LEGISLATIVE RESEARCH SERVICES

Alaska State Legislature
Division of Legal and Research Services
State Capitol, Juneau, AK 99801

(907) 465-3991 phone
(907) 465-3908 fax
research@legis.state.ak.us

Memorandum

TO: Senator Bill Wielechowski
FROM: Katie Spielberger, Legislative Analyst
DATE: March 15, 2012
RE: Federal Privacy Protections for Biometric Information
LRS Report 12.192

You asked for information about federal biometric privacy protections. Specifically, you wished to know whether Senate Bill 98 includes any duplication of federal privacy standards. You were particularly interested in laws regulating collecting biometric information without authorization, secondary uses of the information, disclosing the information to a third party, and disposal of information after intended use.

In brief, Senate Bill 98 would provide broader privacy protections for biometric data than currently exist on a federal level in the United States, and does not duplicate federal protections.[1] There are currently no comprehensive federal privacy laws that specifically address biometric data. While federal laws do offer some protections for personal data, these laws are sectoral—that is, they are applicable only to data collected by a specific industry, for example, or only to data collected by the federal government. In addition, much federal legislation does not explicitly address biometric data in defining what personal data are covered; it would likely need to be determined on a case-by-case basis whether these laws apply to biometric data.

The US is one of very few developed nations without broad-based data privacy legislation. As a report on data privacy produced for the European Commission cautions, "the US approach is incoherent, sectorally-based, and … legislative protections are largely reactive, driven by outrage at particular, narrow practices."[2] In the US, the most comprehensive privacy legislation has generally been passed at the state level, and this seems to be the case with biometric data privacy as well. While most state legislation addressing biometric data privacy is still fairly narrow in scope, we identified three states that have passed more comprehensive measures—Illinois, Indiana, and Texas.

Data privacy issues are not contained by political or national boundaries. Biometric data are used increasingly in passports and border clearance programs—for example, Canada's NEXUS border clearance program, which United States citizens may also participate in, uses iris image scans. In the private sector, electronic data are routinely transferred between countries—for example, the US company Facebook stores digital photos of users from scores of different countries. Since technology development may outpace regulation, many countries have forward-thinking data privacy protections to encompass emerging technologies. In Canada and the European Union (EU), the right to privacy encompasses personal information, and biometric data privacy is typically interpreted in the context of general data privacy. That is, the same laws that apply to data such as names and identification numbers are extended to such data as iris images and DNA.[3]

---

[1] We used bill version CSSB 98 (JUD) for this report. As you know, "biometrics" refers to the various ways humans can be identified through unique aspects of their bodies. CSSB 98 defines "biometric data" as including fingerprints, handprints, voices, facial mapping, retinal images, vein scans, hand geometry, and finger geometry. Given that other biometric identifiers exist—for example, body odor and walking characteristics—and given that other biometric systems may be developed in the future, a broader definition might prove more useful in the long term.

Compared to other forms of identification, biometric data are generally more difficult to steal or falsify, and biometric systems are widely believed to be more reliable and secure than other identification systems. However, there are many privacy concerns specific to biometric data collection. For instance, some biometric information, such as fingerprints and facial images, can be collected without a person's knowledge or consent, which raises concerns about covert surveillance. Additionally, there is no way short of surgery to reassign biometric data—a person can be given a new social security number but not a new fingerprint—so protections against the mishandling of biometric data are especially important.

[2] "Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments-United States of America," by Chris Hoofnagle, can be viewed at *http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B1_usa.pdf.*

[3] The right of privacy was added to the Alaska Constitution by a 1972 amendment in response to fears of electronic surveillance, and may be understood to include the right to privacy of personal information (Gordon Harrison, *Alaska's Constitution: A Citizen's Guide*, 4th ed., Legislative Affairs Agency, 2002). Other states with similar constitutional rights to privacy are Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington.

Many countries, including Canada and EU member states, have a central Privacy Commissioner or equivalent position to enforce privacy laws. Citizens of these countries who believe their personal data have been mishandled, or who believe themselves to be victims of identity theft, have the right to file complaints to this office, which is responsible for investigating such cases. In the US there is no Privacy Commissioner or equivalent.[4]

US Federal Data Privacy Laws and Applications to Biometrics

While there are no broad federal laws specifically addressing biometric data privacy, the US government's increasing use of biometric technology in the last decade, largely in the interest of national security, has raised questions about how existing federal privacy laws apply to biometric data. The National Biometric Security Project (NBSP), a non-profit consultancy under contract to the National Security Agency, has prepared several helpful reports on the application of privacy laws to biometrics, both in the US and internationally.[5] The organization's report on US privacy laws notes that since September 11, 2001, the nation's concerns for national security have generally outweighed concerns for privacy, and laws protecting privacy are far more lax in the context of national security; the report, however, still recommends that the government protect any data collected against unauthorized use or disclosure.

Much federal data privacy legislation can be traced to recommendations made in 1973 by the Department of Health Education and Welfare, which advocated for broad federal legislation to protect personal data from being mishandled in light of new technology. Of federal laws that regulate government collection of information on people, the Privacy Act of 1974 is likely the one most applicable to biometric data.

There is no data privacy legislation governing the entire private sector in the US; rather, privacy legislation governs the concerns of specific industries, such as the Gramm-Leach Bliley Act of 1999, which protects information held by financial institutions. Many private sector laws could be deemed applicable to biometric data, but few explicitly mention biometrics. It is important to note that much private sector privacy legislation is reactionary rather than forward thinking, leading to very narrow protections such as the Video Privacy Protection Act of 1988, which prohibits the disclosure of an individual's rental history without consent and requires that video stores destroy rental records within a year after an account is closed.[6] In 2011, a bill was introduced in the US Senate which would potentially fill some of the gaps in data privacy protections in the private sector; this bill specifically mentions biometric data.

We discuss below what we believe to be the most significant and far-reaching federal data privacy laws; these laws are by no means exhaustive of federal data privacy legislation.

U.S. Department of Health Education and Welfare's Fair Information Practices, 1973

In 1972, the U.S. Department of Health Education and Welfare (HEW) Secretary Elliot Richardson, established an Advisory Committee on Automated Personal Data Systems to analyze potential harmful consequences from using new computer technology to collect, store, and use personal data about citizens. As Secretary Richardson wrote in a public interest determination to establish the committee,

[4] A 2009 American Civil Liberties Union report has called for stronger privacy oversight institutions in the US. The report, "Enforcing Privacy: Building American Institutions to Protect Privacy in the Face of New Technology and Government Powers," can be accessed at *www.aclu.org/technology-and-liberty/enforcing-privacy-building-american-institutions-protect-privacy-face-new-tec*. The *Privacy Journal*, February 2012, notes that the five-member federal Privacy and Civil Liberties Oversight Board has a "miniscule budget" and its members have not yet been confirmed by the Senate.

[5] The National Biometric Security Project's "Report on United States Federal Laws Regarding Privacy and Personal Data and Applications to Biometrics," along with other related reports, can be accessed at *www.nationalbiometric.org*.

[6] The Video Privacy Protection Act of 1988 (18 U.S.C. §§ 2710–2711), passed after Supreme Court nominee Robert Bork's video rental records were disclosed in a newspaper, may be one of the strongest consumer privacy protections in the US, according to the Electronic Privacy Information Center (*www.epic.org*).

> The use of automated data systems containing information about individuals is growing in both the public and private sectors . . . At the same time, there is a growing concern that automated personal data systems present a serious potential for harmful consequences, including infringement of basic liberties. This has led to the belief that special safeguards should be developed to protect against potentially harmful consequences for privacy and due process.

The committee's report, issued in 1973, recommended the enactment of a federal Code of Fair Information Practice for *all* personal data systems, based on the following principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.[7]

Although such omnibus legislation has not been enacted in the US, these principles are reflected to varying in degrees in subsequent US privacy legislation.

Privacy Act of 1974

Many of the HEW principles are embodied in the federal Privacy Act of 1974 (P.L. 93-579, codified at 5 USCA § 552a), which provides protections for records of U.S. citizens and legal resident aliens collected by federal agencies. Under the Act, federal agencies must adopt and publish standards regarding the collection, maintenance, use, and disclosure of *personally identifiable records*. There are provisions in the Act regulating the collection of information—requiring, for example, that each individual be informed of the purpose for which information is collected—and restricting the disclosure of this information to other parties. There are civil and criminal penalties attached to violations of the Act. The Act does not specifically address secondary use of information collected (that is, using the information for purposes other than which it was collected) or require disposal of information after use. The Act defines "record" as follows:

> the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

To be covered by the Privacy Act, a record must be contained in a *system of records,* that is, "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." The NBSP notes that the Privacy Act's definition of "record" and "system of records" could be interpreted in varying ways regarding biometric data, and a case-by-case analysis would likely be needed to determine whether a particular use of biometrics is considered a "record maintained in a system of

[7] The committee's 1973 report to the HEW Secretary can be viewed at *http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm*.

records." All the same, the NBSP recommends that government agencies collecting biometric data strictly comply with the Act, both to avoid potential penalties and to "help allay public fears that the system will be compromised."

The Privacy Act does not address data collected by private entities, or state or local governments. Additionally, there are several significant exceptions to the act, such as disclosures mandated under the Freedom of Information Act.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act (P.L. 104-191) of 1996 (HIPAA) includes a Privacy Rule, which protects "individually identifiable health information" held by health care institutions. "Individually identifiable health information" includes biometric data, both as health information itself (for example, genetic information) and as information that identifies a specific individual (for example, finger prints).

A key concept in the HIPAA Privacy Rule is *minimum necessary* use and disclosure of information—that is, only the minimum necessary amount of protected health information may be used and disclosed. The U.S. Department of Health and Human Services (HHS) Office for Civil Rights enforces the Privacy Rule of HIPAA, including investigating complaints by individuals that their health information has been mishandled. There are both civil and criminal penalties for violation of the Privacy Rule. It should be noted, however, that some organizations holding health information about individuals do not have to follow the Privacy Rule, including life insurers.[8]

Gramm-Leach Bliley Act of 1999

The Gramm-Leach Bliley Act of 1999 (P.L. 106-102, codified at 15 U.S.C. §§ 6801–6809) offers limited protections to "nonpublic personal information" held by financial institutions. The Act requires financial institutions to securely store personal data; inform consumers of the institution's policies on information sharing; and give consumers the option to opt-out of sharing of financial information with a third party. Whether the Act covers biometric data, however, hinges on whether biometric information is considered nonpublic personal information.

Proposed Legislation: Personal Data Privacy and Security Act of 2011

In 2011, Senate Bill 1151 was introduced in the US Senate. The bill is intended to increase safeguards for "sensitive personally identifiable information" and would require, among other things, that all business entities collecting sensitive information on 10,000 or more US persons establish standards for developing and implementing safeguards to protect the security of the information collected. This bill, however, does not specify these standards. The bill uses a very broad definition of "sensitive personal identifiable information," which explicitly mentions "unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation."

Biometric Privacy in Other States—Illinois, Indiana, and Texas

As noted earlier, the most comprehensive legislation we found specifically addressing biometric data privacy in the US is at the state, not the federal, level. According to the National Conference of State Legislatures (NCSL), at least 18 states have passed legislation that addresses biometrics, but many of these laws are somewhat limited in scope—for example, many states regulate the collection of biometric data in the context of driver licensing, and several states require school districts to obtain parental consent before collecting biometric data from students. Based on a recent review by NCSL, it appears that Alaska is one of only a small number of states either considering or having passed comprehensive biometric data privacy legislation. Three states—Illinois, Indiana, and Texas—have passed such broad-based legislation. Of the three, only Indiana's legislation uses a definition of "personal information" sufficiently broad to encompass new identification systems developed in the future. We include copies of these laws as Attachment A.

[8] The US Department of Health and Human Services publishes information about the HIPAA Privacy Rule at *http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html*.

Illinois

Illinois, like Alaska, recognizes the right to privacy in its state constitution. The Illinois Biometric Information Privacy Act (740 ILCS 14/1 *et seq.*), enacted in 2008, addresses biometric data collected by private entities, but not governmental entities. Under the Act, biometric data may not be collected or disclosed without the subject's informed written consent, with few exceptions. The Act obligates entities in possession of biometric data to make a public schedule and create guidelines for destroying the data after the initial purpose for collection has been satisfied, or after three years, whichever comes first. The Act notes that the ramifications of biometric technology are not fully known, yet the definition of "biometric identifier" only includes the following: a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.

Indiana

Indiana Code 4-1-6, Fair Information Practices; Privacy of Personal Information, addresses data collected by governmental agencies, regulating the collection, maintenance, and use of personal information. "Personal information" is here given a broad definition that encompasses biometric identifiers:

> "Personal information" mean any information that describes, locates, or indexes anything about an individual or that affords a basis for inferring personal characteristics about an individual including, but not limited to, his education, financial transactions, medical history, criminal or employment records, finger and voice prints, photographs . . .

The code restricts the collection of personal information to that which is relevant and necessary to accomplish a statutory purpose, and directs state agencies to inform individuals regarding the use and confidentiality of the information. The code includes a right of data subjects to inspect, challenge, or correct their personal information.

Texas

Texas addresses biometric privacy in both its Government Code and Business and Commerce Code, thus covering both public and private sectors. Government Code Chapter 560, enacted in 2001, prohibits government bodies from disclosing biometric data without the subject's consent, and obligates these bodies to securely store and protect biometric data. The Business and Commerce Code Chapter 503, enacted in 2007, requires informed consent for collecting and disclosing biometric data; obligates secure storage; and requires disposal no later than one year after the data are no longer needed. "Biometric identifier" is defined here as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."

International Perspective—OECD Guidelines

As noted above, most other industrialized countries have wide-ranging and forward-thinking data privacy legislation. There is a great deal of overlap in data privacy protections among these countries, in large part stemming from the Organization for Economic Co-Operation and Development's (OECD) 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, a set of nonbinding principles that OECD member countries were recommended to adopt. Data privacy legislation reflects these guidelines in many member countries, including in the EU and Canada. The US, while a member of OECD, has not passed comparable federal legislation.[9]

The OECD Guidelines, which the organization recommends be applied to biometric data as well, are as follows:

- *Collection Limitation Principle*: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

[9] There are 34 OECD Members, including most EU countries, Australia, Canada, Chile, Israel, Japan, Korea, Mexico, New Zealand, and the US.

- *Data Quality Principle*: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- *Purpose Specification Principle*: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- *Use Limitation Principle*: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [The Purpose Specification Principle] except a) with the consent of the data subject; or b) by the authority of law.
- *Security Safeguards Principle*: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
- *Openness Principle*: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- *Individual Participation Principle*: An individual should have the right:

  a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

  b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

  c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

  d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
- *Accountability Principle*: A data controller should be accountable for complying with measures which give effect to the principles stated above.

In a 2004 report, the OECD advocated that these guidelines, as well as its 2002 *Guidelines for the Security of Information Systems and Networks,* be embodied in any biometric system design and project.[10]

Indeed, most, if not all, OECD member countries have determined that existing data privacy legislation generally encompasses biometric data as well. For example, the Office of the Privacy Commissioner of Canada has identified major privacy concerns specific to biometric data collection and has analyzed how these concerns are addressed by privacy principles applicable to personal information in general.[11]

We hope this is helpful. If you have questions or need additional information, please let us know.

[10] "Biometric Based Technologies," a report by the OECD Working Party on Information Security and Privacy, can be accessed at *www.oecd.org/officialdocuments/displaydocumentpdf?cote=dsti/iccp/reg(2003)2/final&doclanguage=en*.

[11] "Data at Your Fingertips: Biometrics and the Challenges to Privacy," Office of the Privacy Commissioner of Canada. This report, as well as links to the complete texts of Canadian data privacy legislation, the Privacy Act and the Personal Information Protection and Electronic Documents Act, can be found on the Privacy Commissioner's website, *www.priv.gc.ca/index_e.cfm.*

Attachment A

740 Illinois Compiled Statutes, 14/1, *et seq.*

Indiana Code 4-1-16, *et seq.*

Texas Government Code 560.001, *et seq.*

Texas Business and Commerce Code 503.011, *et seq*.

( )

(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.)

Go

Information Maintained by the Office of Code Revision Indiana Legislative Services Agency

IC 4-1-6

Chapter 6. Fair Information Practices; Privacy of Personal Information

IC 4-1-6-1

Definitions

Sec. 1. As used in this chapter, the term:

(a) "Personal information system" means any recordkeeping process, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars of a data subject.

(b) "Personal information" means any information that describes, locates, or indexes anything about an individual or that affords a basis for inferring personal characteristics about an individual including, but not limited to, his education, financial transactions, medical history, criminal or employment records, finger and voice prints, photographs, or his presence, registration, or membership in an organization or activity or admission to an institution.

(c) "Data subject" means an individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in a personal information system.

(d) "State agency" means every agency, board, commission, department, bureau, or other entity of the administrative branch of Indiana state government, except those which are the responsibility of the auditor of state, treasurer of state, secretary of state, attorney general, superintendent of public instruction, and excepting the department of state police and state educational institutions.

(e) "Confidential" means information which has been so designated by statute or by promulgated rule or regulation based on statutory authority.

As added by Acts 1977, P.L.21, SEC.1. Amended by Acts 1978, P.L.10, SEC.1; P.L.19-1983, SEC.1; P.L.2-2007, SEC.17.

IC 4-1-6-2

Personal information system

Sec. 2. Any state agency maintaining a personal information system shall:

(a) collect, maintain, and use only that personal information as is relevant and necessary to accomplish a statutory purpose of the agency;

(b) collect information to the greatest extent practicable from the data subject directly when the information may result in adverse determinations about an individual's rights, benefits and privileges under federal or state programs;

(c) collect no personal information concerning in any way the political or religious beliefs, affiliations and activities of an individual unless expressly authorized by law or by a rule promulgated by the oversight committee on public records pursuant to IC 4-22-2;

(d) assure that personal information maintained or disseminated from the system is, to the maximum extent possible, accurate, complete, timely, and relevant to the needs of the state agency;

(e) inform any individual requested to disclose personal information whether that disclosure is mandatory or voluntary, by what statutory authority it is solicited, what uses the agency will make of it, what penalties and specific consequences for the individual, which are known to the agency, are likely to result from nondisclosure, whether the information will be treated as a matter of public record or as confidential information, and what rules of confidentiality will govern the information;

(f) insofar as possible segregate information of a confidential nature from that which is a matter of public record; and, pursuant to statutory authority, establish confidentiality requirements and appropriate access controls for all categories of personal information contained in the system;

(g) maintain a list of all persons or organizations having regular access to personal information which is not a matter

of public record in the information system;

(h) maintain a complete and accurate record of every access to personal information in a system which is not a matter of public record by any person or organization not having regular access authority;

(i) refrain from preparing lists of the names and addresses of individuals for commercial or charitable solicitation purposes except as expressly authorized by law or by a rule promulgated by the oversight committee on public records pursuant to IC 4-22-2;

(j) make reasonable efforts to furnish prior notice to an individual before any personal information on such individual is made available to any person under compulsory legal process;

(k) establish rules and procedures to assure compliance with this chapter and instruct each of its employees having any responsibility or function in the design, development, operation or maintenance of such system or use of any personal information contained therein of each requirement of this chapter and of each rule and procedure adopted by the agency to assure compliance with this chapter;

(l) establish appropriate administrative, technical and physical safeguards to insure the security of the information system and to protect against any anticipated threats or hazards to their security or integrity; and

(m) exchange with other agencies official personal information that it has collected in the pursuit of statutory functions when:

(i) the information is requested for purposes authorized by law including a rule promulgated pursuant to IC 4-22-2;

(ii) the data subject would reasonably be expected to benefit from the action for which information is requested;

(iii) the exchange would eliminate an unnecessary and expensive duplication in data collection and would not tangibly, adversely affect the data subject; or

(iv) the exchange of information would facilitate the submission

of documentation required for various state agencies and departments to receive federal funding reimbursement for programs which are being administered by the agencies and departments.

As added by Acts 1977, P.L.21, SEC.1. Amended by Acts 1978, P.L.10, SEC.2; Acts 1979, P.L.40, SEC.3.

IC 4-1-6-3

Right of inspection by data subject or agent; document search and duplication; standard charges

Sec. 3. Unless otherwise prohibited by law, any state agency that maintains a personal information system shall, upon request and proper identification of any data subject, or his authorized agent, grant such subject or agent the right to inspect and to receive at reasonable, standard charges for document search and duplication, in a form comprehensible to such individual or agent:

(a) all personal information about the data subject, unless otherwise provided by statute, whether such information is a matter of public record or maintained on a confidential basis, except in the case of medical and psychological records, where such records shall, upon written authorization of the data subject, be given to a physician or psychologist designated by the data subject;

(b) the nature and sources of the personal information, except where the confidentiality of such sources is required by statute; and

(c) the names and addresses of any recipients, other than those with regular access authority, of personal information of a confidential nature about the data subject, and the date, nature and purpose of such disclosure.

As added by Acts 1977, P.L.21, SEC.1.

IC 4-1-6-4

Disclosures limited to business hours; standard charges

Sec. 4. An agency shall make the disclosures to data subjects required under this chapter during regular business hours. Copies of the documents containing the personal information sought by the data subject shall be furnished to him or his representative at reasonable, standard charges for document search and duplication.

As added by Acts 1977, P.L.21, SEC.1.

IC 4-1-6-5

Challenge of information by data subject; notice; minimum procedures

Sec. 5. If the data subject gives notice that he wishes to challenge, correct or explain information about him in the personal information system, the following minimum procedures shall be followed:

(a) the agency maintaining the information system shall investigate and record the current status of that personal information;

(b) if, after such investigation, such information is found to be incomplete, inaccurate, not pertinent, not timely or not necessary to be retained, it shall be promptly corrected or deleted;

(c) if the investigation does not resolve the dispute, the data subject may file a statement of not more than two hundred (200) words setting forth his position;

(d) whenever a statement of dispute is filed, the agency maintaining the data system shall supply any previous recipient with a copy of the statement and, in any subsequent dissemination or use of the information in question, clearly mark that it is disputed and supply the statement of the data subject along with the information;

(e) the agency maintaining the information system shall clearly and conspicuously disclose to the data subject his rights to make such a request;

(f) following any correction or deletion of personal information the agency shall, at the request of the data subject, furnish to past recipients notification delivered to their last known address that the item has been deleted or corrected and shall require said recipients to acknowledge receipt of such notification and furnish the data subject the names and last known addresses of all past recipients of the uncorrected or undeleted information.

As added by Acts 1977, P.L.21, SEC.1.

IC 4-1-6-6

Securing of confidential information protected

Sec. 6. The securing by any individual of any confidential information which such individuals may obtain through the exercise of any right secured under the provisions of this chapter shall not condition the granting or withholding of any right, privilege, or benefit, or be made a condition of employment.

As added by Acts 1977, P.L.21, SEC.1.

IC 4-1-6-7

State agencies maintaining one or more systems; requirements

Sec. 7. (a) Any state agency maintaining one (1) or more personal information systems shall file an annual report on the existence and character of each system added or eliminated since the last report with the governor on or before December 31.

(b) The agency shall include in such report at least the following information:

(1) The name or descriptive title of the personal information system and its location.

(2) The nature and purpose of the system and the statutory or administrative authority for its establishment.

(3) The categories of individuals on whom personal information is maintained including the approximate number of all individuals on whom information is maintained and the categories of personal information generally maintained in the system including identification of those which are stored in computer accessible records and those which are maintained manually.

(4) All confidentiality requirements, specifically:

(A) those personal information systems or parts thereof

which are maintained on a confidential basis pursuant to a statute, contractual obligation, or rule; and

(B) those personal information systems maintained on an unrestricted basis.

(5) In the case of subdivision (4)(A) of this subsection, the agency shall include detailed justification of the need for statutory or regulatory authority to maintain such personal information systems or parts thereof on a confidential basis and, in making such justification, the agency shall make reference to section 8 of this chapter.

(6) The categories of sources of such personal information.

(7) The agency's policies and practices regarding the implementation of section 2 of this chapter relating to information storage, duration of retention of information, and elimination of information from the system.

(8) The uses made by the agency of personal information contained in the system.

(9) The identity of agency personnel, other agencies, and persons or categories of persons to whom disclosures of

personal information are made or to whom access to the system may be granted, together with the purposes therefor and the restriction, if any, on such disclosures and access, including any restrictions on redisclosure.

(10) A listing identifying all forms used in the collection of personal information.

(11) The name, title, business address, and telephone number of the person immediately responsible for bringing and keeping the system in compliance with the provisions of this chapter.

As added by Acts 1977, P.L.21, SEC.1. Amended by Acts 1978, P.L.10, SEC.3; P.L.19-1983, SEC.2.

IC 4-1-6-8

Policy of access; restricted access as condition for receipt of donated materials

Sec. 8. (a) All state agencies subject to the provisions of this chapter shall adhere to the policy that all persons are entitled to access to information regarding the affairs of government and the official acts of those who represent them as public servants, such access being required to enable the people to freely and fully discuss all matters necessary for the making of political judgments. To that end, the provisions of this chapter shall be construed to provide access to public records to the extent consistent with the due protection of individual privacy.

(b) Where such assurance is needed to obtain valuable considerations or gifts (which may include information) for the state, any agency, with the prior written approval of the oversight committee on public records, may allow restrictions upon public access to be imposed upon it as a specific condition of a contract, with a time limit not to exceed fifty (50) years or the lifetime of the individual, whichever is less. In order to promote the preservation of

historical, cultural, natural, and other irreplaceable resources, the department of natural resources or the Indiana state library may extend, beyond the lifetime of the individual, restrictions upon disclosure of information received, providing that such restrictions do not exceed fifty (50) years from the date of the donation in the case of the Indiana state library.

As added by Acts 1977, P.L.21, SEC.1. Amended by Acts 1978, P.L.10, SEC.4; Acts 1979, P.L.40, SEC.4; P.L.19-1983, SEC.3.

IC 4-1-6-8.5

Consistent handling of information among and between agencies; principles and procedures

Sec. 8.5. In order to establish consistent handling of the same or similar personal information within and among agencies, each state agency collecting, maintaining, or transmitting such information shall apply the following principles and procedures:

(1) Information collected after December 31, 1978, which is classified as confidential must be clearly and uniformly designated as confidential in any form or other document in which it appears.

(2) When an agency which holds information classified as confidential disseminates that information to another agency, the receiving agency shall treat it in the same manner as the originating agency.

As added by Acts 1978, P.L.10, SEC.5. Amended by P.L.19-1983, SEC.4.

IC 4-1-6-8.6

Requests for access to confidential records; improper disclosure; actions

Sec. 8.6. (a) In cases where access to confidential records containing personal information is desired for research purposes, the agency shall grant access if:

(1) the requestor states in writing to the agency the purpose, including any intent to publish findings, the nature of the data sought, what personal information will be required, and what safeguards will be taken to protect the identity of the data subjects;

(2) the proposed safeguards are adequate to prevent the identity of an individual data subject from being known;

(3) the researcher executes an agreement on a form, approved by the oversight committee on public records, with the agency, which incorporates such safeguards for protection of individual data subjects, defines the scope of the research project, and informs the researcher that failure to abide by conditions of the approved agreement constitutes a breach of contract and could result in civil litigation by the data subject or subjects;

(4) the researcher agrees to pay all direct or indirect costs of the research; and

(5) the agency maintains a copy of the agreement or contract for

a period equivalent to the life of the record.

(b) Improper disclosure of confidential information by a state employee is cause for action to dismiss the employee.
As added by Acts 1978, P.L.10, SEC.6. Amended by Acts 1979, P.L.40, SEC.5; P.L.19-1983, SEC.5.

IC 4-1-6-9

Annual report to general assembly; specific statutory authorization for confidentiality; recommendations

Sec. 9. (a) Under the authority of the governor, a report shall be prepared, on or before December 1 annually, advising the general assembly of the personal information systems, or parts thereof, of agencies subject to this chapter, which are recommended to be maintained on a confidential basis by specific statutory authorization because their disclosure would constitute an invasion of personal privacy and there is no compelling, demonstrable and overriding public interest in disclosure. Such recommendations may include, but not be limited to, specific personal information systems or parts thereof which can be categorized as follows:

(1) Personal information maintained with respect to students and clients, patients or other individuals receiving social, medical, vocational, supervisory or custodial care or services directly or indirectly from public bodies.

(2) Personal information, excepting salary information, maintained with respect to employees, appointees or elected officials of any public body or applicants for such positions.

(3) Information required of any taxpayer in connection with the assessment or collection of any income tax.

(4) Information revealing the identity of persons who file complaints with administrative, investigative, law enforcement or penology agencies.

(b) In addition, such report may list records or categories of records, which are recommended to be exempted from public disclosure by specific statutory authorization for reasons other than that their disclosure would constitute an unwarranted invasion of personal privacy, along with justification therefor.

(c) A report described in this section must be in an electronic format under IC 5-14-6.
As added by Acts 1977, P.L.21, SEC.1. Amended by P.L.28-2004, SEC.13.

GOVERNMENT CODE

TITLE 5. OPEN GOVERNMENT; ETHICS

SUBTITLE A. OPEN GOVERNMENT

CHAPTER 560. BIOMETRIC IDENTIFIER

Sec. 560.001. DEFINITIONS. In this chapter:

(1) "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.

(2) "Governmental body" has the meaning assigned by Section 552.003, except that the term includes each entity within or created by the judicial branch of state government.

Added by Acts 2001, 77th Leg., ch. 634, Sec. 2, eff. Sept. 1, 2001.
Renumbered from Government Code Sec. 559.001 by Acts 2003, 78th Leg., ch. 1275, Sec. 2(78), eff. Sept. 1, 2003.

Sec. 560.002. DISCLOSURE OF BIOMETRIC IDENTIFIER. A governmental body that possesses a biometric identifier of an individual:

(1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless:

(A) the individual consents to the disclosure;

(B) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552; or

(C) the disclosure is made by or to a law enforcement agency for a law enforcement purpose; and

(2) shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the governmental body stores, transmits, and protects its other confidential information.

Added by Acts 2001, 77th Leg., ch. 634, Sec. 2, eff. Sept. 1, 2001.
Renumbered from Government Code Sec. 559.002 by Acts 2003, 78th Leg., ch. 1275, Sec. 2(78), eff. Sept. 1, 2003.

Sec. 560.003. APPLICATION OF CHAPTER 552. A biometric identifier in the possession of a governmental body is exempt from disclosure under Chapter 552.

Added by Acts 2001, 77th Leg., ch. 634, Sec. 2, eff. Sept. 1, 2001.
Renumbered from Government Code Sec. 559.003 by Acts 2003, 78th Leg., ch. 1275,

Sec. 2(78), eff. Sept. 1, 2003.

BUSINESS AND COMMERCE CODE

TITLE 11. PERSONAL IDENTITY INFORMATION

SUBTITLE A. IDENTIFYING INFORMATION

CHAPTER 503. BIOMETRIC IDENTIFIERS

Sec. 503.001. CAPTURE OR USE OF BIOMETRIC IDENTIFIER. (a) In this section, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.

(b) A person may not capture a biometric identifier of an individual for a commercial purpose unless the person:

(1) informs the individual before capturing the biometric identifier; and

(2) receives the individual's consent to capture the biometric identifier.

(c) A person who possesses a biometric identifier of an individual that is captured for a commercial purpose:

(1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless:

(A) the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death;

(B) the disclosure completes a financial transaction that the individual requested or authorized;

(C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code; or

(D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant;

(2) shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects any other confidential information the person possesses; and

(3) shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires, except as provided by Subsection (c-1).

(c-1) If a biometric identifier of an individual captured for a commercial purpose is used in connection with an instrument or document that is required by another law to be maintained for a period longer than the period prescribed by Subsection (c)(3), the person who possesses the biometric identifier shall destroy the biometric identifier within a reasonable time, but

not later than the first anniversary of the date the instrument or document is no longer required to be maintained by law.

(c-2) If a biometric identifier captured for a commercial purpose has been collected for security purposes by an employer, the purpose for collecting the identifier under Subsection (c)(3) is presumed to expire on termination of the employment relationship.

(d) A person who violates this section is subject to a civil penalty of not more than $25,000 for each violation. The attorney general may bring an action to recover the civil penalty.

Added by Acts 2007, 80th Leg., R.S., Ch. 885, Sec. 2.01, eff. April 1, 2009.
Amended by:

Acts 2009, 81st Leg., R.S., Ch. 1163, Sec. 1, eff. September 1, 2009.