SB

98

<TARGET><BILL>SB 98</BILL><SUBJECT>SB
98</SUBJECT><COMM>HJUD27</COMM></TARGET>

ALASKA STATE LEGISLATURE

Session

State Capitol, Rm. 101
Juneau, AK 99801
(907) 465-2435
Fax: (907) 465-6615

Interim

716 W. 4th Ave, Ste. 540
Anchorage, AK 99501
(907) 269-0120
Fax: (907) 269-0122

Senator_Bill_Wielechowski@legis.state.ak.us

Chair
State Affairs Committee

Co-chair
Joint Armed Services Committee

Vice Chair
Resources Committee
Judiciary Committee

Member
Administrative Regulation Review

SENATOR BILL WIELECHOWSKI

SB 98: Biometrics
SPONSOR STATEMENT

"Civilization is the progress toward a society of privacy." – Ayn Rand

Article 1, Section 22 of Alaska's State Constitution explicitly states that "the right of the people to privacy is recognized and shall not be infringed." This constitutional right underscores Alaskans' abiding desire for privacy. Much like genetic information, biometric information holds great promise for fields such as medicine, law enforcement and security. This bill is meant to ensure that Alaskan's constitutional right to privacy is protected by adopting common sense measures of accountability.

In 2004, the Alaska Legislature unanimously passed legislation outlawing the collection, analysis or storage of a law-abiding citizen's genetic information without their express written consent. This legislation was drafted in response to rapidly evolving technology that has the potential to discriminate against citizens based on personal genetic information that would otherwise be private. SB 98 applies the same privacy protections to biometric information, as it is just as permanent and irreplaceable as genetic information.

The term "biometric information" refers to any information about an individual based on their unique behavioral or physiological characteristics. The most commonly known form of biometric information is a person's fingerprints, but also includes hand geometry recognition, voice recognition, iris and retinal scans, and vein recognition.

Data merchants today can exploit Alaskans' private biometric information for financial gain. Certain genetic disorders and medical conditions can be strongly correlated from biometric information. Because it so easy for data to be sold or stolen in today's digital world, Alaska needs to be sure to have strong legal measures in place to protect Alaskans.

Senate Bill 98 will protect Alaskans' biometric information. This legislation is all protecting sensitive information. The bill has strong bipartisan support, passed the Senate unanimously, and will ensure the privacy of all Alaskans is protected.

LEGAL SERVICES

DIVISION OF LEGAL AND RESEARCH SERVICES
LEGISLATIVE AFFAIRS AGENCY
STATE OF ALASKA

(907) 465-3867 or 465-2450
FAX (907) 465-2029
Mail Stop 3101

State Capitol
Juneau, Alaska 99801-1182
Deliveries to: 129 6th St., Rm. 329

MEMORANDUM January 17, 2012

SUBJECT: CSSB 98(JUD) relating to biometric information
(Work Order No. 27-LS0661\R)

TO: Senator Bill Wielechowski
Attn: Samuel Gottstein

FROM: Terry Bannister
Legislative Counsel

You have requested a sectional summary of the above-described bill. As a preliminary matter, note that a sectional summary of a bill should not be considered an authoritative interpretation of the bill and the bill itself is the best statement of its contents.

Section 1. Adds a new chapter, AS 18.14, relating to biometric information.

Sec. 18.14.010(a) prohibits a person from collecting another person's biometric information unless the person first notifies the individual about the collection and receives the individual's full consent. The notification must indicate the specific purpose for which the information will be used and how long it will be kept. The consent may be written, electronic, or in another form that can be documented.

Sec. 18.14.010(b) allows an individual to revoke or amend consent at any time, unless the information was needed for a specific authorized law enforcement, security, or fraud prevention purpose.

Sec. 18.14.020(a) prohibits a collector and the collector's contractor from disclosing, transferring, or distributing an individual's biometric information, except to a contractor or to a person to authenticate the individual's identity.

Sec. 18.14.020(b) limits the disclosures, transfers, and distributions under (a) to the original purpose for which the information was collected.

Sec. 18.14.030 prohibits a person from selling biometric information. But does allow a contractor to sell the contractor's business and transfer the biometric information to the buyer.

Sec. 18.14.040 allows an individual to provide alternate identification to a person administering an occupational examination that requires identifying biometric information, if the alternate identification is acceptable to the person.

Sec. 18.14.050(a) requires a collector to remove an individual's biometric information from databases and storage systems and destroy the information within 120 days when the information is no longer needed or an individual requests the destruction in writing. This requirement is subject to other laws and court orders prohibiting the removal and destruction.

Sec. 18.14.050(b) directs the collector to notify the collector's contractor within 30 days that the collector must remove and destroy the information under this section.

Sec. 18.14.060 prohibits a collector from using biometric information for marketing or general surveillance purposes. But does allow a collector to use the information for a specific authorized security or fraud prevention purpose in addition to the specific purpose for which the information was collected.

Sec. 18.14.070 directs a collector and a contractor to store biometric information in a secure manner.

Sec. 18.14.080(a) allows an individual (except as provided in (b)) to bring a civil action for damages and a penalty against a person who knowingly violates this chapter. Increases the penalty if the violation resulted in profit or monetary gain.

Sec. 18.14.080(b) prohibits an action for damages and penalties against the state, state agencies, or officers or employees of the state or state agencies, for violations of or other claims under this chapter.

Sec. 18.14.085 lists certain exemptions from the chapter. Also removes from the chapter's coverage the retention of voices recorded for quality assurance purposes.

Sec. 18.14.090 defines terms for the chapter.

If I may be of further assistance, please advise.

TLB:ljw
12-021.ljw

ALASKA STATE LEGISLATURE

Session

State Capitol, Rm. 101
Juneau, AK 99801
(907) 465-2435
Fax: (907) 465-6615

Interim

716 W. 4th Ave, Ste. 540
Anchorage, AK 99501
(907) 269-0120
Fax: (907) 269-0122

Senator_Bill_Wielechowski@legis.state.ak.us

Chair
State Affairs Committee

Co-chair
Joint Armed Services Committee

Vice Chair
Resources Committee
Judiciary Committee

Member
Administrative Regulation Review

SENATOR BILL WIELECHOWSKI

Biometrics Fact Sheet

- "Biometric Information" refers to any information about an individual based on their unique behavioral or physiological characteristics. The most commonly known form of biometric information is a person's fingerprints, but also includes hand geometry recognition, voice recognition, iris and retinal scans, and vein recognition.

- Many Alaskans are nervous about their biometric information being sold or stolen. Since biometric information is irreplaceable, this sharing of biometric data can cause Alaskans irreparable harm.

- Certain genetic disorders and medical conditions have been strongly correlated with biometric information, and customers could experience price discrimination based on facial recognition technology.

- Senate Bill 98 will ensure that biometric data is not disseminated to third parties without an individual's consent, and will only be used for the purposes for which it was collected. SB-98 does not ban the collection of biometric data; it simply requires consent for collection and prohibits the sale or unauthorized distribution of the data.

ALASKA STATE LEGISLATURE

SENATOR BILL WIELECHOWSKI

April 10, 2012

The Honorable Steve Thompson, Vice-Chair
House Judiciary Committee
State Capitol, Room 428
Juneau, Alaska 99801

Dear Representative Thompson:

I am writing to request a hearing for the House CS for CS for SB 98(HSS), "An Act relating to biometric information."

House CS for CS for SB 98(HSS) will protect Alaskan citizens from having their biometric information, such as fingerprints and iris images, from being collected and disseminated to third parties without their consent.

While the medical and law enforcement benefits of such biometric information is not in question, law-abiding citizens of the state should not be treated as criminals when being hired or taking a licensing exam.

Privacy is of vital importance to the people of Alaska, and House CS for CS for SB 98(HSS) is intended to ensure that the people are able to protect their most private forms of identification, while still allowing for reasonable, and lawful, use of biometrics throughout the state.

Included with this letter you will find:

1. Sponsor Statement and Fact Sheet
2. Current Version of the Bill (LSO661\L) as well as the previous version R as it passed the Senate
3. Zero Fiscal Note
4. Sectional Summary for version R, an explanation of changes and an adopted conceptual amendment
5. Articles detailing privacy concerns surrounding biometrics
6. Letters of Support
7. List of Alaskan Supporters
8. List of expected testimony

My legislative aide Sam Gottstein is assigned to this legislation. His direct line is 465-2435. He intends to present a PowerPoint presentation during the initial hearing. Thank you for your consideration of this request.

Sincerely,

Senator Bill Wielechowski
Prime Sponsor

Session: State Capitol • Juneau, Alaska 99801 • (907) 465-2435 • (800) 550-2435 • Fax: (907) 465-6615
Interim: 716 West 4th Avenue • Anchorage, Alaska 99501 • (907) 269-0120 • Fax: (907) 269-0122
Senator_Bill_Wielechowski@legis.state.ak.us • www.aksenate.org/wielechowski/

FISCAL NOTE

STATE OF ALASKA cost ≠ codes
2012 LEGISLATIVE SESSION

Bill Version **SB 98**
Fiscal Note Number
Publish Date

Identifier (file name) SB098CS(JUD) LAW-CIV-03-23-12
Title An Act relating to biometric information.
Sponsor SENATORS WIELECHOWSKI
Requester (H) Health & Social Services

Dept. Affected Law
Appropriation Civil
Allocation Human Services
OMB Component Number 2962

Expenditures/Revenues (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

	FY13 Appropriation Requested	Included in Governor's FY13 Request	Out-Year Cost Estimates				
OPERATING EXPENDITURES	**FY13**	**FY13**	**FY14**	**FY15**	**FY16**	**FY17**	**FY18**
Personal Services							
Travel							
Services							
Commodities							
Capital Outlay							
Grants, Benefits							
Miscellaneous							
TOTAL OPERATING	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

FUND SOURCE		(Thousands of Dollars)						
1002	Federal Receipts							
1003	GF Match							
1004	GF							
1005	GF/Prgm (DGF)							
1037	GF/MH (UGF)							
1178	temp code (UGF)							
TOTAL		**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

POSITIONS							
Full-time							
Part-time							
Temporary							

CHANGE IN REVENUES							

Estimated SUPPLEMENTAL (FY12) operating costs _____ *(separate supplemental appropriation required)*
(discuss reasons and fund source(s) in analysis section)

Estimated CAPITAL (FY13) costs _____ *(separate capital appropriation required)*
(discuss reasons and fund source(s) in analysis section)

Why this fiscal note differs from previous version (if initial version, please note as such)

Updated for new Attorney General.

Prepared by Sheila Bugbee, Administrative Officer
Division Administrative Services
Phone 465-5427
Date/Time 3/23/12 10:00AM

Approved by Michael C. Geraghty, Attorney General
Department of Law
Date 3/23/2012

(Revised 8/17/2011 OMB)

FISCAL NOTE

STATE OF ALASKA **BILL NO.** SB 98
2012 LEGISLATIVE SESSION

Analysis

This bill provides a framework for all entities, including state agencies that collect, analyze, or distribute biometric information. The state uses biometric information in a number of instances, such as occupational licensing, back ground checks, etc... This bill provides specific rules as to the retention and destruction of biometric information and includes express exceptions for law enforcement, information collected by the DMV, and for uses that are authorized by state and federal law. Finally, although this bill includes a private right of action if this statute is violated, it also includes an immunity provision for state agencies. With this immunity provision, the fiscal impact of this legislation is zero.

April 13, 2012

AMERICAN CIVIL LIBERTIES UNION OF ALASKA
1057 W. Fireweed, Suite 207
Anchorage, AK 99503
(907) 258-0044
(907) 258-0288 (fax)
WWW.AKCLU.ORG

OFFICERS AND DIRECTORS
SUSAN WINGROVE, Anchorage
PRESIDENT

RICH CURTNER, Anchorage
VICE PRESIDENT

LLOYD EGGAN, Anchorage
TREASURER

MICHAEL KING, Anchorage
SECRETARY

WILLIE ANDERSON, Juneau
AFFIRMATIVE ACTION OFFICER

DONNA J. GOLDSMITH, Anchorage
PAUL GRANT, Juneau
SCOTT HENDERSON, Anchorage
KATIE HURLEY, Wasilla
MARJORIE KAISER, Anchorage
CONNIE OZER, Anchorage
GALEN PAINE, Sitka
STEPHANIE PAWLOWSKI, Anchorage
JUNE PINNELL-STEPHENS, Fairbanks
TONY STRONG, Juneau

EMMA HILL, Anchorage
STUDENT ADVISOR

The Honorable Steve Thompson
House Judiciary Committee
Alaska State House of Representatives
State Capitol
Juneau, AK 99801
via email: Representative_Steve_Thompson@legis.state.ak.us

Re: Committee Substitute for Senate Bill 98 (HSS)
ACLU Statement of Support

Dear Representative Thompson:

Thank you for the opportunity to submit a written statement of support for the Health and Social Services Committee Substitute for Senate Bill 98.

The American Civil Liberties Union of Alaska represents thousands of members and activists throughout the State of Alaska who seek to preserve and expand individual freedoms and civil liberties guaranteed under the United States and Alaska Constitutions.

From a constitutional rights and privacy perspective, **the ACLU of Alaska endorses protections for individuals' personal biometric information, and supports this Bill's goal of avoiding violations of privacy before they occur**.

Need for Biometrics Legislation

Recent advances in genomics, bioinformatics and data mining are encouraging a worldwide proliferation of "gene banks" – large collections of biological samples that usually include genetic information derived from those samples, as well as linked medical, family history or lifestyle

information. The use of these biological repositories for genetics research could lead to advances in public health, such as the identification of genetic factors in diseases, or the development of diagnostic tests. ***On the other hand, they also create an avenue for privacy infringements, stigmatization and discrimination, and improper commercial exchange of personal data.***

The ACLU supports legislation to prevent privacy infringement and genetic discrimination. SB 98 can advance these goals.

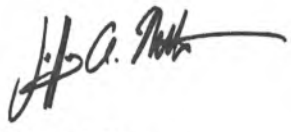
Protections Against Coerced Consent

Given the ability to condition the provision of necessary services on the disclosure of personal information, we also note that CS for SB 98 (HSS) is intended to protect against coerced "consent."

Given the sensitivity of biometric information, and the plethora of medical information obtainable from it, we endorse legislation that would protect Alaskans from improperly being compelled to waive their rights to protect their personal, private information.

Thank you again for the opportunity to share our support of this bill. Please feel free to contact the undersigned should you have any questions or seek additional information.

Sincerely,



Jeffrey Mittman
Executive Director
ACLU of Alaska

cc: Representative Wes Keller, Representative_Wes_Keller@legis.state.ak.us
Representative Bob Lynn, Representative_Bob_Lynn@legis.state.ak.us
Representative Lance Pruitt, Representative_Lance_Pruitt@legis.state.ak.us
Representative Max Gruenberg, Representative_Max_Gruenberg@legis.state.ak.us
Representative Lindsey Holmes, Representative_Lindsey_Holmes@legis.state.ak.us
Representative Mike Hawker, Representative_Mike_Hawker@legis.state.ak.us
Senator Bill Wielechowski, Senator_Bill_Wielechowski@legis.state.ak.us

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.*

Information maintained by the Legislative Reference Bureau

Updating the database of the Illinois Compiled Statutes (ILCS) is an ongoing process. Recent laws may not yet be included in the ILCS database, but they are found on this site as Public Acts soon after they become law. For information concerning the relationship between statutes and Public Acts, refer to the Guide.

Because the statute database is maintained primarily for legislative drafting purposes, statutory changes are sometimes included in the statute database before they take effect. If the source note at the end of a Section of the statutes includes a Public Act that has not yet taken effect, the version of the law that is currently in effect may have already been removed from the database and you should refer to that Public Act to see the changes made to the current law.

( )

(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.)

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.

PALMER — Smashed windows and damage totaling more than $10,000 were

andrew.welbner@frontiersman.com or 352-2270.

HELP US STOP COMPULSORY FINGERPRINTING OF INNOCENT ALASKANS:

Right now in Alaska, students who refuse to submit their fingerprints "for ID purposes" to a national database are being denied educational and testing opportunities... and that's just not right.

to a national biometric database "as ID" or they will be denied the opportunity to take the SAT...and thus denied the ability to attend most colleges. Without Juneau passing a tough new privacy law, this could happen to kids here in Alaska.

For some exams, even if you present a US passport as ID, you will be denied access to the exam room if you don't first submit to a fingerprinting supposedly "for ID purposes." The Wall Street Journal even exposed that the firm giving the SAT exam has considered requiring children to submit their biometrics/fingerprints

Call Representative Gatto 465-3743 and Representative Wes Keller 465-2186, tell them to stand up for Alaskans and our right to privacy. If a US passport is good enough ID to travel the world and enter the USA, it's good enough ID to take an exam. This is America, let's take our privacy back.

Citizens for Privacy in Alaska PrivacyNowAK@aol.com www.PrivacyNowAlaska.org

Interested in a great life in A

HOPE Community Resources Inc.

We at Hope in the are seeking outgoi who will enjoy sha lives with two indi who describe thei follows:

"My friend and I share a home together locat Wasilla, Alaska. We love the outdoors, exer good meals and fun times together. We also need assistance with our personal c meal preparation, homecare and going to/fr variety of community locations."

Job descriptions, pay rates and other employment in availableatwww.hopealaska.org,oryoucancontactthel at our local office by calling 433-4762. Many describ work as life-changing and rewarding. Lots of traini Give Hope a call and stop in to meet us.

We can all enjoy Alaska together

Lifeline service.

Qualified low-income residents of Alaska may receive discounted service

Valley Healing Se

March 3rd

6 p.m. – 8:30 p.

Church on the Roc

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,

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.

Stronger Privacy Laws

The Alaskan Biometric Privacy bill SB-98 February 21, 2012

Dear Representative Gatto:

In your district and all over Alaska, Alaskans are now being denied educational opportunities and the ability to take many exams unless they first submit their fingerprints & biometrics to a database as a form of identification. Shockingly, even students who show a US passport and driver's license are being *refused educational opportunities* if they don't submit to a fingerprinting "as ID." As you may know, this happened to me in February 2008.

If a US passport is good enough identification to travel the world and enter the United States…it is certainly good enough identification to take a test. This is what The Alaskan Biometric Privacy Bill SB-98 is all about; standing up for Alaskans and their right to privacy.

Last April, the Senate unanimously voted to support SB-98. The bill is now before the House Health & Social Services and the Judiciary committees. Senate co-sponsors include Senators Coghill (R), Menard (R), Giessel (R), McGuire (R), Paskvan (D), Thomas (D), Ellis (D), Wagoner (R), Egan (D) and Dyson (R).

As you can imagine, the Privacy Bill is extremely popular with Alaskan voters – and only opposed by the data mining corporations and the biometrics industry lobbyists (SIA/LexisNexis|ChoicePoint/Prometric) *who are currently making money off exploiting Alaskans' loss of privacy.* Luckily, they don't vote.

Mandating fingerprints as ID for an exam is already illegal in Canada under their PIPEDA (Personal Information Protection and Electronic Documents Act) privacy laws, but no such protection exists for Alaskans. We need your help to change that.

Important: The current wording in the critical "Alternative ID" section 18.14.040 of SB-98 is too loose, essentially undermining much of the bill's intended protection. It needs to be clear that

1) If an individual shows a US Passport or State ID (driver's license), they don't need to also submit to being fingerprinting for identification
2) An individual can't be discriminated against and denied educational or testing opportunities because of their refusal to provide their biometrics as identification if they provide an Alternative ID.

As you know, Article 1 Section 22 of the Alaska Constitution states "the right of the people to privacy is recognized and shall not be infringed." There are very few issues on which Alaskans from across the political spectrum agree. The *urgent* need to protect our privacy from constant corporate and Federal Government intrusion is one of them.

Sincerely,

Jason Giaimo
Co-Chairman, Citizens for Privacy in Alaska
602-9250 giaimo1@aol.com
www.PrivacyNowAlaska.org

Tim Pearson
Co, Chairman, Citizens for Privacy in Alaska
952-3498
tim@timpearson.net

Citizens for Privacy in Alaska is a group of concerned Alaskans now nearly 1,000 strong who support stronger State privacy laws.

Facts about data privacy:

• 24 million customer records at Amazon.com accessed by criminals 1/16/2012
Have you ever shopped at Amazon.com? As reported in USA Today just a few weeks ago on 1/16, their "state-of-the-art" database was hacked into and criminals gained access to 24 million confidential customer records—maybe yours. **What if a similarly "state-of-the-art" database that contained the fingerprints of you or your children were hacked into, and your prints were planted at a crime scene?** If your fingerprints were found, would you really be able to prove you weren't there? Is this really the sort of Orwellian surveillance society Alaskans in your district want to live in?

• "There have been 535 data breaches made public in 2012 alone, affecting a total of 30.4 million records. 2011 saw some of the biggest data breaches in history, coming in a number of different forms and affecting a wide range of industries." Privacy Rights Clearinghouse notes that over 544 million confidential records have been compromised since just 2005. http://www.privacyrights.org/

• FBI, Pentagon pays ChoicePoint for access to trove of public records
National Journal Reports: By Shane Harris *sharris@nationaljournal.com*:
"…the FBI and the Defense Department…have been paying a Georgia-based company [ChoicePoint/LexisNexis—*the same firm collecting Alaskan fingerprints for some exams*] for access to its vast databases that contain billions of personal records about nearly every person in the United States. This system allows for the ability to use the private data broker to do something that they legally can't -- keep tabs on nearly every American citizen and foreigner in the United States. ChoicePoint is famous for being the largest and most sophisticated aggregator of public records on U.S. citizens and residents. The company has built an enormous electronic cache of more than 19 billion records." 11/11/2005
http://www.govexec.com/story_page.cfm?filepath=/dailyfed/1105/111105nj1.htm&oref=search

• Biometrics collection is Big Business, and very lucrative
The international Biometric Group estimates that annual biometric industry revenue for 2012 will be over $12.4 billion dollars, with 25% of revenues being related to fingerprinting, and 13% related to facial recognition (www.biometricgroup.com).

• US Senator Charles Schumer and Lindsey Graham proposed a compulsory fingerprinting of all Americans as a requirement to work (National work ID cards)
In an article written by them in the Washington Post, Schumer and Graham state that as a "cornerstone" of their Immigration Reform Proposal, we "would require all US citizens who want to work to obtain a biometric social security card." The compulsory fingerprinting of all law-abiding Americans is essentially a **National ID card.** Washington Post, 3/19/2010

• "Biometric requirement could make E-Verify worth billions"
Sen. Charles Schumer (D-N.Y.) enthusiastically supports adding a biometric identifier [ie. the compulsory fingerprinting of all working Americans] to the federal E-Verify employment eligibility verification system, which is setting the stage for potentially one of the largest federal biometric collection opportunities, potentially encompassing the entire U.S. workforce of 140 million employees. "Obviously, it will be a big boost for the industry," said David Coleman of International Biometric Group. SIA, the Security Industry Association also strongly supports it, as their members would profit greatly.
http://washingtontechnology.com/articles/2009/08/10/policy--everify-biometrics.aspx

ISSUE SUMMARY & FAQ:

SB-98 The Alaskan Biometric Privacy Bill

2/21/2012

Last session, the Alaskan Senate voted unanimously to pass The Alaskan Biometric Privacy Bill, SB-98. The bill is now in the House Health & Social Services and Judiciary committees.

What's this all about?

It's about standing up for Alaskan's privacy, and stopping corporations from compelling innocent Alaskans to submit to fingerprinting as ID.

The goal is to make illegal the practice of compelling people to submit their fingerprints or other biometrics as identification when they are willing to show their driver's license or a United States passport. This does not affect fingerprinting done for background checks, and law enforcement is exempt from this bill.

Why this is urgently needed:

An update to our privacy laws is urgently needed to address the rapid & accelerating erosion of personal privacy, driven in large part by the biometrics and data mining industry-fueled "identity paranoia." Compelling an individual to submit fingerprints as ID for an exam is already illegal in Canada under their PIPEDA privacy laws (Private Information Protection and Electronic Documents Act), but no such protection exists for Alaskans.

1) It is offensive and immoral to treat honest, law-abiding and privacy loving Alaskans like criminals needing to be fingerprinted. Alaskans have a deep-seated respect for their privacy, AND it's guaranteed by our Constitution. We'll show our State ID/driver's license or passport- that's enough.

2) The right to privacy is fundamental to Alaska's heritage and unique culture, and is guaranteed by Article 1, Section 22 of the Alaska Constitution: *"The right of the people to privacy is recognized and shall not be infringed."*

3) Updated privacy laws will help to stem the rapid erosion of personal privacy; reining in some of the worst abuses of data technology by both private industry and government:

"The FBI is embarking on a $1 billion effort to build the world's largest computer database of people's physical characteristics, a project that would give the government unprecedented abilities to identify individuals in the United States and abroad. Digital images of faces, fingerprints and palm patterns are flowing into FBI systems in a climate-controlled, secure basement in Clarksburg. West Virginia. Next month, the FBI intends to award a 10-year contract that would significantly expand the amount and kinds of biometric information it receives." By Ellen Nakashima, The Washington Post, 12/23/07
http://seattletimes.nwsource.com/html/politics/2004088505_biometrics23.html?syndication=rss

4) Despite the industry's best efforts and "state-of-the-art database security," major data breaches are practically a daily occurrence in the news. There were over 223 million data records of US residents exposed due to security breaches in the last 3 years alone (privacyrights.org).

Fingerprints are like passwords that can never be changed.
Once compromised, individuals will be at risk of identity theft for the rest of their lives.

5) The best way to keep personal data from being lost, hacked or exposed is to not collect it in the first place. After-the-fact restrictions will be largely ineffective, as we will never know what global datamining firms do with the data once collected. **This legislation will protect Alaskans from identity theft.**

6) As of January 1, 2008, Alaskan college students, and anyone else who takes any part of the CPA and various other Prometric-proctored exams are being forced to submit their fingerprints to a global fingerprint database maintained by a foreign-owned data-reseller called ChoicePoint, now part of Reed Elsevier Corp. This is the same company which was assessed a $15 million fine, *the largest fine in the history of the Federal Trade Commission* for "making false and misleading statements about privacy policies, violating privacy rights and violating Federal Laws" according to the FTC website. ChoicePoint combines personal data sourced from multiple public and private databases and sells it to "an estimated 7,000 clients" including the Dept of Homeland Security (see item #3 above). This is just one example of the existing and potential privacy abuses which updated privacy laws would stop. Some exam centers in Alaska (PearsonVue) are right now even forcing exam candidates into having their veins of their palms scanned (by infrared radiation) in addition to fingerprinting, even if a US passport is presented as ID.

This "identity paranoia" is as lucrative to the companies involved as it is absurd. Compelling an individual who is willing to show their US passport or driver's license to submit fingerprints to the database of a private foreign-owned corporation "for ID" is unnecessary and it violates our Constitutionally guaranteed right to privacy.

What is Biometrics?
Biometrics include: fingerprints, DNA, hand geometry, vein scanning, retinal or iris scans and similar technology.

If a US passport is sufficient ID to travel the world and enter the USA, it is certainly sufficient ID to take a test.
Clearly, the goal is to collect & transmit the fingerprints. Both the test center at the University of Alaska-Fairbanks and the Prometric exam centers in Spenard are collecting fingerprints and immediately transferring them over the internet to the notorious data reseller ChoicePoint/ReedElsevier, whose largest customer is the Federal Government. Unlike in Canada, there is currently no law to protect Alaskans from this.

Will this stop the police from using fingerprints on criminals?
No. This does not in any way affect laws or procedures related to law enforcement.

But isn't biometrics "the way of the future?"
Loss of our personal privacy is not the "future" Alaskans want.

Don't the US Government and the Dept of Homeland Security want our fingerprints?
You bet they do (see #3 above)! Some Federal Legislators (Chuck Schumer of NY in particular) are even pushing for a biometric social security card *which would require every American to get fingerprinted in order to work* -- a compelling reason on its own to quickly strengthen our State's biometric privacy laws.

Is the current Alaskan Biometric Privacy Bill SB-98 sufficient?

No – not as worded currently. The most important section of the bill by far in our opinion is the "Alternative Identification" section; however it is so loosely worded so to undermine most of the protection in this bill. **The only true protection is to not compel Alaskans to submit their fingerprints and other biometrics "for ID" in the first place**. IF A US PASSPORT IS SUFFICIENT IDENTIFICATION TO TRAVEL THE WORLD AND ENTER THE USA, IT IS GOOD ENOUGH IDENTIFICATION TO TAKE A TEST.

As Ronald Reagan once said, "Freedom is never more than one generation away from extinction." This is a critical moment. This is our chance to help preserve something all Alaskans hold dear.

By Rep. Greenberg / HJUD
SB98 4/14/12

HIPAA PRIVACY RULE

Law Enforcement Purposes. Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.[34]

http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

The HIPAA Privacy Rule provides a great model for definition of *'law enforcement purposes'*