division of Mental Health, containing personal information pertaining to the person's victim or the victim's family, including, but not limited to, a victim's home address, home telephone number, work or school address, work telephone number, social security number, or any other identifying information, except as may be relevant to a requester's current or potential case or claim.

(e-10) Law enforcement records of other persons requested by a person committed to the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail, including, but not limited to, arrest and booking records, mug shots, and crime scene photographs, except as these records may be relevant to the requester's current or potential case or claim.

(f) Preliminary drafts, notes, recommendations, memoranda and other records in which opinions are expressed, or policies or actions are formulated, except that a specific record or relevant portion of a record shall not be exempt when the record is publicly cited and identified by the head of the public body. The exemption provided in this paragraph (f) extends to all those records of officers and agencies of the General Assembly that pertain to the preparation of legislative documents.

(g) Trade secrets and commercial or financial information obtained from a person or business where the trade secrets or commercial or financial information are furnished under a claim that they are proprietary, privileged or confidential, and that disclosure of the trade secrets or commercial or financial information would cause competitive harm to the person or business, and only insofar as the claim directly applies to the records requested.

The information included under this exemption includes all trade secrets and commercial or financial information obtained by a public body, including a public pension fund, from a private equity fund or a privately held company within the investment portfolio of a private equity fund as a result of either investing or evaluating a potential investment of public funds in a private equity fund. The exemption contained in this item does not apply to the aggregate financial performance information of a private equity fund, nor to the identity of the fund's managers or general partners. The exemption contained in this item does not apply to the identity of a privately held company within the investment portfolio of a private equity fund, unless the disclosure of the identity of a privately held company may cause competitive harm.

Nothing contained in this paragraph (g) shall be construed to prevent a person or business from consenting to disclosure.

(h) Proposals and bids for any contract, grant, or agreement, including information which if it were disclosed would frustrate procurement or give an advantage to any person proposing to enter into a contractor agreement with the body, until an award or final selection is made. Information prepared by or for the body in preparation of a bid solicitation shall be exempt until an award or final selection is made.

(i) Valuable formulae, computer geographic systems,

designs, drawings and research data obtained or produced by any public body when disclosure could reasonably be expected to produce private gain or public loss. The exemption for "computer geographic systems" provided in this paragraph (i) does not extend to requests made by news media as defined in Section 2 of this Act when the requested information is not otherwise exempt and the only purpose of the request is to access and disseminate information regarding the health, safety, welfare, or legal rights of the general public.

(j) The following information pertaining to educational matters:

(i) test questions, scoring keys and other examination data used to administer an academic examination;

(ii) information received by a primary or secondary school, college, or university under its procedures for the evaluation of faculty members by their academic peers;

(iii) information concerning a school or university's adjudication of student disciplinary cases, but only to the extent that disclosure would unavoidably reveal the identity of the student; and

(iv) course materials or research materials used by faculty members.

(k) Architects' plans, engineers' technical submissions, and other construction related technical documents for projects not constructed or developed in whole or in part with public funds and the same for projects constructed or developed with public funds, including but not limited to power generating and distribution stations and other transmission and distribution facilities, water treatment facilities, airport facilities, sport stadiums, convention centers, and all government owned, operated, or occupied buildings, but only to the extent that disclosure would compromise security.

(l) Minutes of meetings of public bodies closed to the public as provided in the Open Meetings Act until the public body makes the minutes available to the public under Section 2.06 of the Open Meetings Act.

(m) Communications between a public body and an attorney or auditor representing the public body that would not be subject to discovery in litigation, and materials prepared or compiled by or for a public body in anticipation of a criminal, civil or administrative proceeding upon the request of an attorney advising the public body, and materials prepared or compiled with respect to internal audits of public bodies.

(n) Records relating to a public body's adjudication of employee grievances or disciplinary cases; however, this exemption shall not extend to the final outcome of cases in which discipline is imposed.

(o) Administrative or technical information associated with automated data processing operations, including but not limited to software, operating protocols, computer program abstracts, file layouts, source listings, object modules, load modules, user guides, documentation pertaining to all logical and physical design of computerized systems, employee manuals, and any other information that, if disclosed, would jeopardize the security of the system or its data or the security of materials exempt under this Section.

(p) Records relating to collective negotiating matters between public bodies and their employees or representatives, except that any final contract or agreement shall be subject to inspection and copying.

(q) Test questions, scoring keys, and other examination data used to determine the qualifications of an applicant for a license or employment.

(r) The records, documents, and information relating to real estate purchase negotiations until those negotiations have been completed or otherwise terminated. With regard to a parcel involved in a pending or actually and reasonably contemplated eminent domain proceeding under the Eminent

Domain Act, records, documents and information relating to that parcel shall be exempt except as may be allowed under discovery rules adopted by the Illinois Supreme Court. The records, documents and information relating to a real estate sale shall be exempt until a sale is consummated.

(s) Any and all proprietary information and records related to the operation of an intergovernmental risk management association or self-insurance pool or jointly self-administered health and accident cooperative or pool. Insurance or self insurance (including any intergovernmental risk management association or self insurance pool) claims, loss or risk management information, records, data, advice or communications.

(t) Information contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of a public body responsible for the regulation or supervision of financial institutions or insurance companies, unless disclosure is otherwise required by State law.

(u) Information that would disclose or might lead to the disclosure of secret or confidential information, codes, algorithms, programs, or private keys intended to be used to create electronic or digital signatures under the Electronic Commerce Security Act.

(v) Vulnerability assessments, security measures, and response policies or plans that are designed to identify, prevent, or respond to potential attacks upon a community's population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community, but only to the extent that disclosure could reasonably be expected to jeopardize the effectiveness of the measures or the safety of the personnel who implement them or the public. Information exempt under this item may include such things as details pertaining to the mobilization or deployment of personnel or equipment, to the operation of communication systems or protocols, or to tactical operations.

(w) (Blank).

(x) Maps and other records regarding the location or security of generation, transmission, distribution, storage, gathering, treatment, or switching facilities owned by a utility, by a power generator, or by the Illinois Power Agency.

(y) Information contained in or related to proposals, bids, or negotiations related to electric power procurement under Section 1-75 of the Illinois Power Agency Act and Section 16-111.5 of the Public Utilities Act that is determined to be confidential and proprietary by the Illinois Power Agency or by the Illinois Commerce Commission.

(z) Information about students exempted from disclosure under Sections 10-20.38 or 34-18.29 of the School Code, and information about undergraduate students enrolled at an institution of higher education exempted from disclosure under Section 25 of the Illinois Credit Card Marketing Act of 2009.

(aa) Information the disclosure of which is exempted under the Viatical Settlements Act of 2009.

(bb) Records and information provided to a mortality review team and records maintained by a mortality review team appointed under the Department of Juvenile Justice Mortality Review Team Act.

(cc) Information regarding interments, entombments, or inurnments of human remains that are submitted to the Cemetery Oversight Database under the Cemetery Care Act or the Cemetery Oversight Act, whichever is applicable.

(dd) Correspondence and records (i) that may not be disclosed under Section 11-9 of the Illinois Public Aid Code or (ii) that pertain to appeals under Section 11-8 of the Illinois Public Aid Code.

(ee) The names, addresses, or other personal information of persons who are minors and are also participants and registrants in programs of park districts, forest preserve districts, conservation districts, recreation agencies, and special recreation associations.

(ff) The names, addresses, or other personal information of participants and registrants in programs of park districts, forest preserve districts, conservation districts, recreation agencies, and special recreation associations where such programs are targeted primarily to minors.

(gg) Confidential information described in Section 1-100 of the Illinois Independent Tax Tribunal Act of 2012.

(hh) The report submitted to the State Board of Education by the School Security and Standards Task Force under item (8) of subsection (d) of Section 2-3.160 of the School Code and any information contained in that report.

(ii) Records requested by persons committed to or detained by the Department of Human Services under the Sexually Violent Persons Commitment Act or committed to the Department of Corrections under the Sexually Dangerous Persons Act if those materials: (i) are available in the library of the facility where the individual is confined; (ii) include records from staff members' personnel files, staff rosters, or other staffing assignment information; or (iii) are available through an administrative request to the Department of Human Services or the Department of Corrections.

(jj) Confidential information described in Section 5-535 of the Civil Administrative Code of Illinois.

(kk) Records concerning the work of the threat assessment team of a school district.

(1.5) Any information exempt from disclosure under the Judicial Privacy Act shall be redacted from public records prior to disclosure under this Act.

(2) A public record that is not in the possession of a public body but is in the possession of a party with whom the agency has contracted to perform a governmental function on behalf of the public body, and that directly relates to the governmental function and is not otherwise exempt under this Act, shall be considered a public record of the public body, for purposes of this Act.

(3) This Section does not authorize withholding of information or limit the availability of records to the public, except as stated in this Section or otherwise provided in this Act.

(Source: P.A. 100-26, eff. 8-4-17; 100-201, eff. 8-18-17; 100-732, eff. 8-3-18; 101-455, eff. 8-23-19.)

(5 ILCS 140/7.1)

Sec. 7.1. (Repealed).

(Source: P.A. 95-331, eff. 8-21-07. Repealed by P.A. 96-542, eff. 1-1-10.)

(5 ILCS 140/7.5)

(Text of Section from P.A. 101-600)

Sec. 7.5. Statutory exemptions. To the extent provided for by the statutes referenced below, the following shall be exempt from inspection and copying:

(a) All information determined to be confidential under Section 4002 of the Technology Advancement and Development Act.

(b) Library circulation and order records identifying library users with specific materials under the Library Records Confidentiality Act.

(c) Applications, related documents, and medical records received by the Experimental Organ Transplantation Procedures Board and any and all documents or other records prepared by the Experimental Organ

Transplantation Procedures Board or its staff relating to applications it has received.

(d) Information and records held by the Department of Public Health and its authorized representatives relating to known or suspected cases of sexually transmissible disease or any information the disclosure of which is restricted under the Illinois Sexually Transmissible Disease Control Act.

(e) Information the disclosure of which is exempted under Section 30 of the Radon Industry Licensing Act.

(f) Firm performance evaluations under Section 55 of the Architectural, Engineering, and Land Surveying Qualifications Based Selection Act.

(g) Information the disclosure of which is restricted and exempted under Section 50 of the Illinois Prepaid Tuition Act.

(h) Information the disclosure of which is exempted under the State Officials and Employees Ethics Act, and records of any lawfully created State or local inspector general's office that would be exempt if created or obtained by an Executive Inspector General's office under that Act.

(i) Information contained in a local emergency energy plan submitted to a municipality in accordance with a local emergency energy plan ordinance that is adopted under Section 11-21.5-5 of the Illinois Municipal Code.

(j) Information and data concerning the distribution of surcharge moneys collected and remitted by carriers under the Emergency Telephone System Act.

(k) Law enforcement officer identification information or driver identification information compiled by a law enforcement agency or the Department of Transportation under Section 11-212 of the Illinois Vehicle Code.

(l) Records and information provided to a residential health care facility resident sexual assault and death review team or the Executive Council under the Abuse Prevention Review Team Act.

(m) Information provided to the predatory lending database created pursuant to Article 3 of the Residential Real Property Disclosure Act, except to the extent authorized under that Article.

(n) Defense budgets and petitions for certification of compensation and expenses for court appointed trial counsel as provided under Sections 10 and 15 of the Capital Crimes Litigation Act. This subsection (n) shall apply until the conclusion of the trial of the case, even if the prosecution chooses not to pursue the death penalty prior to trial or sentencing.

(o) Information that is prohibited from being disclosed under Section 4 of the Illinois Health and Hazardous Substances Registry Act.

(p) Security portions of system safety program plans, investigation reports, surveys, schedules, lists, data, or information compiled, collected, or prepared by or for the Regional Transportation Authority under Section 2.11 of the Regional Transportation Authority Act or the St. Clair County Transit District under the Bi-State Transit Safety Act.

(q) Information prohibited from being disclosed by the Personnel Record Review Act.

(r) Information prohibited from being disclosed by the Illinois School Student Records Act.

(s) Information the disclosure of which is restricted under Section 5-108 of the Public Utilities Act.

(t) All identified or deidentified health information in the form of health data or medical records contained in, stored in, submitted to, transferred by, or released from the Illinois Health Information Exchange, and

identified or deidentified health information in the form of health data and medical records of the Illinois Health Information Exchange in the possession of the Illinois Health Information Exchange Authority due to its administration of the Illinois Health Information Exchange. The terms "identified" and "deidentified" shall be given the same meaning as in the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, or any subsequent amendments thereto, and any regulations promulgated thereunder.

(u) Records and information provided to an independent team of experts under the Developmental Disability and Mental Health Safety Act (also known as Brian's Law).

(v) Names and information of people who have applied for or received Firearm Owner's Identification Cards under the Firearm Owners Identification Card Act or applied for or received a concealed carry license under the Firearm Concealed Carry Act, unless otherwise authorized by the Firearm Concealed Carry Act; and databases under the Firearm Concealed Carry Act, records of the Concealed Carry Licensing Review Board under the Firearm Concealed Carry Act, and law enforcement agency objections under the Firearm Concealed Carry Act.

(w) Personally identifiable information which is exempted from disclosure under subsection (g) of Section 19.1 of the Toll Highway Act.

(x) Information which is exempted from disclosure under Section 5-1014.3 of the Counties Code or Section 8-11-21 of the Illinois Municipal Code.

(y) Confidential information under the Adult Protective Services Act and its predecessor enabling statute, the Elder Abuse and Neglect Act, including information about the identity and administrative finding against any caregiver of a verified and substantiated decision of abuse, neglect, or financial exploitation of an eligible adult maintained in the Registry established under Section 7.5 of the Adult Protective Services Act.

(z) Records and information provided to a fatality review team or the Illinois Fatality Review Team Advisory Council under Section 15 of the Adult Protective Services Act.

(aa) Information which is exempted from disclosure under Section 2.37 of the Wildlife Code.

(bb) Information which is or was prohibited from disclosure by the Juvenile Court Act of 1987.

(cc) Recordings made under the Law Enforcement Officer-Worn Body Camera Act, except to the extent authorized under that Act.

(dd) Information that is prohibited from being disclosed under Section 45 of the Condominium and Common Interest Community Ombudsperson Act.

(ee) Information that is exempted from disclosure under Section 30.1 of the Pharmacy Practice Act.

(ff) Information that is exempted from disclosure under the Revised Uniform Unclaimed Property Act.

(gg) Information that is prohibited from being disclosed under Section 7-603.5 of the Illinois Vehicle Code.

(hh) Records that are exempt from disclosure under Section 1A-16.7 of the Election Code.

(ii) Information which is exempted from disclosure under Section 2505-800 of the Department of Revenue Law of the Civil Administrative Code of Illinois.

(jj) Information and reports that are required to be

submitted to the Department of Labor by registering day and temporary labor service agencies but are exempt from disclosure under subsection (a-1) of Section 45 of the Day and Temporary Labor Services Act.

(kk) Information prohibited from disclosure under the Seizure and Forfeiture Reporting Act.

(ll) Information the disclosure of which is restricted and exempted under Section 5-30.8 of the Illinois Public Aid Code.

(mm) Records that are exempt from disclosure under Section 4.2 of the Crime Victims Compensation Act.

(nn) Information that is exempt from disclosure under Section 70 of the Higher Education Student Assistance Act.

(oo) Communications, notes, records, and reports arising out of a peer support counseling session prohibited from disclosure under the First Responders Suicide Prevention Act.

(pp) Names and all identifying information relating to an employee of an emergency services provider or law enforcement agency under the First Responders Suicide Prevention Act.

(qq) Information and records held by the Department of Public Health and its authorized representatives collected under the Reproductive Health Act.

(rr) Information that is exempt from disclosure under the Cannabis Regulation and Tax Act.

(ss) Data reported by an employer to the Department of Human Rights pursuant to Section 2-108 of the Illinois Human Rights Act.

(tt) Recordings made under the Children's Advocacy Center Act, except to the extent authorized under that Act.

(uu) Information that is exempt from disclosure under Section 50 of the Sexual Assault Evidence Submission Act.

(vv) Information that is exempt from disclosure under subsections (f) and (j) of Section 5-36 of the Illinois Public Aid Code.

(ww) Information that is exempt from disclosure under Section 16.8 of the State Treasurer Act.

(xx) Information that is exempt from disclosure or information that shall not be made public under the Illinois Insurance Code.

(Source: P.A. 100-20, eff. 7-1-17; 100-22, eff. 1-1-18; 100-201, eff. 8-18-17; 100-373, eff. 1-1-18; 100-464, eff. 8-28-17; 100-465, eff. 8-31-17; 100-512, eff. 7-1-18; 100-517, eff. 6-1-18; 100-646, eff. 7-27-18; 100-690, eff. 1-1-19; 100-863, eff. 8-14-18; 100-887, eff. 8-14-18; 101-13, eff. 6-12-19; 101-27, eff. 6-25-19; 101-81, eff. 7-12-19; 101-221, eff. 1-1-20; 101-236, eff. 1-1-20; 101-375, eff. 8-16-19; 101-377, eff. 8-16-19; 101-452, eff. 1-1-20; 101-466, eff. 1-1-20; 101-600, eff. 12-6-19.)

(Text of Section from P.A. 101-620)

Sec. 7.5. Statutory exemptions. To the extent provided for by the statutes referenced below, the following shall be exempt from inspection and copying:

(a) All information determined to be confidential under Section 4002 of the Technology Advancement and Development Act.

(b) Library circulation and order records identifying library users with specific materials under the Library Records Confidentiality Act.

(c) Applications, related documents, and medical records received by the Experimental Organ Transplantation Procedures Board and any and all documents or other records prepared by the Experimental Organ Transplantation Procedures Board or its staff relating to applications it has received.

(d) Information and records held by the Department of

Public Health and its authorized representatives relating to known or suspected cases of sexually transmissible disease or any information the disclosure of which is restricted under the Illinois Sexually Transmissible Disease Control Act.

(e) Information the disclosure of which is exempted under Section 30 of the Radon Industry Licensing Act.

(f) Firm performance evaluations under Section 55 of the Architectural, Engineering, and Land Surveying Qualifications Based Selection Act.

(g) Information the disclosure of which is restricted and exempted under Section 50 of the Illinois Prepaid Tuition Act.

(h) Information the disclosure of which is exempted under the State Officials and Employees Ethics Act, and records of any lawfully created State or local inspector general's office that would be exempt if created or obtained by an Executive Inspector General's office under that Act.

(i) Information contained in a local emergency energy plan submitted to a municipality in accordance with a local emergency energy plan ordinance that is adopted under Section 11-21.5-5 of the Illinois Municipal Code.

(j) Information and data concerning the distribution of surcharge moneys collected and remitted by carriers under the Emergency Telephone System Act.

(k) Law enforcement officer identification information or driver identification information compiled by a law enforcement agency or the Department of Transportation under Section 11-212 of the Illinois Vehicle Code.

(l) Records and information provided to a residential health care facility resident sexual assault and death review team or the Executive Council under the Abuse Prevention Review Team Act.

(m) Information provided to the predatory lending database created pursuant to Article 3 of the Residential Real Property Disclosure Act, except to the extent authorized under that Article.

(n) Defense budgets and petitions for certification of compensation and expenses for court appointed trial counsel as provided under Sections 10 and 15 of the Capital Crimes Litigation Act. This subsection (n) shall apply until the conclusion of the trial of the case, even if the prosecution chooses not to pursue the death penalty prior to trial or sentencing.

(o) Information that is prohibited from being disclosed under Section 4 of the Illinois Health and Hazardous Substances Registry Act.

(p) Security portions of system safety program plans, investigation reports, surveys, schedules, lists, data, or information compiled, collected, or prepared by or for the Regional Transportation Authority under Section 2.11 of the Regional Transportation Authority Act or the St. Clair County Transit District under the Bi-State Transit Safety Act.

(q) Information prohibited from being disclosed by the Personnel Record Review Act.

(r) Information prohibited from being disclosed by the Illinois School Student Records Act.

(s) Information the disclosure of which is restricted under Section 5-108 of the Public Utilities Act.

(t) All identified or deidentified health information in the form of health data or medical records contained in, stored in, submitted to, transferred by, or released from the Illinois Health Information Exchange, and identified or deidentified health information in the form of health data and medical records of the Illinois Health Information Exchange in the possession of the Illinois Health Information Exchange Authority due to its administration of the Illinois

Health Information Exchange. The terms "identified" and "deidentified" shall be given the same meaning as in the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, or any subsequent amendments thereto, and any regulations promulgated thereunder.

(u) Records and information provided to an independent team of experts under the Developmental Disability and Mental Health Safety Act (also known as Brian's Law).

(v) Names and information of people who have applied for or received Firearm Owner's Identification Cards under the Firearm Owners Identification Card Act or applied for or received a concealed carry license under the Firearm Concealed Carry Act, unless otherwise authorized by the Firearm Concealed Carry Act; and databases under the Firearm Concealed Carry Act, records of the Concealed Carry Licensing Review Board under the Firearm Concealed Carry Act, and law enforcement agency objections under the Firearm Concealed Carry Act.

(w) Personally identifiable information which is exempted from disclosure under subsection (g) of Section 19.1 of the Toll Highway Act.

(x) Information which is exempted from disclosure under Section 5-1014.3 of the Counties Code or Section 8-11-21 of the Illinois Municipal Code.

(y) Confidential information under the Adult Protective Services Act and its predecessor enabling statute, the Elder Abuse and Neglect Act, including information about the identity and administrative finding against any caregiver of a verified and substantiated decision of abuse, neglect, or financial exploitation of an eligible adult maintained in the Registry established under Section 7.5 of the Adult Protective Services Act.

(z) Records and information provided to a fatality review team or the Illinois Fatality Review Team Advisory Council under Section 15 of the Adult Protective Services Act.

(aa) Information which is exempted from disclosure under Section 2.37 of the Wildlife Code.

(bb) Information which is or was prohibited from disclosure by the Juvenile Court Act of 1987.

(cc) Recordings made under the Law Enforcement Officer-Worn Body Camera Act, except to the extent authorized under that Act.

(dd) Information that is prohibited from being disclosed under Section 45 of the Condominium and Common Interest Community Ombudsperson Act.

(ee) Information that is exempted from disclosure under Section 30.1 of the Pharmacy Practice Act.

(ff) Information that is exempted from disclosure under the Revised Uniform Unclaimed Property Act.

(gg) Information that is prohibited from being disclosed under Section 7-603.5 of the Illinois Vehicle Code.

(hh) Records that are exempt from disclosure under Section 1A-16.7 of the Election Code.

(ii) Information which is exempted from disclosure under Section 2505-800 of the Department of Revenue Law of the Civil Administrative Code of Illinois.

(jj) Information and reports that are required to be submitted to the Department of Labor by registering day and temporary labor service agencies but are exempt from disclosure under subsection (a-1) of Section 45 of the Day and Temporary Labor Services Act.

(kk) Information prohibited from disclosure under the Seizure and Forfeiture Reporting Act.

(ll) Information the disclosure of which is restricted and exempted under Section 5-30.8 of the Illinois Public Aid Code.

(mm) Records that are exempt from disclosure under Section 4.2 of the Crime Victims Compensation Act.

(nn) Information that is exempt from disclosure under Section 70 of the Higher Education Student Assistance Act.

(oo) Information prohibited from being disclosed under the Illinois Educational Labor Relations Act.

(pp) Information prohibited from being disclosed under the Illinois Public Labor Relations Act.

(qq) Information prohibited from being disclosed under Section 1-167 of the Illinois Pension Code.

(Source: P.A. 100-20, eff. 7-1-17; 100-22, eff. 1-1-18; 100-201, eff. 8-18-17; 100-373, eff. 1-1-18; 100-464, eff. 8-28-17; 100-465, eff. 8-31-17; 100-512, eff. 7-1-18; 100-517, eff. 6-1-18; 100-646, eff. 7-27-18; 100-690, eff. 1-1-19; 100-863, eff. 8-14-18; 100-887, eff. 8-14-18; 101-620, eff. 12-20-19.)

(5 ILCS 140/7.6)

Sec. 7.6. (Repealed).

(Source: P.A. 100-555, eff. 11-16-17. Repealed by P.A. 100-731, eff. 1-1-19.)

(5 ILCS 140/8)

Sec. 8. (Repealed).

(Source: P.A. 85-1357. Repealed by P.A. 96-542, eff. 1-1-10.)

(5 ILCS 140/8.5)

Sec. 8.5. Records maintained online.

(a) Notwithstanding any provision of this Act to the contrary, a public body is not required to copy a public record that is published on the public body's website. The public body shall notify the requester that the public record is available online and direct the requester to the website where the record can be reasonably accessed.

(b) If the person requesting the public record is unable to reasonably access the record online after being directed to the website pursuant to subsection (a) of this Section, the requester may re-submit his or her request for the record stating his or her inability to reasonably access the record online, and the public body shall make the requested record available for inspection or copying as provided in Section 3 of this Act.

(Source: P.A. 98-1129, eff. 12-3-14.)

(5 ILCS 140/9) (from Ch. 116, par. 209)

Sec. 9. (a) Each public body denying a request for public records shall notify the requester in writing of the decision to deny the request, the reasons for the denial, including a detailed factual basis for the application of any exemption claimed, and the names and titles or positions of each person responsible for the denial. Each notice of denial by a public body shall also inform such person of the right to review by the Public Access Counselor and provide the address and phone number for the Public Access Counselor. Each notice of denial shall inform such person of his right to judicial review under Section 11 of this Act.

(b) When a request for public records is denied on the grounds that the records are exempt under Section 7 of this Act, the notice of denial shall specify the exemption claimed to authorize the denial and the specific reasons for the denial, including a detailed factual basis and a citation to supporting legal authority. Copies

of all notices of denial shall be retained by each public body in a single central office file that is open to the public and indexed according to the type of exemption asserted and, to the extent feasible, according to the types of records requested.

(c) Any person making a request for public records shall be deemed to have exhausted his or her administrative remedies with respect to that request if the public body fails to act within the time periods provided in Section 3 of this Act. (Source: P.A. 96-542, eff. 1-1-10.)

(5 ILCS 140/9.5)

Sec. 9.5. Public Access Counselor; opinions.

(a) A person whose request to inspect or copy a public record is denied by a public body, except the General Assembly and committees, commissions, and agencies thereof, may file a request for review with the Public Access Counselor established in the Office of the Attorney General not later than 60 days after the date of the final denial. The request for review must be in writing, signed by the requester, and include (i) a copy of the request for access to records and (ii) any responses from the public body.

(b) A person whose request to inspect or copy a public record is made for a commercial purpose as defined in subsection (c-10) of Section 2 of this Act may not file a request for review with the Public Access Counselor. A person whose request to inspect or copy a public record was treated by the public body as a request for a commercial purpose under Section 3.1 of this Act may file a request for review with the Public Access Counselor for the limited purpose of reviewing whether the public body properly determined that the request was made for a commercial purpose.

(b-5) A person whose request to inspect or copy a public record was treated by a public body, except the General Assembly and committees, commissions, and agencies thereof, as a voluminous request under Section 3.6 of this Act may file a request for review with the Public Access Counselor for the purpose of reviewing whether the public body properly determined that the request was a voluminous request.

(c) Upon receipt of a request for review, the Public Access Counselor shall determine whether further action is warranted. If the Public Access Counselor determines that the alleged violation is unfounded, he or she shall so advise the requester and the public body and no further action shall be undertaken. In all other cases, the Public Access Counselor shall forward a copy of the request for review to the public body within 7 business days after receipt and shall specify the records or other documents that the public body shall furnish to facilitate the review. Within 7 business days after receipt of the request for review, the public body shall provide copies of records requested and shall otherwise fully cooperate with the Public Access Counselor. If a public body fails to furnish specified records pursuant to this Section, or if otherwise necessary, the Attorney General may issue a subpoena to any person or public body having knowledge of or records pertaining to a request for review of a denial of access to records under the Act. To the extent that records or documents produced by a public body contain information that is claimed to be exempt from disclosure under Section 7 of this Act, the Public Access Counselor shall not further disclose that information.

(d) Within 7 business days after it receives a copy of a request for review and request for production of records from the Public Access Counselor, the public body may, but is not required to, answer the allegations of the request for review. The answer may take the form of a letter, brief, or memorandum. The Public Access Counselor shall forward a copy of the answer to the person submitting the request for review, with any alleged confidential information to which the request pertains redacted from the copy. The requester may, but is not required to, respond in writing to the answer within 7 business days and shall provide a copy of the response to the public body.

(e) In addition to the request for review, and the answer and the response thereto, if any, a requester or a public body may furnish affidavits or records concerning any matter germane to the review.

(f) Unless the Public Access Counselor extends the time by no more than 30 business days by sending written notice to the requester and the public body that includes a statement of the reasons for the extension in the notice, or decides to address the matter without the issuance of a binding opinion, the Attorney General shall examine the issues and the records, shall make findings of fact and conclusions of law, and shall issue to the requester and the public body an opinion in response to the request for review within 60 days after its receipt. The opinion shall be binding upon both the requester and the public body, subject to administrative review under Section 11.5.

In responding to any request under this Section 9.5, the Attorney General may exercise his or her discretion and choose to resolve a request for review by mediation or by a means other than the issuance of a binding opinion. The decision not to issue a binding opinion shall not be reviewable.

Upon receipt of a binding opinion concluding that a violation of this Act has occurred, the public body shall either take necessary action immediately to comply with the directive of the opinion or shall initiate administrative review under Section 11.5. If the opinion concludes that no violation of the Act has occurred, the requester may initiate administrative review under Section 11.5.

A public body that discloses records in accordance with an opinion of the Attorney General is immune from all liabilities by reason thereof and shall not be liable for penalties under this Act.

(g) If the requester files suit under Section 11 with respect to the same denial that is the subject of a pending request for review, the requester shall notify the Public Access Counselor, and the Public Access Counselor shall take no further action with respect to the request for review and shall so notify the public body.

(h) The Attorney General may also issue advisory opinions to public bodies regarding compliance with this Act. A review may be initiated upon receipt of a written request from the head of the public body or its attorney, which shall contain sufficient accurate facts from which a determination can be made. The Public Access Counselor may request additional information from the public body in order to assist in the review. A public body that relies in good faith on an advisory opinion of the Attorney General in responding to a request is not liable for penalties under this Act, so long as the facts upon which the opinion is based have been fully and fairly disclosed to the Public Access Counselor.

(Source: P.A. 97-579, eff. 8-26-11; 98-1129, eff. 12-3-14.)

(5 ILCS 140/10)

Sec. 10. (Repealed).

(Source: P.A. 83-1013. Repealed by P.A. 96-542, eff. 1-1-10.)

(5 ILCS 140/11) (from Ch. 116, par. 211)

Sec. 11. (a) Any person denied access to inspect or copy any public record by a public body may file suit for injunctive or declaratory relief.

(a-5) In accordance with Section 11.6 of this Act, a requester may file an action to enforce a binding opinion issued under Section 9.5 of this Act.

(b) Where the denial is from a public body of the State, suit may be filed in the circuit court for the county where the public body has its principal office or where the person denied access resides.

(c) Where the denial is from a municipality or other public body, except as provided in subsection (b) of this Section, suit may be filed in the circuit court for the county where the public body is located.

(d) The circuit court shall have the jurisdiction to enjoin the public body from withholding public records and to order the production of any public records improperly withheld from the person seeking access. If the public body can show that exceptional circumstances exist, and that the body is exercising due diligence in responding to the request, the court may retain jurisdiction and allow the agency additional time to complete its review of the records.

(e) On motion of the plaintiff, prior to or after in camera inspection, the court shall order the public body to provide an index of the records to which access has been denied. The index shall include the following:

(i) A description of the nature or contents of each document withheld, or each deletion from a released document, provided, however, that the public body shall not be required to disclose the information which it asserts is exempt; and

(ii) A statement of the exemption or exemptions claimed for each such deletion or withheld document.

(f) In any action considered by the court, the court shall consider the matter de novo, and shall conduct such in camera examination of the requested records as it finds appropriate to determine if such records or any part thereof may be withheld under any provision of this Act. The burden shall be on the public body to establish that its refusal to permit public inspection or copying is in accordance with the provisions of this Act. Any public body that asserts that a record is exempt from disclosure has the burden of proving that it is exempt by clear and convincing evidence.

(g) In the event of noncompliance with an order of the court to disclose, the court may enforce its order against any public official or employee so ordered or primarily responsible for such noncompliance through the court's contempt powers.

(h) Except as to causes the court considers to be of greater importance, proceedings arising under this Section shall take precedence on the docket over all other causes and be assigned for hearing and trial at the earliest practicable date and expedited in every way.

(i) If a person seeking the right to inspect or receive a copy of a public record prevails in a proceeding under this Section, the court shall award such person reasonable attorney's fees and costs. In determining what amount of attorney's fees is reasonable, the court shall consider the degree to which the relief obtained relates to the relief sought. The changes contained in this subsection apply to an action filed on or after January 1, 2010 (the effective date of Public Act 96-542).

(j) If the court determines that a public body willfully and intentionally failed to comply with this Act, or otherwise acted in bad faith, the court shall also impose upon the public body a civil penalty of not less than $2,500 nor more than $5,000 for each occurrence. In assessing the civil penalty, the court shall consider in aggravation or mitigation the budget of the public body and whether the public body has previously been assessed penalties for violations of this Act. The court may impose an additional penalty of up to $1,000 for each day the violation continues if:

(1) the public body fails to comply with the court's order after 30 days;

(2) the court's order is not on appeal or stayed; and

(3) the court does not grant the public body additional time to comply with the court's order to disclose public records.

The changes contained in this subsection made by Public Act 96-542 apply to an action filed on or after January 1, 2010 (the effective date of Public Act 96-542).

(k) The changes to this Section made by this amendatory Act of the 99th General Assembly apply to actions filed on or after the effective date of this amendatory Act of the 99th General Assembly.

(Source: P.A. 99-586, eff. 1-1-17; 99-642, eff. 7-28-16.)

(5 ILCS 140/11.5)
Sec. 11.5. Administrative review. A binding opinion issued by the Attorney General shall be considered a final decision of an administrative agency, for purposes of administrative review under the Administrative Review Law (735 ILCS 5/Art. III). An action for administrative review of a binding opinion of the Attorney General shall be commenced in Cook or Sangamon County. An advisory opinion issued to a public body shall not be considered a final decision of the Attorney General for purposes of this Section.
(Source: P.A. 96-542, eff. 1-1-10.)

(5 ILCS 140/11.6)
Sec. 11.6. Noncompliance with binding opinion.
(a) The requester may file an action under Section 11 and there shall be a rebuttable presumption that the public body willfully and intentionally failed to comply with this Act for purposes of subsection (j) of Section 11 if:
(1) the Attorney General issues a binding opinion pursuant to Section 9.5;
(2) the public body does not file for administrative review of the binding opinion within 35 days after the binding opinion is served on the public body; and
(3) the public body does not comply with the binding opinion within 35 days after the binding opinion is served on the public body.
For purposes of this subsection (a), service of the binding opinion shall be by personal delivery or by depositing the opinion in the United States mail as provided in Section 3-103 of the Code of Civil Procedure.
(b) The presumption in subsection (a) may be rebutted by the public body showing that it is making a good faith effort to comply with the binding opinion, but compliance was not possible within the 35-day time frame.
(c) This Section applies to binding opinions of the Attorney General requested or issued on or after the effective date of this amendatory Act of the 99th General Assembly.
(Source: P.A. 99-586, eff. 1-1-17.)

Illinois Personal Information Protection Act (815 ILCS 530/)

(815 ILCS 530/1)
Sec. 1. Short title. This Act may be cited as the Personal Information Protection Act.
(Source: P.A. 94-36, eff. 1-1-06.)

(815 ILCS 530/5)
Sec. 5. Definitions. In this Act:
"Data collector" may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial

institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

"Breach of the security of the system data" or "breach" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. "Breach of the security of the system data" does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

"Health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any medical information in an individual's health insurance application and claims history, including any appeals records.

"Medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional, including such information provided to a website or mobile application.

"Personal information" means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security:

(A) Social Security number.

(B) Driver's license number or State identification card number.

(C) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

(2) User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.

(Source: P.A. 99-503, eff. 1-1-17.)

(815 ILCS 530/10)

Sec. 10. Notice of breach; notice to Attorney General.

(a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of

the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows:

(1) With respect to personal information as defined in Section 5 in paragraph (1) of the definition of "personal information":

(A) the toll-free numbers and addresses for consumer reporting agencies;

(B) the toll-free number, address, and website address for the Federal Trade Commission; and

(C) a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

(2) With respect to personal information defined in Section 5 in paragraph (2) of the definition of "personal information", notice may be provided in electronic or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.

The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

(b) Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

(b-5) The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

(c) For purposes of this Section, notice to consumers may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the data collector demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the data collector has an email address for the subject persons; (ii) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and (iii) notification to

major statewide media or, if the breach impacts residents in one geographic area, to prominent local media in areas where affected individuals are likely to reside if such notice is reasonably calculated to give actual notice to persons whom notice is required.

(d) Notwithstanding any other subsection in this Section, a data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.

(e)(1) This subsection does not apply to data collectors that are covered entities or business associates and are in compliance with Section 50.

(2) Any data collector required to issue notice pursuant to this Section to more than 500 Illinois residents as a result of a single breach of the security system shall provide notice to the Attorney General of the breach, including:

(A) A description of the nature of the breach of security or unauthorized acquisition or use.

(B) The number of Illinois residents affected by such incident at the time of notification.

(C) Any steps the data collector has taken or plans to take relating to the incident.

Such notification must be made in the most expedient time possible and without unreasonable delay but in no event later than when the data collector provides notice to consumers pursuant to this Section. If the date of the breach is unknown at the time the notice is sent to the Attorney General, the data collector shall send the Attorney General the date of the breach as soon as possible.

Upon receiving notification from a data collector of a breach of personal information, the Attorney General may publish the name of the data collector that suffered the breach, the types of personal information compromised in the breach, and the date range of the breach.

(Source: P.A. 100-201, eff. 8-18-17; 101-343, eff. 1-1-20.)

(815 ILCS 530/12)

Sec. 12. Notice of breach; State agency.

(a) Any State agency that collects personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data or written material following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to information as follows:

(1) With respect to personal information defined in Section 5 in paragraph (1) of the definition of "personal information":

(i) the toll-free numbers and addresses for consumer reporting agencies;

(ii) the toll-free number, address, and website address for the Federal Trade Commission; and

(iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

(2) With respect to personal information as defined in Section 5 in paragraph (2) of the definition of "personal information", notice may be provided in electronic or other form directing the Illinois resident whose

personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.

The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

(a-5) The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the State agency with a written request for the delay. However, the State agency must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

(b) For purposes of this Section, notice to residents may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the State agency demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the State agency does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the State agency has an email address for the subject persons; (ii) conspicuous posting of the notice on the State agency's web site page if the State agency maintains one; and (iii) notification to major statewide media.

(c) Notwithstanding subsection (b), a State agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act shall be deemed in compliance with the notification requirements of this Section if the State agency notifies subject persons in accordance with its policies in the event of a breach of the security of the system data or written material.

(d) If a State agency is required to notify more than 1,000 persons of a breach of security pursuant to this Section, the State agency shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. Section 1681a(p), of the timing, distribution, and content of the notices. Nothing in this subsection (d) shall be construed to require the State agency to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients.

(e) Notice to Attorney General. Any State agency that suffers a single breach of the security of the data concerning the personal information of more than 250 Illinois residents shall provide notice to the Attorney General of the breach, including:

(A) The types of personal information compromised in the breach.

(B) The number of Illinois residents affected by such incident at the time of notification.

(C) Any steps the State agency has taken or plans to take relating to notification of the breach to consumers.

(D) The date and timeframe of the breach, if known at the time notification is provided.

Such notification must be made within 45 days of the State agency's discovery of the security breach or when the State agency provides any notice to consumers required by this Section, whichever is sooner, unless the State agency has good cause for reasonable delay to determine the scope of the breach and restore the integrity, security, and confidentiality of the data system, or when law enforcement

requests in writing to withhold disclosure of some or all of the information required in the notification under this Section. If the date or timeframe of the breach is unknown at the time the notice is sent to the Attorney General, the State agency shall send the Attorney General the date or timeframe of the breach as soon as possible.

(f) In addition to the report required by Section 25 of this Act, if the State agency that suffers a breach determines the identity of the actor who perpetrated the breach, then the State agency shall report this information, within 5 days after the determination, to the General Assembly, provided that such report would not jeopardize the security of Illinois residents or compromise a security investigation.

(g) A State agency directly responsible to the Governor that has been subject to or has reason to believe it has been subject to a single breach of the security of the data concerning the personal information of more than 250 Illinois residents or an instance of aggravated computer tampering, as defined in Section 17-53 of the Criminal Code of 2012, shall notify the Office of the Chief Information Security Officer of the Illinois Department of Innovation and Technology and the Attorney General regarding the breach or instance of aggravated computer tampering. The notification shall be made without delay, but no later than 72 hours following the discovery of the incident.

Upon receiving notification of such incident, the Chief Information Security Officer shall without delay take necessary and reasonable actions to:

(i) assess the incident to determine the potential impact on the overall confidentiality, security, and availability of State of Illinois data and information systems;

(ii) ensure the security incident is contained to minimize additional impact and risk to the State;

(iii) identify the root cause of the incident;

(iv) provide recommendations to the impacted State agency to assist with eradicating the threat and removing and mitigating any vulnerabilities to reduce the risk of further compromise; and

(v) assist the impacted State agency in any necessary recovery efforts to ensure effective return to a state of normal operations.

The Department of Innovation and Technology may agree to submit the reports required in subsections (e) and (f) of this Section and in Section 25 in lieu of the impacted agency.

(h) Upon receiving notification from a State agency of a breach of personal information or from the Department of Innovation and Technology in lieu of the impacted agency, the Attorney General may publish the name of the State agency that suffered the breach, the types of personal information compromised in the breach, and the date range of the breach.

(Source: P.A. 99-503, eff. 1-1-17; 100-412, eff. 8-25-17.)

(815 ILCS 530/15)

Sec. 15. Waiver. Any waiver of the provisions of this Act is contrary to public policy and is void and unenforceable.

(Source: P.A. 94-36, eff. 1-1-06.)

(815 ILCS 530/20)

Sec. 20. Violation. A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.

(Source: P.A. 94-36, eff. 1-1-06.)

(815 ILCS 530/25)

Sec. 25. Annual reporting. Any State agency that collects personal data and has had a breach of security of the system data or written material shall submit a report within 5 business days of the discovery or notification of the breach to the General Assembly listing the breaches and outlining any corrective measures that have been taken to prevent future breaches of the security of the system data or written material. Any State agency that has submitted a report under this Section shall submit an annual report listing all breaches of security of the system data or written materials and the corrective measures that have been taken to prevent future breaches.

(Source: P.A. 94-947, eff. 6-27-06.)

(815 ILCS 530/30)

Sec. 30. Safe disposal of information. Any State agency that collects personal data that is no longer needed or stored at the agency shall dispose of the personal data or written material it has collected in such a manner as to ensure the security and confidentiality of the material.

(Source: P.A. 94-947, eff. 6-27-06.)

(815 ILCS 530/40)

Sec. 40. Disposal of materials containing personal information; Attorney General.

(a) In this Section, "person" means: a natural person; a corporation, partnership, association, or other legal entity; a unit of local government or any agency, department, division, bureau, board, commission, or committee thereof; or the State of Illinois or any constitutional officer, agency, department, division, bureau, board, commission, or committee thereof.

(b) A person must dispose of the materials containing personal information in a manner that renders the personal information unreadable, unusable, and undecipherable. Proper disposal methods include, but are not limited to, the following:

(1) Paper documents containing personal information may be either redacted, burned, pulverized, or shredded so that personal information cannot practicably be read or reconstructed.

(2) Electronic media and other non-paper media containing personal information may be destroyed or erased so that personal information cannot practicably be read or reconstructed.

(c) Any person disposing of materials containing personal information may contract with a third party to dispose of such materials in accordance with this Section. Any third party that contracts with a person to dispose of materials containing personal information must implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation, and disposal of materials containing personal information.

(d) Any person, including but not limited to a third party referenced in subsection (c), who violates this Section is subject to a civil penalty of not more than $100 for each individual with respect to whom personal information is disposed of in violation of this Section. A civil penalty may not, however, exceed $50,000 for each instance of improper disposal of materials containing personal information. The Attorney General may impose a civil penalty after notice to the person accused of violating this Section and an opportunity for that person to be heard in the matter. The Attorney General may file a civil action in the circuit court to recover any penalty imposed under this Section.

(e) In addition to the authority to impose a civil penalty under subsection (d), the

Attorney General may bring an action in the circuit court to remedy a violation of this Section, seeking any appropriate relief.

(f) A financial institution under 15 U.S.C. 6801 et. seq. or any person subject to 15 U.S.C. 1681w is exempt from this Section.

(Source: P.A. 97-483, eff. 1-1-12.)

(815 ILCS 530/45)

Sec. 45. Data security.

(a) A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

(b) A contract for the disclosure of personal information concerning an Illinois resident that is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

(c) If a state or federal law requires a data collector to provide greater protection to records that contain personal information concerning an Illinois resident that are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this Section.

(d) A data collector that is subject to and in compliance with the standards established pursuant to Section 501(b) of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. Section 6801, shall be deemed to be in compliance with the provisions of this Section.

(Source: P.A. 99-503, eff. 1-1-17.)

(815 ILCS 530/50)

Sec. 50. Entities subject to the federal Health Insurance Portability and Accountability Act of 1996. Any covered entity or business associate that is subject to and in compliance with the privacy and security standards for the protection of electronic health information established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act shall be deemed to be in compliance with the provisions of this Act, provided that any covered entity or business associate required to provide notification of a breach to the Secretary of Health and Human Services pursuant to the Health Information Technology for Economic and Clinical Health Act also provides such notification to the Attorney General within 5 business days of notifying the Secretary.

(Source: P.A. 99-503, eff. 1-1-17.)

(815 ILCS 530/900)

Sec. 900. (Amendatory provisions; text omitted).

(Source: P.A. 94-36, eff. 1-1-06; text omitted.)

Biometric Information Privacy Act (740 ILCS14/)

(740 ILCS 14/1)
Sec. 1. Short title. This Act may be cited as the Biometric Information Privacy Act.
(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/5)
Sec. 5. Legislative findings; intent. The General Assembly finds all of the following:
(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.
(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.
(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.
(d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.
(e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.
(f) The full ramifications of biometric technology are not fully known.
(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.
(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/10)
Sec. 10. Definitions. In this Act:
"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific

testing or screening.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

"Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.

"Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.

"Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment. (Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/15)

Sec. 15. Retention; collection; disclosure; destruction.

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

(c) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

(2) the disclosure or redisclosure completes a

financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(e) A private entity in possession of a biometric identifier or biometric information shall:

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/20)

Sec. 20. Right of action. Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:

(1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;

(2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;

(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

(4) other relief, including an injunction, as the State or federal court may deem appropriate.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/25)

Sec. 25. Construction.

(a) Nothing in this Act shall be construed to impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person.

(b) Nothing in this Act shall be construed to conflict with the X-Ray Retention Act, the federal Health Insurance Portability and Accountability Act of 1996 and the rules promulgated under either Act.

(c) Nothing in this Act shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder.

(d) Nothing in this Act shall be construed to conflict with the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004 and the rules promulgated thereunder.

(e) Nothing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/30)
Sec. 30. (Repealed).
(Source: P.A. 95-994, eff. 10-3-08. Repealed internally, eff. 1-1-09.)

(740 ILCS 14/99)
Sec. 99. Effective date. This Act takes effect upon becoming law.
(Source: P.A. 95-994, eff. 10-3-08.)

Municipal Code of Chicago Chapter 2-173 Welcoming City Ordinance

ORDINANCE
BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF CHICAGO:

SECTION 1. Chapter 2-173 of the Municipal Code of Chicago is hereby amended by deleting the language struck through and adding the language underscored, as follows:

2-173-010 Definitions.

As used in this ordinance, the following words and phrases shall mean and include For purposes of this Chapter, the following definitions shall apply:

"Administrative warrant" means any document issued by ICE that can form the basis for an individual's arrest or detention for a civil immigration enforcement purpose an immigration warrant of arrest, order to detain or release aliens, notice of custody determination, notice to, appear, removal order, warrant of removal, or any other document that can form the basis for an individual's arrest or detention for a civil immigration enforcement purpose, non-limiting examples of which include Form 1-200 "Warrant for the Arrest of Alien," Form 1-205 "Warrant of Removal/Deportation," any predecessor or successor form, and all wants, hits, or requests contained in the "Immigration Violator File" of the FBI's National Crime Information Center database. This definition does not include any a criminal warrant issued upon a judicial determination of probable cause, and in compliance with the requirements of the Fourth Amendment to the U.S. Constitution and Article I, Section 6 of the Illinois Constitution.

Agency. "Agency" means every City department, agency, division, commission, council, committee, board, other body, or person established by authority of an ordinance, executive order, or City Council order.

Agent. 'Agent" means any person employed by or acting on behalf of an agency.

Citizenship or immigration status. "Citizenship or immigration status" means all matters regarding questions of citizenship of the United States or any other country, the authority to reside in or otherwise be present in the United States,

"Coercion" means the use of improper or unlawful force or threats, express or implied, in order to compel a person to act against his or her will. As defined herein, "coercion" includes compelling a person to make statements.

"CBP" means United States Customs and Border Protection. "CPD" means the Chicago Department of Police.

(Omitted text is not affected by this ordinance.)

"HSI" means Homeland Security Investigations.

"Immigration detainer" means a request by ICE to a federal, state or local law enforcement agency to provide notice of release or maintain custody of an individual based on an alleged violation of a civil immigration law, non-limiting examples of which include detainers • issued pursuant to Sections 1226 or 1357 of Title 8 of the United States Code or Sections 287.7 or 236.1 of Title 8 of the Code of Federal Regulations, Form I-247A "Immigration Detainer- Notice of Action" and any predecessor or successor form.

(Omitted text is not affected by this ordinance.)

2-173-043 Prohibited activities

(a) No agency or agent shall assist ICE, HSI, CBP. or another successor agency with a civil immigration enforcement operation, including by being present to support or assist such an operation, establishing a traffic perimeter, or providing other on-site support.

(1) If CPD receives a request from ICE, HSI, CBP, or another successor agency to provide such assistance, a CPD supervising officer shall determine whether such request is to assist in the enforcement of civil immigration law. If the supervisor determines that the request is to assist in the enforcement of civil immigration law, the supervisor shall decline the request. The supervisor shall also notify the Office of Emergency Management and Communications with an identifier that indicates that the event is a request for assistance with civil immigration enforcement.

(2) An agency or agent is authorized to communicate with ICE in order to determine whether any matter involves enforcement based upon a violation of a civil immigration law.

(b) No agency or agent shall enter into an agreement under Section 1357(q) of Title 8 of the United States Code or any other provision of federal law that permits state or local governmental entities to enforce federal civil immigration law.

(c) After January 1, 2020, no agency or agent shall enter into or renew any agreement providing direct access to any electronic database or other data-sharing platform maintained by any agency, or otherwise provide direct access to such database, to any federal agency, if the agency or agent determines that the purpose of such access is for the enforcement of civil immigration law.

2-173-050 No private cause of action

This chapter does not create or form the basis for liability on the part of the City, its agents, or agencies. The exclusive A remedy for the violation of this chapter shall be through the City's disciplinary procedures for officers and employees under regulations including but not limited to this City personnel rules, union contracts, civil service commission rules, or any other agency rules and/or regulations. A person alleging a violation of this chapter against a member of the Chicago Police Department shall forward a complaint to the Independent Police Review Authority Civilian Office of Police Accountability, or any successor independent police review agency; all other complaints shall be forward to the Office of the Inspector General ("Inspector General") who shall process it in accordance with the complaint-processing procedures established in Chapter 2-56 of this Code except that if the complaint is against any member of the City Council or any employee or staff person of any City Council committee, the Inspector General

shall promptly transmit said complaint to the Chairman of the City Council Committee on Committees and Rules for processing or such successor committee having jurisdiction over said matters. Nothing in this section shall preclude an individual from seeking injunctive or declaratory relief for a violation of this Chapter.

2-173-065 Policies for public facilities.

The Corporation Counsel, in consultation with appropriate stakeholders, shall develop model policies for public libraries, community mental health centers, administrative hearing facilities, and any other appropriate public facilities administered or operated by the City to ensure that all such facilities remain safe and accessible to all Chicago residents, regardless of immigration status. All such facilities shall establish public policies that limit immigration enforcement operations on their premises to the fullest extent possible consistent with federal and state law. The City shall also make such policies available to facilities operated by sister agencies, including public schools and park district facilities.

2-173-067 Calls related to immigration enforcement operations.

The City shall take reasonable steps to provide a service through 311 that provides callers with information on immigration resources, which may include directing calls to an organization that can provide assistance. If such a system is established, the City shall ensure

•that residents who have limited proficiency in the English language have meaningful access to such service in accordance with Chapter 2-40 of the Municipal Code of Chicago. ,

2-173-069 Reporting Requirements.

(a) In order to ensure compliance with this Chapter, starting July 1, 2020. CPD shall submit a quarterly report to the Office of the Mayor and the Office of the Inspector General describing its compliance with this Chapter in the preceding quarter, which shall include:

> (1) A list of the notifications made by CPD to the Office of Emergency Management and Communications with events describing a request for assistance with the enforcement of federal civil immigration law, as required under Section 2-173-043(b)(1)(D).
>
> (2) With regard to immigration detainers or administrative warrants received by CPD that are related to enforcement of civil immigration law:
>
> > (A) The date that CPD received the immigration detainer or administrative warrant; and
> >
> > (B) Whether CPD transferred the individual subject to the immigration detainer or administrative warrant to a federal agency's custody and, if so, which agency.

(b) The Office of the Mayor and the Office of the Inspector General shall make such reports publicly available, including through the Internet.

SECTION 2. This ordinance shall take effect following due passage and publication.

Appendix E—CPIC Privacy Policy