SB

98

<TARGET><BILL>SB 98</BILL><SUBJECT>SB
98</SUBJECT><COMM>HHSS27</COMM></TARGET>

ALASKA STATE LEGISLATURE

SENATOR BILL WIELECHOWSKI

January 24, 2011

The Honorable Wes Keller, Chair
House Health & Social Services Committee
State Capitol, Room 432
Juneau, Alaska 99801

Dear Representative Keller:

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

CS for SB 98(JUD) will protect Alaskan citizens from having their biometric information, such as fingerprints and facial 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 CS for SB 98(JUD) 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\R) as well as the two previous versions
3. Two zero Fiscal Notes
4. Sectional Summary
5. Three articles detailing privacy concerns surrounding biometrics
6. Letters of Support
7. List of Alaskan Supporters
8. Committee and voting history of the bill
9. List of expected testimony

My legislative aide Sam Gottstein is assigned to this legislation. His direct line is 465-2435. Thank you for your consideration of this request.

Sincerely,

Bill Wielechowski

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/

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 giving Alaskans a choice in whether or not they want to share their biometric data, and 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 and facial recognition, iris and retinal scans, and vein recognition.

Data merchants today can exploit Alaskans' private biometric information for financial gain. Under the status quo, certain academic and professional testing agencies require Alaskans to submit their biometric data to multinational corporations. 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 about giving Alaskans a choice to decide whether or not they want to submit their biometric information to a private company, and what happens to the sensitive information after it has been collected. 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 and facial recognition, iris and retinal scans, and vein recognition.

- Certain academic and professional testing agencies currently require Alaskans to submit their biometric data to multinational corporations to access services. A United States passport is sufficient identification to travel to other countries and should be a suitable alternative form of identification.

- 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.

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
Approved by Michael C. Geraghty, Attorney General
Department of Law

Phone 465-5427
Date/Time 3/23/12 10:00AM
Date 3/23/2012

(Revised 8/17/2011 OMB)

FISCAL NOTE

STATE OF ALASKA
2012 LEGISLATIVE SESSION

BILL NO. SB 98

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.

FISCAL NOTE

STATE OF ALASKA
2011 LEGISLATIVE SESSION

Fiscal Note Number: 2
Bill Version: **CSSB 98(JUD)**
(S) Publish Date: 4/16/11

Identifier (file name): SB098CS(JUD)-LAW-CIV-04-14-11
Title: An Act relating to biometric information.
Sponsor: SENATOR(S) WIELECHOWSKI
Requester: (S) Judiciary

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.

	Appropriation Required	Information					
OPERATING EXPENDITURES	**FY 2012**	**FY 2012**	**FY 2013**	**FY 2014**	**FY 2015**	**FY 2016**	**FY 2017**
Personal Services							
Travel							
Services							
Commodities							
Capital Outlay							
Grants							
Miscellaneous							
TOTAL OPERATING	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
CAPITAL EXPENDITURES							
CHANGE IN REVENUES							

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts							
1003 GF Match							
1004 GF							
1005 GF/Program Receipts							
1037 GF/Mental Health							
Other (please identify)							
TOTAL	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Estimate of any current year (FY2011) cost 0.0

POSITIONS

Full-time							
Part-time							
Temporary							

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

Fiscal impact changed to zero and fiscal analysis changed.

Prepared by: Eileen Donahue, Division Operations Manager
Division: Administrative Services
Phone: 465-5427
Date/Time: 4/15/11 4:00 PM
Approved by: John J. Burns, Attorney General
Department of Law
Date: 4/15/2011

(Revised 1/27/2011 OMB)

STATE OF ALASKA
2011 LEGISLATIVE SESSION

BILL NO. CSSB 98(JUD)

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.

FISCAL NOTE

STATE OF ALASKA
2011 LEGISLATIVE SESSION

Fiscal Note Number: 1
Bill Version: **CSSB 98(STA)**
(S) Publish Date: 3/18/11

Identifier (file name)
Title: SB 98-- Biometric Information for ID
Sponsor: Senator Wielechowski
Requester

Dept. Affected
Appropriation
Allocation
OMB Component Number

Expenditures/Revenues (Thousands of Dollars)

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

	Appropriation Required	Information					
OPERATING EXPENDITURES	**FY 2012**	**FY 2012**	**FY 2013**	**FY 2014**	**FY 2015**	**FY 2016**	**FY 2017**
Personal Services							
Travel							
Services							
Commodities							
Capital Outlay							
Grants							
Miscellaneous							
TOTAL OPERATING	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
CAPITAL EXPENDITURES							
CHANGE IN REVENUES							

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts							
1003 GF Match							
1004 GF							
1005 GF/Program Receipts							
1037 GF/Mental Health							
Other (please identify)							
TOTAL	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Estimate of any current year (FY2011) cost

POSITIONS

Full-time							
Part-time							
Temporary							

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

Prepared by: SENATE STATE AFFAIRS COMMITTEE
Division
Approved by: /s/ Senator Wielechowski, Chair

Phone: 465-2435
Date/Time: 3/17/11 8:00 AM
Date

(Revised 1/27/2011 OMB)

STATE OF ALASKA
2011 LEGISLATIVE SESSION

BILL NO. CSSB 98(STA)

Analysis

No Fiscal Impact

LEGISLATIVE RESEARCH SERVICES

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

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

Memorandum

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

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

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

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

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

---

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

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

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

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

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

US Federal Data Privacy Laws and Applications to Biometrics

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

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

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

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

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

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

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

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

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

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

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

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

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

Privacy Act of 1974

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

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

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

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

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

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

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

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

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

Gramm-Leach Bliley Act of 1999

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

Proposed Legislation: Personal Data Privacy and Security Act of 2011

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

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

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

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

Illinois

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

Indiana

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

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

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

Texas

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

International Perspective—OECD Guidelines

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

Attachment A

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

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

Texas Government Code 560.001, *et seq.*

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

( )

(740 ILCS 14/1)

Sec. 1. Short title. This Act may be cited as the Biometric Information Privacy Act.
(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/5)

Sec. 5. Legislative findings; intent. The General Assembly finds all of the following:

(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.

(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.

(e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.

(f) The full ramifications of biometric technology are not fully known.

(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.
(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/10)

Sec. 10. Definitions. In this Act:

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

"Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.

"Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.

"Written release" means informed written consent or, in the context of employment, a release

executed by an employee as a condition of employment.
(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/15)

Sec. 15. Retention; collection; disclosure; destruction.

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

(c) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(e) A private entity in possession of a biometric identifier or biometric information shall:

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/20)

Sec. 20. Right of action. Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:

(1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;

(2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;

(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

(4) other relief, including an injunction, as the State or federal court may deem appropriate.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/25)

Sec. 25. Construction.

(a) Nothing in this Act shall be construed to impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person.

(b) Nothing in this Act shall be construed to conflict with the X-Ray Retention Act, the federal Health Insurance Portability and Accountability Act of 1996 and the rules promulgated under either Act.

(c) Nothing in this Act shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder.

(d) Nothing in this Act shall be construed to conflict with the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004 and the rules promulgated thereunder.

(e) Nothing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/30)

Sec. 30. (Repealed).

(Source: P.A. 95-994, eff. 10-3-08. Repealed internally, eff. 1-1-09.)

(740 ILCS 14/99)

Sec. 99. Effective date. This Act takes effect upon becoming law.

(Source: P.A. 95-994, eff. 10-3-08.)

Go

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

IC 4-1-6

Chapter 6. Fair Information Practices; Privacy of Personal Information

IC 4-1-6-1

Definitions

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

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

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

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

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

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

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

IC 4-1-6-2

Personal information system

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

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

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

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

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

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

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

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

of public record in the information system;

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

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

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

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

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

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

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

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

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

(iv) the exchange of information would facilitate the submission

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

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

IC 4-1-6-3

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

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

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

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

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

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

IC 4-1-6-4

Disclosures limited to business hours; standard charges

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

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

IC 4-1-6-5

Challenge of information by data subject; notice; minimum procedures

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

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

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

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

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

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

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

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

IC 4-1-6-6

Securing of confidential information protected

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

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

IC 4-1-6-7

State agencies maintaining one or more systems; requirements

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

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

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

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

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

(4) All confidentiality requirements, specifically:

(A) those personal information systems or parts thereof

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

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

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

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

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

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

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

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

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

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

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

IC 4-1-6-8

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

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

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

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

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

IC 4-1-6-8.5

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

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

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

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

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

IC 4-1-6-8.6

Requests for access to confidential records; improper disclosure; actions

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

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

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

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

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

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

a period equivalent to the life of the record.

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

IC 4-1-6-9

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

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

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

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

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

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

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

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

GOVERNMENT CODE

TITLE 5. OPEN GOVERNMENT; ETHICS

SUBTITLE A. OPEN GOVERNMENT

CHAPTER 560. BIOMETRIC IDENTIFIER

Sec. 560.001. DEFINITIONS. In this chapter:

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

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

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

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

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

(A) the individual consents to the disclosure;

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

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

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

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

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

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

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

BUSINESS AND COMMERCE CODE

TITLE 11. PERSONAL IDENTITY INFORMATION

SUBTITLE A. IDENTIFYING INFORMATION

CHAPTER 503. BIOMETRIC IDENTIFIERS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 March 16, 2012

SUBJECT: Information regarding the handling of biometric information (CSSB 98(JUD); Work Order No. 27-LS0661 R)

TO: Representative Wes Keller
Attn: Ernest Prax

FROM: Terry Bannister
Legislative Counsel

You have asked three questions about the regulation of biometric information. You have provided some documents about this subject. You have indicated that the context of this bill is SB 98. For the purposes of this memo, I am using "biometric information" in the sense of the measurement and analysis of human body characteristics. Under CSSB 98(JUD), "biometric data" means fingerprints, handprints, voices, facial mapping, iris images, retinal images, vein scans, hand geometry, or finger geometry.

Because of the scope of this request, this memo is limited to providing you with a general overview of the existing legal areas that appear to relate to your questions. Each of the items in this memo could be discussed in more detail, but I did not want to delay getting this to you. This memo does not address proposals for the handling of biometric data. If you need more information on a particular item, or if this memo does not discuss an item that you believe is significant, please contact me so that we can discuss the item.

1. What legal provisions are in place that may affect how biometric information is collected, stored, shared, and used by private sector entities?

A. Alaska statutes.

(1) Alaska Personal Information Protection Act (AS 45.48). The sections on breach of security involving personal information (AS 45.48.010 - 45.48.090) do not appear to cover biometric information because the definition of "personal information" in AS 45.48.090 does not contain a term that would cover biometric information. The sections on credit reports and credit score security freezes (AS 45.48.100 - 45.48.290) do not appear to cover biometric information, just credit reports. The sections on the protection of social security numbers (AS 45.48.400 - 45.48.480) apply only to social security numbers, not other personal information. The sections that regulate the disposal of records (AS 45.48.500 - 45.48.590) may arguably cover biometric information because the definition of "records" covers "material on which information that is written, drawn, spoken, visual, or electromagnetic is recorded or preserved," except publicly available

information. The sections allowing a factual declaration of innocence after identify theft (AS 45.48.600 - 45.48.670) arguably cover identify theft by using another person's biometric information, but the section is limited to correcting a criminal conviction. The section allowing the right to file a police report regarding identify theft (AS 45.48.680) arguably covers identity theft by using another person's biometric information, and allows an individual to report identity theft. The section on the truncation of card information (AS 45.48.750) only addresses card number digits and expiration dates.

(2) AS 06.01.028 (Depositor and customer records confidential). To the extent any biometric information is contained in depositor and customer records, this section would apply to prevent financial institutions that are subject to AS 06 from releasing them, but there are some exceptions. Under AS 06.01.050, this includes a commercial bank, savings bank, credit union, premium finance company, small loan company, bank holding company, financial holding company, trust company, savings and loan association, deferred deposit advance licensee under AS 06.50, and a licensee under AS 06.60. A financial institution that violates this section is liable to a depositor or customer for damages caused by the disclosure.

(3) Revised Alaska Trust Company Act. AS 06.26.610 makes trust company records relating to customers confidential, with exceptions. To the extent any biometric information is contained in those records, this section would apply to prevent their disclosure.

(4) State criminal offenses. It may be possible to use one or more of the following sections when a factual situation involves biometric information.

AS 11.46.180, theft (of property) by deception, and AS 11.46.190, theft by receiving (stolen property). The application to biometric information depends on how "property," as defined under AS 11.81.900, is interpreted and what factual situation is involved.

AS 11.46.200, theft of services. Covers computer access, so arguably covers access to biometric material on a computer or the use of biometric material to access a computer.

AS 11.46.600, scheme to defraud--by using false or fraudulent pretense, representation to obtain property or services. Arguably could cover using another person's biometric information to obtain property or services.

AS 11.46.740, criminal use of a computer. Broad provision relating to use of a computer to obtain a person's information, introducing false information to damage the information record of a person, and other situations. Arguably applies to obtaining or interfering, etc., with a person's biometric information contained in a computer under certain factual conditions.

(5) AS 45.50.471 - 45.50.561 (Alaska Unfair Trade Practices and Consumer Protection Act). Covers unfair trade practices, so arguably could cover, for example, misrepresentation caused by using false biometric information, or other misuse of

biometric information, by a seller or other entity in a commercial transaction. It may be possible to use this Act to remedy violations of the US-EU Safe Harbor Program by private businesses who participate in that program if the violations amount to misrepresentation of the adoption or use of the program principles. Both the state and private persons have remedies under the Act. There are exceptions to the coverage of the Act.

B. Federal statutes and executive orders.

(1) The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 - 3422). Protects the confidentiality of personal financial records contained in bank records. A financial record means any record held by a financial institution relating to a customer's relationship with the financial institution. So any biometric information contained in a customer's record at a financial institution would arguably be subject to the Act.

(2) Financial Modernization Act of 1999 (Gramm-Leach-Bliley Act) (15 U.S.C. 6801 - 6827). This Act regulates the disclosure of the financial information of the customers of financial institutions. The Act at 15 U.S.C. 6803 requires a financial institution to disclose its privacy policy for nonpublic personal information of the bank's customer, and the Act at 15 U.S.C. 6802 requires the financial institution to give the customer the opportunity to opt out of certain disclosures. The definition of "nonpublic personal information" provided at 15 U.S.C. 6809 is very broad and could arguably cover biometric information in a customer's file with the financial institution. Under 15 U.S.C. 6824, the Act allows for enforcement under state laws, if consistent with the Act, including state laws that provide greater protection.

(3) Federal Trade Commission Act (15 U.S.C. 41 - 58). As mentioned under the US-EU Safe Harbor Program later in this memo, this Act is being used to remedy violations of that program by private businesses who participate in that program.

(4) Fair Credit Protection Act (15 U.S.C. 1681 - 1681x). Governs consumer-reporting agencies, which are agencies that regularly engage in the practice of assembling or evaluating consumer information for the purpose of furnishing consumer reports to third parties. The Act sets restrictions on the disclosure of "medical information." The term could theoretically include biometric information, but is directed to the health or medical condition of an individual for credit purposes.

(5) Health Insurance Portability and Accountability Act of 1996: HIPAA Privacy Rule (45 C.F.R. Parts 160 and 164). Contains restrictions and requirements that "covered entities" (e.g., under 45 C.F.R. 160.103, a health care provider and a health plan) must follow to protect the security of an individual's health information. The Privacy Rule refers to the removal of "biometric identifiers," among other items, in one approach that it approves for making health information not individually identifiable. 45 C.F.R. 164.514(b)(2)(i)(P).

(6) Federal Trade Commission Fair Information Practice Principles. These principles are directed at the privacy of personal information involved in online transactions and they are voluntary. This personal information could theoretically include biometric information.

C. State constitutional provisions.

Article I, sec. 22. Explicit right to privacy. The primary purpose of this right to privacy is to protect the personal privacy of individuals from unwarranted intrusions by the government.[1] Therefore, unless there is some state action involved, this constitutional provision does not apply to the private sector's operations.

D. Federal constitutional provisions.

The federal constitutional provisions that might apply (e.g., the Fourth Amendment's search and seizure provisions and the the Fourteenth Amendment's due process provision) apply to governmental action and, unless some governmental connection can be proven, not to private sector operations. The case that you cited, Whalen v. Roe, 429 U.S. 589 (1977), involved a state statute, so any right to privacy arguably recognized by that case requires that there be some state or federal action involved. State action frequently is based on a statute. I am not aware that the state or federal supreme courts have at this time recognized a specific privacy right in biometric information.

E. International provisions.

US-EU Safe Harbor Program.[2] In light of the EU's privacy protections, this program was established to enable U.S. entities to satisfy the EU's privacy directive[3] ("Directive") and prevent U.S. entities from being shut out of the EU market because they had inadequate information protection. The program appears to cover biometric information because the Directive's definition appears to cover biometric information.[4]

---

[1] State v. Planned Parenthood of Alaska, 35 P.3d 30, 38 (Alaska 2001), cited by Miller v. Safeway, Inc., 102 P.3d 282, 288 (Alaska 2004).

[2] For an overview, see "http://export.gov/safeharbor/eu/eg_main_018476.asp".

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as amended. (For text of the Directive, see "http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT".)

[4] Directive, Chapter 1, Article 2(a): "(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;".

As part of their US-EU Safe Harbor program obligations, organizations are required to have in place a dispute resolution system that will investigate and resolve individual complaints and disputes and procedures for verifying compliance. They are also required to remedy problems arising out of a failure to comply with the principles. Sanctions that dispute resolution bodies can apply must be severe enough to ensure compliance by the organization; they must include publicity for findings.

The Federal Trade Commission and the U.S. Department of Transportation have both stated in letters to the European Commission that they will take enforcement action against organizations that state that they are in compliance with the US-EU Safe Harbor framework, but then fail to live up to their statements.

F. Privacy tort provisions.

At this time, there appear to be four general privacy torts recognized by courts. These are discussed in Section 652 of the Restatement (Second) of Torts. Section 652H discusses the damages that can be awarded for these torts. The use of each tort for biometric information depends on the factual situation involved in the particular care and whether that factual situation satisfies the specific requirements for the tort. The following descriptions of these torts give a general overview of the tort and do not provide all of the specific requirements for each.

(1) Unreasonable intrusion upon the seclusion of another. According to sec. 652B, this privacy tort can occur by intentionally intruding on another person's private affairs or concerns if the intrusion would be highly offensive. Only occurs when the intrusion is into a private place of the person. Theoretically, this could apply to biometric information obtained in this manner.

(2) Appropriation of another person's name or likeness. According to sec. 652C, this privacy tort involves the use of someone else's name or likeness for personal gain or benefit without the person's consent or other authorization. The theory behind this tort is the recognition that a person has the right to exclusively benefit from the person's own name and being. Theoretically, this privacy tort could apply to biometric information if a person uses the biometric information of another person in the person's business or to steal from the person, as in identity theft.

(3) Unreasonable publicity given to another person's private life. According to sec. 652D, this privacy tort involves publicly disclosing someone's private (non-public) personal information without consent or authorization. The dissemination of information contained in a public record, however, is not an actionable offense because the information is already rightfully in the public domain (e.g. a criminal or court record). Theoretically, this privacy tort may apply to biometric information that is not public information.

(4) Publicity that unreasonably places another person in a false light before the public. According to sec. 652E, this privacy tort involves intentionally or recklessly disseminating to the public information about a person that is both false and would be considered highly offensive to a reasonable person. Theoretically, this privacy tort could apply to biometric information if the biometric information of one person were used in some way to place the person in a false position in the public eye.

G. Misrepresentation tort provisions.

A this time there appear to be two misrepresentation torts recognized by the courts and discussed by the Restatement (Second) of Torts that may apply to biometric information. The first is intentional misrepresentation and the second is negligent misrepresentation.

(1) Fraudulent misrepresentation. According to sec. 525, this tort applies when a person fraudulently makes a misrepresentation to induce another person to act or refrain from acting in reliance on the misrepresentation. In your context, this tort might apply, for example, if a business misrepresents that the person has adopted the US-EU Safe Harbor program information privacy principles in order to obtain customers that provide biometric information to the business. This is just one possible application.

(2) Negligent misrepresentation. This tort covers information negligently supplied for the guidance of others. According to sec. 552, this tort applies when a person in the course of business, employment, or another transaction in which the person has a financial interest negligently supplies false information for the guidance of persons in their business transactions. The person is subject to liability for financial loss caused by the recipient's justifiable reliance on the information -- under certain conditions. In your context, this tort might apply, for example, if a business negligently provided incorrect biometric information to a person who relied on the information in the person's business, and that incorrect biometric information caused the person to suffer financial damages as a result.

H. Contractual approach.

If there is a contract that involves the taking, keeping, storing, etc., of biometric information, then a breach of that contract will make the person who breaches the contract liable for the damages resulting from the breach.

2. Are private entities that collect biometric information required to have a privacy policy or a terms of use agreement outlining how biometric information will be used, stored, shared, and disposed of? Are they required to notify a person submitting their biometric information? Could the private entity expose itself to legal action if it does not have a privacy policy or a terms of use agreement?

There does not appear to be any general governmental requirement in the U.S. that a company have a privacy policy specifically addressing the collection, use, storage, sharing, or disposition of biometric information. Of course, as indicated under

question 1, if biometric information occurs in a situation that is covered by a governmental confidentiality or regulatory requirement, then the private company will have to comply with that requirements. One example would be found in bank records that contain any biometric information (e.g., for account access or identification); in that case, both state and federal law regulate the sharing of those records.

As discussed earlier in this memo, a private business can enter into a voluntary agreement under the US-EU Safe Harbor Program if it wants to participate in the E.U. market and avoid violating the E.U.'s privacy laws. The US-EU Safe Harbor program is not directly enforceable by U.S. law. However, the Federal Trade Commission and the U.S. Department of Transportation have both stated in letters to the European Commission that they will take enforcement action against organizations that state that they are in compliance. In addition, as discussed under question 1, an intentional or negligent failure to comply with a policy so adopted by a company could expose the company to private or state or federal action for misrepresentation under unfair trade practices laws.

3. Are there existing guidelines that the State of Alaska must abide by regarding the collection and use of biometric information?

There are no express existing general guidelines for the state when it collects biometric information.

However, AS 12.62.160 and AS 12.64.010 provide fairly comprehensive confidentiality provisions for information that lands in the criminal justice system, including fingerprints. AS 12.62.160 exempts criminal justice information from disclosure under the state's public record disclosure requirements under AS 40.25. AS 12.64.010 enacts the National Crime Prevention and Privacy Compact. In general, this Compact organizes an electronic information sharing system among the federal government and the states to exchange criminal history records for noncriminal justice purposes authorized by federal or state law, such as background checks for governmental licensing and employment. One of the purposes of the Compact is to require the FBI and each state that is a party to the Compact to adhere to certain standards concerning record dissemination, use, response times, system security, and information quality, including the accuracy and privacy of such records. In the Compact, the definition of "positive identification" includes a reference to fingerprints and other biometric identification techniques.

Aside from criminal justice information, if a factual situation covers biometric information and falls within any of the confidentiality provisions salted throughout the statutes (or federal provisions that apply to the particular state action) those provisions may apply to the particular situation. In addition to other statutory provisions mentioned elsewhere in this memo, the following statutes provide examples of these confidentiality statutes.

AS 06.01.025 (Records of department). Under this section, the information in the records of the department obtained through the administration of AS 06 (Banks and Financial Institutions) is confidential, is not subject to subpoena, and may be revealed only with the

consent of the department. In the future, the information collected from financial institutions through state banking inspections could contain biometric information (e.g., a fingerprint for security or access purposes).

AS 06.55.407 (Confidentiality) (Alaska Uniform Money Services Act). This section is similar to AS 06.01.025, but applies only to persons engaging in providing money services.

AS 08.02.040 addresses the confidentiality of patient mental health records received under certain licensing chapters by the Department of Health and Social Services.

AS 12.65.015 and 12.65.140 provide the confidentiality requirements for state child fatality review teams.

Motor vehicle-related records. Under AS 28.15.151(f), the Department of Administration must maintain, with certain exceptions, the confidentiality of the records kept by the department relating to, e.g., driver's licenses and accident reports. This would, for example, cover facial images taken for drivers' licenses. Under AS 28.35.030(d), the department must maintain the confidentiality of records related to the treatment program ordered for operating a motor vehicle, aircraft, or watercraft while under the influence of, for example, alcohol. This would cover biometric information taken during those programs.

DNA Identification System. Under AS 44.41.035(f), the Department of Public Safety must keep the information in its DNA Identification System confidential. And AS 44.41.035(h) requires the adoption of reasonable procedures for the collection, use, storage, and expungement of the information in the system.

The provisions in AS 45.48.500 - 45.48.590 that regulate the disposal of records appear to cover biometric information because the definition of "records" covers "material on which information that is written, drawn, spoken, visual, or electromagnetic is recorded or preserved," except publicly available information. The sections apply to state governmental agencies, except the judicial branch.

If I may be of further assistance, please advise.

TLB:ljw
12-208.ljw

Protecting Alaskan's Privacy

SB 98 – Biometric Information

Privacy in the Constitution

- "The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section."
  - Alaska State Constitution: Article 1, Section 22

Genesis of Alaska's Right to Privacy

- "[the right to privacy in Alaska's Constitution] was prompted by fear of the potential for misuse of computerized information systems, which were then in their infancy."
  - *Alaska's Constitution: A Citizen's Guide* by the Gordon Harrison with the Legislative Affairs Agency, page 37.
- We are in the same situation today, with computerized information threatening our privacy.

Legislative Obligation to Protect

- Alaskan's right to privacy passed overwhelmingly on the 1972 ballot
  - Over 86% approval
- The Legislature has an affirmative constitutional obligation to protect Alaskan's privacy.
- Alaska has a stronger right to privacy than is outlined in the US Constitution

DNA Privacy Protections

- Legislature passed protections in 2004
  - Unanimous support in both bodies
  - SB 98 passed the Senate unanimously
- Maintaining a healthy, thriving private sector is important
- But the Legislature is constitutionally obligated to protect Alaskan's privacy

What are Biometrics?

- Definitions start on page 4 of SB 98
- Some examples of biometrics include fingerprints, hand geometry recognition, vein recognition, facial mapping, retinal scans, voice recognition, etc.

Biometric Privacy is similar to Genetic Privacy

- Increasing number of markers to link health impacts to biometric information
  - Certain fingerprints can be linked to certain diseases and genetic disorders
  - Iris scans can show diabetes, hypertension, etc.
  - Vein scans can indicate heart disease
  - Hand geometry can indicate testosterone levels, which can indicate health risks
- Biometric information should get the same protections afforded to DNA

Federal Privacy Laws Lacking

- The US Constitution does not explicitly give citizens a right to privacy
- Federal laws only focus on specific sectors
  - Federal Government with the Privacy Act of 1974
  - Healthcare through HIPPA in 1996
  - Financial Institutions with the Gramm-Leach-Bliley Act of 1999
- No federal law protects biometric information

Others States address Biometrics

- 18 other states have laws on biometrics
- California has strong privacy laws
  - ChoicePoint data breach in 2006 was disclosed because of these strong protections
  - Data compromised by ChoicePoint selling the data to a fraudulent company
- Legislative Research did a closer analysis of three states, Illinois, Indiana and Texas
  - Highlights the variety of policy decisions in terms of where protections can apply

The Need for Biometric Privacy

- Without legislative action, Alaskans' privacy can be exploited for financial gain
- Invasive, unsettling possibilities
  - False fingerprints on crime scenes
  - Different pricing for customers
- Cannot replace biometric identifiers
  - Different from a credit card or even a SSN
- Nothing is more fundamentally private than DNA and biometric information

Biometrics easy to duplicate

- Easily duplicated, copied, stolen, etc.
  - "Biometric information…can be copied easily, shared quickly and widely, combined, and stored for long periods of time without degrading. That is how **modern identification systems** most **threaten practical obscurity and the privacy it has afforded people for all of history.**" (emphasis added)
    - Jim Harper, Cato Institute

Data breaches are common

- Data breaches are common, even for companies with top security systems
  - RSA data breach with Lockheed Martin records
  - Over 30 million sensitive records compromised in 2011

SB 98 Increases Privacy Protections

- Increases Privacy Protections
  - Clear notification, authorization and usage
  - No distribution or sale of information, safe storage
  - Requires disposal after use
  - Possible civil suits for violations

SB 98 Gives Alaskans a Choice

- Alternative ID section preserves choice
- Proposed alternative language
  - Sec 18.14.040. Alternative identification. If a person who administers an examination requires an individual taking the examination to provide biometric information to the person for the purposes of identifying the individual taking the examination, the person may not require that the individual provide the biometric information if the individual provides the person with a passport, or an alternative identification acceptable to the person administering the examination.

Conclusion

- SB 98 is a compromise
- Not a ban on obtaining biometric information
- SB 98 simply adds reasonable protections and preserves choice

Walter Hamilton Response to Questions

1: What good/bad do you see in SB 98?

The bill targets a specific technology and places general restrictions on the use of biometrics. We don't believe that such legislation is appropriate because (i) it would discourage the use of biometrics as a legitimate and efficient tool for protection against fraud, identity theft and unauthorized access, (ii) it may have unintended consequences that are hard to predict, (iii) it can lead to excessive litigation, and (iv) it may weaken the security of certain applications by giving the individual the sole option of providing less secure forms of identification. We believe that the concerns that originally led to this bill result from a basic misunderstanding of biometric technology and how it is used.

2: What would you recommend the AK Legislature do regarding private and public sector uses of biometric information? Should we focus on restricting the use of new technologies or make sure strong liability protections are in place?

We believe that biometric data should be treated like other personally identifiable information (PII) and should be protected and not shared without informed consent. The biometrics industry has supported voluntary standards for such data protection for years. However, we believe that any legislation that is considered should avoid singling out a specific technology but should instead set standards and safeguards to protect the security of all personally identifiable information, including biometric data.

3: Unless clearly identifiable harm occurs to private individuals, should the AK legislature restrict the flow of information or what types are collected? How do you define harm? Should the government or the consumer have the final say in how personal information is used?

There is less potential for harm from the collection of a person's biometric data than there is from the collection of other sensitive personal information such as credit card numbers, social security numbers, medical information, financial information, etc. Biometric data is not nearly as exploitable in the sense that other sensitive data might be. If an unencrypted biometric record is stolen from a database, the person that obtains the data has no practical way to present it to a biometric sensor to gain the access or privilege that has been granted to the related identity record. Biometric data is mathematically extracted from the original input image or signal into a compact collection of ones and zeros called a "template" which is the format used for all biometric matching systems. A biometric sensor is expecting to see a human face or finger presented to the sensor – not a string of numbers.

Regardless, IBIA believes that biometric data should be subject to the same standards of care that society requires of their other personal information. We do not object to legislation that defines reasonable standards for the protection of personally identifiable information (including biometrics) that is collected by commercial organizations. As previously mentioned, it would be appropriate to include biometrics in a broad definition of personally identifiable information.

4: Describe why you believe current forms of ID verification (driver's license, passports etc.) are inadequate. How does biometrics address this problem? Can biometric information enhance privacy?

There are many web sites that will provide a person with high quality fake government ID documents for a modest fee. These false IDs would be difficult to detect – even by trained security personnel. Depending on the application, an organization may need to conduct additional protective measures to ensure a high level of confidence when establishing an initial identity record. For example, an application for employment could additionally include a check of public records, reference checks, review of other documents and even a criminal history records check through law enforcement agencies. Indeed, many occupations that command a high level of public trust require applicants to submit ten fingerprints to check for criminal records. These include such occupations as airline pilots, school bus drivers, nurses, stock brokers, maritime workers, military personnel, airport workers, bankers, hazardous materials truck drivers, police officers, day care workers, casino workers, etc.

However, for most commercial applications, biometrics does not play a role in the process of establishing the initial identity record. Instead, it is simply used to bind the physical person to their already-established identity record. This allows an organization to quickly and efficiently confirm that the person is still the same person when they appear later to request access, a service or a privilege associated with an identity record. This enhances privacy and protects against identity theft because no one can claim another person's identity since they don't possess the same unique biometric characteristics. Biometric verification of a claimed identity is also convenient and quick for the individual and allows organizations to eliminate reliance on less secure government ID documents or other less secure forms of authentication to confirm a person's claim of identity.

5: Please discuss the differences between verification and identification. Which represents the greater privacy concern?

Biometric verification (or authentication) is the one-to-one comparison of a presented biometric sample to a single previously enrolled biometric record. Biometric verification is always preceded by a claim of identity (such as entering a user name or presenting an access control card) that points to a specific enrolled biometric record. This is followed by presentation of a biometric sample. Biometric verification answers the question "are you who you claim to be?" An example application would be a health care provider accessing a patient's electronic medical record on a computer by entering a user name followed by a biometric - instead of a password.

Biometric identification is the one-to-many comparison of a presented biometric sample against all of the biometric records in a database. An example would be a law enforcement search of criminal records to see if a person has an outstanding warrant or prior conviction. Biometric identification answers the question "who are you?" to see if the person is known in the system. It should be noted that biometric identification can also be used in commercial applications to increase user convenience by eliminating the need to enter a user name or the need to carry an electronic token such as an access control card.

Either method is appropriate for a wide range of applications. However, it is generally felt that biometric one-to-many identification represents more of a privacy concern when used in certain contexts such as covert surveillance applications.

6: Please discuss the concepts of "opt-in" versus "opt-out." Do they apply to SB 98?

In the context of biometrics, opt-in means to explicitly participate in a system that requires an individual to present a biometric characteristic. Opt-out means to explicitly choose not to provide a biometric characteristic when engaged with such a system. If submission of a biometric is a requirement of the system, then a person that opts out would not be a participant in the system. In Sec. 18.14.040, SB 98 allows an individual to provide alternate identification to a person that is administering an occupational examination. This appears to be a form of "opt out" for the individual. Most systems that require biometrics also have a procedure to handle exception situations where an individual is not capable of using the technology due to a physical disability or some other condition. However, for sensitive or high security applications, it is quite unusual to allow the individual to freely choose to offer another less secure form of identification.

7: Please discuss biometric technology in terms of what it should and should not be used for.

Biometric technology should be used as a "gatekeeper" to protect against unauthorized access to certain privileges, sensitive information, or even to secure facilities. There are numerous specific applications where biometrics might play an important role. Following are a few examples.

Biometrics should be used to:

a. Increase the security of information systems and enhance user convenience by replacing passwords which can be hacked, stolen or borrowed.
b. Protect our borders by screening foreign visitors against criminal and terrorist watch lists.
c. Ensure that persons applying for positions of public trust are not a threat to society.
d. Ensure that driver license applicants don't already have a license under another identity.
e. Ensure that a person's time card entry at their place of employment was not made by a person committing payroll fraud by "buddy punching" for them.
f. Provide an audit trail of authorized financial transactions that cannot be repudiated.
g. Secure access to patient electronic health records.
h. Match parents with children in day care centers to prevent kidnapping.
i. Prevent bullying for lunch money and to avoid stigmatizing low-income children who receive public assistance for school lunch programs.
j. Confirm that the person appearing for a professional examination is the same person that originally registered to take the exam.

Certain uses of biometric technology can raise worrisome privacy concerns. For example, it is now technically possible to "mine" the Internet using web crawler software to collect and build a repository of tagged facial images without a person's knowledge or consent. These images can then be processed into biometric "faceprints" and searched at high speed to look for matches. Association of these matched faceprints with their tagged biographical information can assist in

building a complete profile of a person that could be used for cyber voyeurism or to steal one's identity. IBIA has made recommendations to the Federal Trade Commission to address such concerns which have been appropriately raised by members of Congress.

8: Should private and public personal information databases be strictly separated?

The context of the question is difficult to understand without an example. However, it is generally considered best privacy practice to separate biometric data from personally identifiable biographical or other data. Such records would be linked using unique identifier numbers. If a biometric database was compromised, there would be no association with a person's biographical other personal information.

9: Talk about biometric "liveness." Is a non-live sample useful? Is biometric data easily reverse engineered?

It is possible to "spoof" some biometric sensors through the presentation of a fake biometric sample. An example would be a mold of someone's fingerprint or a photo of someone's face or iris pattern. The biometrics industry recognized this as a legitimate concern some years ago and has vigorously invested research and development effort into building countermeasures into sensor hardware and software that detect "liveness" of the presented biometric sample. These liveness detection features are now commercially available in many biometric products and include such techniques as detecting the presence of blood in human tissue through reflected visible or infrared light. Other techniques measure involuntary motion of the face or eye. Still other techniques measure electrical frequency emitting by living human tissue. The value proposition of such countermeasures varies widely depending on the risk/management assessment of the application. Generally, applications for unattended or remote use of biometrics should use biometric systems that detect liveness.

Contrary to media coverage of some laboratory experiments that suggests otherwise, biometric data in a template format cannot be reconstructed into the original image that a human would recognize. Simply put, too much visual data has been lost during the template generation process. It may be possible to reconstruct partial vectors of a fingerprint pattern from a processed fingerprint template and have that pattern recognized by a template generation algorithm. However, a human would not see the reconstructed image as resembling a fingerprint pattern and there is no practical way of presenting the reconstructed image to a fingerprint sensor – particularly if the sensor is equipped with liveness detection features.

10: Is biometric information used in the same manner as my buying history, credit reports, and websites I visit? Is it similarly bought and sold?

Biometric information has little or no value to a commercial organization that is interested in buying or selling personal buying pattern information for marketing purposes. We are not aware of any sale of biometric data for marketing or other commercial purposes.

11: In terms of a cost benefit analysis, what expertise would it take to find, steal, and replicate another person's biometric information? Is there an incentive to steal biometric information in order to commit other crimes or is it a CSI/Mission Impossible "perfect crime?"

Generally, a biometric is not a secret. A human face is a biometric that can be observed and photographed. An individual's fingerprint pattern can be lifted from a cup of coffee. An iris pattern can be photographed with a high resolution camera. For these biometric modalities, it doesn't take a lot of expertise to obtain the biometric characteristics of a person – even without their knowledge or consent.

However, the criminal or hacker has the non-trivial problem of how to exploit the biometric information. They would have great difficulty mimicking the biometric characteristics of another person using collected images – particularly if the biometric sensor is equipped with liveness detection features. The problem is in no way equivalent to the situation where the criminal possesses an ID card, a PIN or a password and can easily exploit it.

The challenge for the criminal or hacker becomes even more difficult when they obtain processed biometric data that was stored in a database. This data is typically in the form of compact digital template records instead of the initial raw biometric data or image. The template is a much smaller record that contains a mathematical representation of the biometric features.

Criminals and hackers will attack systems at their weakest points and where attacks are easiest to mount. Biometric-based attacks are extremely difficult to conduct and have a low chance of success. In terms of a cost benefit analysis, an attacker is unlikely to choose the biometric elements of a system as a point of attack and will likely look for other areas of greater vulnerability.

12: Is the consequences of stolen biometric information as great as the consequences of someone accessing my bank account for example?

Hacking into someone's bank account will have far more damaging consequences than having their biometric stolen. As previously stated, stolen biometric information is extremely difficult to exploit.

Citizens for Privacy in Alaska

"Our goal is to make illegal the practice of requiring innocent people to provide fingerprints or other biometrics as identification when they are willing to show their driver's license (State/military issued ID) or a United States passport."

We are very concerned with the rapid erosion of our privacy rights, and we urge you to support legislation to strengthen our biometric privacy laws this session. If someone can present a valid US Passport OR a driver's license (State issued ID) as identification, they should be exempt from any biometrics (fingerprints)-as-ID mandate *(note that criminal background checks will not be affected by this legislation. This legislation is specifically focused on biometrics-as-ID mandates).*

	STATUS: AGREED WITH THE GOAL?	FIRST & LAST NAME	ORGANIZATION	TITLE	CITY & STATE	PERSONAL STATEMENT
	SEE STATEMENT	Whitney Brewster	Alaska State Director, Division of Motor Vehicles	Director	Anchorage, AK	"The Alaska State Division of Motor Vehicles has no interest in capturing Alaskans fingerprints, retinal or iris scans, palm veins or other biometric information."
1	**YES**	**Horst Poepperl**	Borealis Broadband Co	President, IT security expert	Anchorage, AK	

1	**SEE STATEMENT**	Jeffrey Mittman	ACLU - Alaska	Executive Director	Anchorage, AK	"...the ACLU of Alaska endorses protection for individuals' personal biometric information, and applauds the proactive introduction of this bill (SB190) to avoid violations before they occur. The ACLU will be pleased to support SB190 subsequent to the minor revisions outlined below..."
	YES	Gretchen Guess	Alaska	Former Senator	Anchorage, AK	"I AGREE..... thank you for taking up the cause...I know the time and energy it takes to get one of these bills past the choicepoint lobbyists..."
	YES	Mark Lerner	Stop Real ID National Coalition	President, Founder	Missouri	"I AGREE. Information is being shared far more broadly than anyone is being told. Most importantly, the courts have not previously factored in that biometrics do not determine identity, breeder documents do."
2	**YES**	Jason Giaimo	Net Gain Business Consultants of Alaska	President. Former VP of the Alaska chapter of the Institute of Management Accountants	Anchorage, AK	Our privacy is guaranteed by Section 22 of the Alaska State Constitution, "The right of the people to privacy is recognized and shall not be infringed." Our privacy laws urgently need to be updated to reflect new technology, to include biometrics, and to stem the rapid erosion of our privacy.
2	**YES**	Tim Pearson	Pearson Consulting	President, Pearson Consulting	Anchorage, AK	I AGREE and look forward to helping you with this campaign!

2	**YES**	Allan Johnston	Wedbush Morgan Securities	Managing Director, Retired	Anchorage, AK	
2	**YES**	Tyler Arnold	TylerSystems Inc.	President & CEO	Anchorage, AK	"Being forced to hand over private data, that will in turn be commercialized, just so I can gain a common industry accreditation is simply unacceptable. I look forward to doing everything I can to pass sensible legislation that will help me preserve my rights as an Alaskan citizen. "
2	**YES**	Barbara Brown	Alaska voter	Alaska voter	Anchorage, AK	Oh, this steams me up. I am so sorry for you, and I AGREE with you…NO FINGERPRINTS!
2	**YES**	Dan Boland	State of Alaska, Audit Division	Auditor, State of Alaska	Anchorage, AK	"This whole thing about a foreign (or American) owned company accumulating and storing personal data including biometrics is just criminal. Seems to me, criminals are writing the laws. This biometric requirement should be repealed, apologies sent out to CPA applicants, the data destroyed and the company and the folks promoting it exposed. Additionally those people that instituted this policy both on the national level and the state level should be investigated for improper behavior....I applaud you for standing up to the thugs."

2	**YES**	Patrick Lorenz	British Petroleum	Senior Financial Analyst, BP Alaska	Anchorage, AK	"For what its worth, I do agree with you goal, but if unable to influence the process, would have to weigh the advantages of being a CPA or putting my identity at risk with these companies. Unfortunately I would choose to not take the risk."
	YES	Tim Wiepking	Institute of Management Accountants, fmr. President	Fmr. President	Anchorage, AK	It is very admirable you are standing up to this…I VERY much agree, NO FINGERPRINTS!
	YES	Tom Gill	UAA, formerly with BP	Engineering Dept Student	Anchorage, AK	Finger printing should NOT be the required form of identification to sit for the CPA exam.--Tom Gill
	YES	Karen Demichelis	Demichelis & Associates	President	Anchorage, AK	I SUPPORT THIS!
	YES	Chris Brownwell	Resident, Alaska, noted author			"I agree with your legislation push…(the Federal) policies always have a nefarious, hidden purpose. Leftists want to control our lives and will use our identities to do just that."

	YES	Jack-Taylor Ridgeway	Privacy Rights supporter	Privacy Rights supporter		"All of these oppressive encroachments are whittling away at the average Americans ability to engage in free commerce. These practices are unconstitutional, therefore unlawful....this has got to stop now."
	YES	Hetal Giaimo			Anchorage, AK	Collecting fingerprints as ID is clearly unnecessary when a US passport or drivers license is offered. This is really disgraceful and needs to be stopped.
	YES	Laura Dirksen	20 year teacher at an Anchorge Christian School.	Alaska resident, teacher	Anchorage, AK	Having been a teacher for nearly 20 years at an Anchorage Christian school....I AGREE, our privacy laws need to be updated to prevent fingerprint collection.
	YES	Joe Dirksen	US ARMY	Aircraft specialist	Anchorage, AK	
	YES	Cindy Miller	Accenture	Fmr. Acting CFO, Unocal Alaska	Anchorage, AK	I DO NOT SUPPORT FINGERPRINTING ANYONE FOR ENTRANCE EXAMS! THIS IS ALMOST OBSCENE.

ELECTRONIC FRONTIER FOUNDATION

Biometrics: Who's Watching You?

September 2003

Introduction

Among the many reactions to the September 11 tragedy has been a renewed attention to biometrics. The federal government has led the way with its new concern about border control. Other proposals include the use of biometrics with ID cards and in airports, e.g. video surveillance enhanced by facial-recognition technology.

The purpose of this document is to sketch out EFF's concerns about biometrics. In today's public arena, biometric technologies are being marketed as a "silver bullet" for terrorism; however, very little independent, objective scientific testing of biometrics has been done. Deploying biometric systems without sufficient attention to their dangers makes them likely to be used in a way dangerous to civil liberties. This document is very much a work in progress and we welcome comments.

What Are Biometrics?

Biometrics refers to the automatic identification or identity verification of living persons using their enduring physical or behavioral characteristics. Many body parts, personal characteristics and imaging methods have been suggested and used for biometric systems: fingers, hands, feet, faces, eyes, ears, teeth, veins, voices, signatures, typing styles, gaits and odors.

Our Major Concerns

- **Biometric technology is inherently individuating and interfaces easily to database technology, making privacy violations easier and more damaging.** If we are to deploy such systems, privacy must be designed into them from the beginning, as it is hard to retrofit complex systems for privacy.
- **Biometric systems are useless without a well-considered threat model.** Before deploying any such system on the national stage, we must have a realistic threat model, specifying the categories of people such systems are supposed to target, and the threat they pose in light of their abilities, resources, motivations and goals. Any such system will also need to map out clearly in advance how the system is to work, in both in its successes and in its failures.
- **Biometrics are no substitute for quality data about potential risks.** No matter how accurately a person is identified, identification alone reveals nothing about whether a person is a terrorist. Such information is completely external to any biometric ID system.
- **Biometric identification is only as good as the initial ID.** The quality of the initial "enrollment" or "registration" is crucial. Biometric systems are only as good as the initial identification, which in any foreseeable system will be based on exactly the document-based methods of identification upon which biometrics are supposed to be an improvement. A terrorist with a fake passport would be issued a US visa with his own biometric attached to the name on the phony passport. Unless the terrorist A) has already entered his biometrics into the database, and B) has garnered enough suspicion at the border to merit a full database search, biometrics won't stop him at the border.
- **Biometric identification is often overkill for the task at hand.** It is not necessary to identify a person (and to create a record of their presence at a certain place and time) if all you really want to know is whether they're entitled to do something or be somewhere. When in a bar, customers use IDs to prove they're old enough to drink, not to prove who they are, or to create a record of their presence.
- **Some biometric technologies are discriminatory.**A nontrivial percentage of the population cannot present suitable features to participate in certain biometric systems. Many people have fingers that simply do not "print well." Even if people with "bad prints" represent 1% of the population, this would mean massive inconvenience and suspicion for that minority. And scale matters. The INS, for example, handles about 1 billion distinct entries and exits every year. Even a seemingly low error rate of 0.1% means 1 million errors, each of which translates to INS resources lost following a false lead.
- **Biometric systems' accuracy is impossible to assess before deployment** Accuracy and error rates published by biometric technology vendors are not trustworthy, as biometric error rates are intrinsically manipulable. Biometric systems fail in two ways: false match (incorrectly matching a subject with someone else's reference sample) and false non-match (failing to match a subject with her own reference sample). There's a trade-off between these two types of error, and biometric systems may be "tuned" to favor one error type over another. When subjected to real-world testing in the proposed operating environment, biometric systems frequently fall short of the performance promised by vendors.
- **The cost of failure is high.** If you lose a credit card, you can cancel it and get a new one. If you lose a biometric, you've lost it for life. Any biometric system must be built to the highest levels of data security, including transmission that prevents interception, storage that prevents theft, and system-wide architecture to prevent both intrusion and compromise by corrupt or deceitful agents within the organization.

Despite these concerns, political pressure for increasing use of biometrics appears to be informed and driven more by marketing from the biometrics industry than by scientists. Much federal attention is devoted to deploying biometrics for border security. This is an easy sell,

because immigrants and foreigners are, politically speaking, easy targets. But once a system is created, new uses are usually found for it, and those uses will not likely stop at the border.

With biometric ID systems, as with national ID systems, we must be wary of getting the worst of both worlds: a system that enables greater social surveillance of the population in general, but does not provide increased protection against terrorists.

Some Current Biometric Initiatives

Sec. 403(c) of the **USA-PATRIOT Act** specifically requires the federal government to "develop and certify a technology standard that can be used to verify the identity of persons" applying for or seeking entry into the United States on a U.S. visa "for the purposes of conducting background checks, confirming identity, and ensuring that a person has not received a visa under a different name."

The recently enacted **Enhanced Border Security and Visa Entry Reform Act of 2002**, Sec. 303(b)(1), requires that only "machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers" shall be issued to aliens by October 26, 2004. The Immigration and Naturalization Service (INS) and the State Department currently are evaluating biometrics for use in U.S. border control pursuant to EBSVERA.

Even prior to September 11, however, large-scale civilian biometric identification systems were being pushed. Both the **Personal Responsibility and Work Opportunity Act of 1995** (PRWOA), a welfare reform law, and the **Immigration Control and Financial Responsibility Act of 1996** (ICFRA), an immigration reform law, called for the use of "technology" for identification purposes.

The PRWOA requires the states to implement an electronic benefits transfer program "using the most recent technology available . . . which may include personal identification numbers, photographic identification . . . and other measures to protect against fraud and abuse." This law covers, for example, the Food Stamps program.

The ICFRA requires the President to "develop and recommend . . . a plan for the establishment of a data system or alternative system . . . to verify eligibility for employment in the United States, and immigration status in the United States for purposes of eligibility for benefits under public assistance programs . . . or government benefits." This system "must be capable of reliably determining with respect to an individual whether . . . the individual is claiming the identity of another person."

The **Illegal Immigration Reform and Immigrant Responsibility Act of 1996** (IIRAIRA) requires the INS to include on alien border crossing cards "a biometric identifier (such as the fingerprint or handprint of the alien) that is machine readable." The State Department collects fingerprints and photographs of aliens for these cards.

The **Truck and Bus Safety and Regulatory Reform Act of 1988** (TBSRRA) requires "minimum uniform standards for the biometric identification of commercial drivers."

EFF's concerns about biometrics

Why be concerned about biometrics? Proponents argue that: A) biometrics themselves aren't dangerous because all the real dangers are associated with the database behind the biometric information, which is little different from problems of person-identifying information (PII) databases generally; B) biometrics actually promote privacy, e.g., by enabling more reliable identification and thus frustrating identity fraud.

But biometric systems have many components. Only by analyzing a system as a whole can one understand its costs and benefits. Moreover, we must understand the unspoken commitments any such system imposes.

Surveillance

The chronic, longitudinal capture of biometric data is useful for surveillance purposes. Our Surveillance Monitor page highlights some of these issues. Biometric systems entail repeat surveillance, requiring an initial capture and then later captures.

Another major issue relates to the "voluntariness" of capture. Some biometrics, like faces, voices, and fingerprints, are easily "grabbed." Other biometrics, at least under present technology, must be consciously "given." It is difficult, for instance, to capture a scan of a person's retina or to gather a hand geometry image without the subject's cooperation. Easily grabbed biometrics are a problem because people can't control when they're being put into the system or when they're being tracked. But even hard-to-grab biometrics involve a trust issue in the biometric capture device and the overall system architecture.

Databases

To be effective, a biometric system must compare captured biometric data to a biometric database. Our National ID System page highlights issues surrounding database abuse, which has both static and dynamic dimensions.

The static issues surrounding databases are mainly about safeguarding large and valuable collections of personally identifying information. If these databases are part of an important security system, then they (and the channels used to share PII) are natural targets for attack, theft, compromise, and malicious or fraudulent use.

The dynamic issues surrounding databases mainly concern the need to maintain reliable, up-to-date information. Databases that seek to maintain accurate residence information must be updated whenever one moves. Databases that are used to establish eligibility for benefits must be updated so as to exclude persons no longer eligible. The broader the function of the system, the more and broader the updating that is required, increasing the role of general social surveillance in the system.

It may seem that one of the issues that plagues token-based ID systems (like ID cards) -- the security or integrity of the token itself -- does not apply for biometric systems, because "you are your ID." But the question of the reliability of the token is really a question about trust. In an ID card system, the question is whether the system can trust the card. In biometric systems, the question is whether the individual can trust the system. If someone else captures your signature, fingerprint, or voice, for instance, what prevents it from being used by others? Any use of biometrics with a scanner run by someone else involves trusting someone's claim about what the scanner does and how the captured information will be used.

Vendors and scanner operators may say that they protect privacy in some way, perhaps by hashing the biometric data or designing the database to enforce a privacy policy. But the end user typically has no way to verify whether such technical protections are effective or implemented properly. End-users should be able to verify any such claims, and to leave the system completely if they are not satisfied. Exiting the system, of course, should at least include the expungement of the end-user's biometric data and records.

Linking

An oft-noted risk of biometric systems is the use of biometrics as a linking identifier. This risk, of course, depends to some extent on standardization. Consider, for instance, the use of the Social Security number as a linker across disparate databases. While the private sector would not have been able to develop anything like the SSN on its own, once the government created this identifier, it became a standard way of identifying individuals. Standardization therefore creates new privacy risks because information gathered for one purpose can be used for completely unrelated, unconsented-to purposes.

Currently, Automated Fingerprint ID Systems (AFIS) are heavily used by the government in connection with law enforcement, but there is at present little standardization within the AFIS industry. If law enforcement and private industry were to unify their fingerprint databases under one common standard, such as under a national ID system, this would potentially put one's entire life history in interoperating databases that are only a fingerprint away.

Tracking

By far the most significant negative aspect of biometric ID systems is their potential to locate and track people physically. While many surveillance systems seek to locate and track, biometric systems present the greatest danger precisely because they promise extremely high accuracy. Whether a specific biometric system actually poses a risk of such tracking depends on how it is designed.

Why should we care about perfect tracking? EFF believes that perfect tracking is inimical to a free society. A society in which everyone's actions are tracked is not, in principle, free. It may be a livable society, but would not be our society.

EFF believes that perfect surveillance, even without any deliberate abuse, would have an extraordinary chilling effect on artistic and scientific inventiveness and on political expression. This concern underlies constitutional protection for anonymity, both as an aspect of First Amendment freedoms of speech and association, and as an aspect of Fourth Amendment privacy.

Implemented improperly, biometric systems could:

- increase the visibility of individual behavior. This makes it easier for measures to be taken against individuals by agents of the government, by corporations, and by our peers.
- result in politically damaging and personally embarrassing disclosures, blackmail and extortion. This hurts democracy, because it reduces the willingness of competent people to participate in public life.
- increase the 'circumstantial evidence' available for criminal prosecution. This might dramatically affect the existing balance of plausible -sounding evidence available to prosecutors, and hence increase the incidence of wrongful conviction. Many criminal cases are decided by plea bargaining, a process that is sensitive to the perceived quality of evidence. Even ambiguous or spurious evidence generated by complex technical systems may be difficult for overburdened public defenders to challenge.
- enable the matching of people's behavior against pre-determined patterns. This could be used by the government to generate suspicion, or by the private sector to classify individuals into micro-markets, the better to manipulate consumer behavior.
- aid in repressing readily locatable and trackable individuals. While the public's concern is usually focused on the exercise of state power, these technologies may also greatly empower corporations. If proper privacy safeguards are not constructed into such systems, they would prove useful in dealing with such troublesome opponents as competitors, regulators, union organizers, whistleblowers, and lobbyists, as well as employees, consumer activists, customers and suppliers.

The Attributes of Biometric Systems

How Do Biometrics Compare to Other Types of ID?

Currently other than personally recognizing someone, or having a trusted third party personally swear to their identity, the only other technique for identifying a person is through the use of a "token." These tokens, which are in essence representations of the oath of a trusted third party, come in two basic forms:

- **Knowledge tokens**, such as passwords, secret PINs (Personal Identification Numbers), or knowledge of personal data (knowing one's mother's maiden name, e.g.), or
- **Physical tokens** such as ID cards, passports, chip cards, or plain old keys.

Token IDs offer certain advantages over biometric identification. Security against "false acceptance" of impostors can be raised by increasing the complexity of the token used for identification. Also, in the event of loss or compromise, the token, be it a password, PIN, key, or ID card, can be revoked, changed or reissued, a biometric measurement cannot.

The advantage of biometrics is that unlike tokens, biometrics cannot be lost, loaned, or forgotten. Token-based systems must verify that the presenter is the authorized user, not an unauthorized person who has come to possess the token.

Used carefully, biometrics may be combined with token-based systems to mitigate the vulnerability of ID tokens to unauthorized use.

Functions of Biometric Systems

One useful way of thinking about biometrics is that they are used for one of two purposes: A) To prove that you are who you say you are (positive ID), or B) To prove that you are not who you say you are not (negative ID).

In a positive ID situation, the subject asserts that she is Jane Doe and submits a "live" sample (a fingerprint, for example) to the system. The system then checks its database of previously enrolled or registered samples to see if the live sample matches the reference sample. A positive ID system is designed to prevent more than one person from using a single identity.

In a negative ID situation, John Roe claims *not* to be someone already known to the system. Here, the system checks its database to see that Roe is not on the watchlist of suspected criminals and terrorists, whose biometrics are already in the system. A negative ID system is designed to prevent one person from using more than one identity.

When biometrics are employed to effect negative identification, one need not be enrolled. The only persons who must be "in" the database are those whom the operator is trying to keep out or catch.

Biometrics alone cannot establish "true identity." A biometric system cannot prevent someone from furnishing fake credentials when they first enter the system. They can only prevent them from using another identity once enrolled.

Common Aspects of All Biometric Systems:

All biometric technology systems have certain aspects in common. All are dependent upon an accurate reference or "registration" sample. If a biometric system is to identify a person, it first must have this sample, positively linked to the subject, to compare against. Modern biometric identification systems, based on digital technology, analyze personal physical attributes at the time of registration and distill them into a series of numbers. Once this reference sample is in the system, future attempts to identify a person are based on a comparison of a "live" sample and the reference sample or samples.

A perfect system would recognize a person 100% of the time, and reject an impostor 100% of the time. However, biometric samples are gathered from people in environmental conditions that are uncontrollable, over equipment that may slowly be wearing out, and using technologies and methods that vary in their level of precision. Consequently, the accuracy of biometric systems is assessed in light of these confounding variables via its tendency to experience either a "false match" (also called a "false accept") or a "false non-match" ("false reject"). The point at which these two rates intersect is called the equal error rate or crossover point.

Biometric systems may be "tuned" to diverge from the equal error rate to provide a match threshhold that satisfies the designer's requirements. If a system compares a large number of persons against a small number of samples, and the consequence of a false match is low, (for example, at a border crossing or airport that is looking for a short list of criminals) a system biased towards a higher "false accept" or "false match" rate may be desirable. The advantage to biasing a system in this manner is that it is likely to err on the side of safety, and less likely to let a criminal slip through undetected. The disadvantage is that the system will falsely associate innocent people with criminals. If other safeguards are in place and the system operators understand the system's bias towards false match, the result can be a relatively trivial loss of convenience due to increased scrutiny (extra inspection of luggage, questioning, etc.) Biasing such a system towards a high "false non-match" or "false reject" rate will result in fewer passengers slowed down at the gate, but at the cost of possibly losing the sought-after criminals.

When assessing the utility or the cost of a biometric system, it's important to bear the common features of all such systems in mind. How is the reference sample to be gathered and catalogued? How it the live sample going to be gathered? Can a live sample be captured without the subject's knowledge and cooperation? What are the implications of all four possible outcomes (true match, true non-match, false match, false non-match)? What is the value of a successful system, and what is the cost, to all parties, should it fail?

Further, we should not assess failure simply from the perspective of the core biometric technology itself. Even an ideal system can be defeated easily if it is incorporated into an insecure or poorly-designed overall system architecture. Any biometric system, especially one that involves a component of telecommunication, **must** be very carefully designed to prevent the loss or interception of user biometrics. Any deployed system must incorporate safeguards to prevent the interception of biometric data while it is being communicated. If a user's biometric is intercepted, criminals may be able to replicate either the sample itself or the string of binary data produced by a successfully-matched sample. Armed with such intercepted biometric data, a criminal would be able to effect a potentially very damaging identity theft.

Types of Biometrics

A proper assessment is built not only on a general understanding of biometrics, but also on an understanding of specific technologies. An understanding of both biometrics in general and specific biometric technologies is a necessary condition for a solid understanding of the larger social implications of biometrics.

Signature

The biometric most familiar to us is the signature. Our ability to judge by sight if one signature matches another has made this a time-proven and legally-binding biometric. However, by sight alone, most of us cannot recognize the pressure of the pen on the paper or the speed and rhythms of its traverse of the page. Computers can do all these things, and quantify, analyze and compare each of these properties to make signature recognition a viable biometric technology. Being based on things that are not visible (pen pressure and velocity, for example), signature-based biometric technology, offers a distinct advantage over regular signature verification -- in addition to mimicking the letter forms, any potential forger has to fabricate a signature at the same speed, and with the same pen weight, as his victim.

Signature biometrics pose a couple of unique problems. The first is the comfort with which people are already willing to use their signature as a form of identification. While this high level of consumer acceptance is viewed as a strength by vendors of such systems, this bears with it a strong downside. Without proper notification, a person may sign an electronic signature pad and unwittingly also be surrendering a reference or live biometric sample. Since the custom of leaving a signature as one's "official mark" is based on the presumption of irreproducibility (i.e., that a forger would be hard-pressed to imitate a signature just by looking at it), people are willing to provide a signature without giving its potential for reproduction a second thought. However, electronic data is easy to copy and transmit. And so, a forger posing as a delivery man might fraudulently secure a signature biometric by presenting a victim with a "gift" box, requesting a signature to confirm delivery, and making off with the victim's biometric data.

The second unique property of signature biometrics is that unlike all other biometrics, which either establish an identity (identification) or confirm an identity (authentication), a signature can convey *intent* (authorization). In other words, a traditional signature on paper is taken both to authenticate the signator, and to convey the signator's legal authority. An electronic system that solicits a user's non-signature biometric must provide a separate step to convey the user's legal authorization for any binding transaction. A signature-based biometric system could mimic our current legally customary acceptance of a signature to simultaneously convey both identity and authority.

Keystroke Dynamics

The rhythms with which one types at a keyboard are sufficiently distinctive to form the basis of the biometric technology known as keystroke dynamics. While distinct, keystroke dynamics are not sufficiently unique to provide identification, but can be used to confirm a user's identity.

Keystroke dynamics, unlike other biometric technologies, is 100% software-based, requiring no sensor more sophisticated than a home computer. Because of this, deployment is occurring in fairly low-stakes, computer-centric applications, such as content filtering (Net Nanny owns BioPassword, the leading keystroke dynamics vendor) and digital rights management, in which passwords to download music are bolstered with by keystroke dynamic verification, to prevent password-sharing. As a general rule, any method involving home or office computers is inherently insecure, as these devices leave a lot more room for experimentation than devices like ATMs or entry systems, and the information they use tends to travel over unsecured communication lines.

Hand Geometry

Perhaps the most ubiquitous electronic biometric systems are hand geometry based. Hand-geometry-based systems require the subject to place his or her hand (usually the right hand) on a plate where it is photographically captured and measured. Made of 27 bones and a complex web of interconnected joints, muscles, and tendons, the human hand presents a sufficiently peculiar conformation of anatomical features to enable authentication, but is not considered sufficiently unique to provide full identification. Further, the geometry of the hand is variable over time, as hand shape may be altered due to injury, disease, aging, or dramatic weight swings. A simple hand-geometry system will measure length and thickness of digits, width of the palm at various points, and the radius of the palm. This results in a relatively simple identification that can be expressed in a very simple, compact string of data. Efforts have been made to improve the accuracy of hand geometry, including three-dimensional sampling (i.e., a second camera measuring the thickness of the hand from the side), and a patented

system (owned by the British concern, Neusciences) that measures the pattern of the veins of the hand. Neusciences claims that their system provides a high degree of accuracy and that the hand vein feature is unique and relatively invariable, changing little over a person's lifespan.

In deployment, traditional hand geometry systems have found acceptance in applications requiring verification of an identity, rather than a full proof or establishment of an identity. Airports, prisons, and factories have successfully employed hand-geometry-based systems to restrict access to runways, to prevent walk-out escapes during visits, and to ensure that time cards are being punched only by the worker, and not by that worker's pal on his or her behalf. In all these instances, the subject is attempting to prove or disprove his or her membership in a relatively small group of people (authorized runway personnel, prisoners/visiting family, factory workers). When stakes are high, these systems are not relied on exclusively to confirm identity; rather, they are used to provide an additional layer of security above and beyond that provided by existing security systems.

Since they must accommodate the largest of hands, any hand geometry or hand vein system must be somewhat bulky, and requires the user to perform an obtrusive task (placing his or her hand on the platen for sampling). Because of this obtrusiveness, hand-based biometrics represent less of a privacy threat than some other systems: subjects cannot have their biometric features sampled without their knowledge, and the sampling method is unambiguous in its intent.

Fingerprint

Fingerprinting is a highly familiar and well-established biometric science. The traditional use of fingerprinting, of course, has been as a forensic criminological technique, used to identify perpetrators by the fingerprints they leave behind them at crime scenes. Scientists compare a latent sample left at a crime scene against a known sample taken from a suspect. This comparison uses the unique features of any given fingerprint, including its overall shape, and the pattern of ridges, valleys, and their bifurcations and terminations, to establish the identity of the perpetrator.

In the context of modern biometrics, these features, called fingerprint minutiae, can be captured, analyzed, and compared electronically, with correlations drawn between a live sample and a reference sample, as with other biometric technologies. Fingerprints offer tremendous invariability, changing only in size with age, are highly resistant to modification or injury, and very difficult to "forge" in any useful way. Although the development of some sort of surreptitious sensor is not inconceivable, the reality is that sensors remain obtrusive, requiring a willful finger pressure to gather a useful sample. Unlike other systems, based on cameras and high-tech sensors, fingerprint sampling units are compact, rugged, and inexpensive, with commercially available systems from multiple vendors offering very good accuracy. Next-generation scanners can analyze below the surface of the skin, and can add pore pattern recognition in addition to the more obvious minutia of the fingerprint.

Facial Recognition

Facial recognition sprung into the national spotlight during the 2001 Super Bowl, when Tampa police scanned the faces of game fans without their knowledge for the purpose of spotting terrorists in the crowd. While this proved a public relations nightmare in January 2001, the use of this technology in New Orleans at the post-9/11 Super Bowl of 2002 generated little controversy. Facial recognition remains one of the more controversial biometric technologies because of its very *un*obtrusiveness. With good cameras and good lighting, a facial recognition system can sample faces from tremendous distances without the subject's knowledge or consent.

Most facial recognition technology works by one of two methods: facial geometry or eigenface comparison. Facial geometry analysis works by taking a known reference point (for example, the distance from eye to eye), and measuring the various features of the face in their distance and angles from this reference point. Eigenface comparison uses a palette of about 150 facial abstractions, and compares the captured face with these archetypal abstract faces. In laboratory settings, facial recognition results are excellent, but critics have questioned the effectiveness of the technology in real-world circumstances. Nevertheless, the accuracy of facial recognition has been good enough for casinos to have put the the technology to use since the late 1990s as a means to spot banned players. Facial recognition technology proponents claim good performance even against disguises, weight changes, aging, or changes in hairstyle or facial hair.

Eye biometrics: Iris/Retina

The human eye offers two features with excellent properties for identification. Both the iris (the colored part visible at the front of the eye) and the veins of the retina (the thin film of nerve endings inside the eyeball that capture light and send it back to your brain) provide patterns that can uniquely identify an individual. Retinal scanning is the older technology, and requires the subject to look into a reticle and focus on a visible target while the scan is completed. It's definitely one of the more intrusive biometric technologies, with some subjects reporting discomfort at the scanning method. Iris recognition has an advantage in ease of use, in that it merely requires the subject to look at a camera from a distance of three to ten inches. The iris scanner illuminates the iris with invisible infra-red light, which shows details on darker -colored eyes that are not visible to the naked eye. The pattern of lines and colors on the eye are, as with other biometrics, analyzed, digitized, and compared against a reference sample for verification.

Iridian Technologies, who hold the patents on iris recognition, claim that the iris is the most accurate and invariable of biometrics, and that their system is the most accurate form of biometric technology. Iridian's system also has the benefit of extremely swift comparisons. The compay claims that it can match an iris against a database of 100,000 reference samples in 2-3 seconds, whereas a fingerprint search against a comparable database might take 15 minutes.

Voice Verification

None of us finds it remarkable when a friend recognizes our voice on the telephone. However, what we find easy to do is still a very hard problem for computers, especially when their job is to identify someone positively. The prospect of accurate voice verification offers one great advantage, which is that it would allow a remote identification using the phone system, an infrastructure that's already been built and thus has zero client-side cost: no special reader needs to be installed in your home. Even without the phone system, the sampling apparatus, a microphone, remains far cheaper than competing, largely optically-based biometric technologies.

But voice recognition technology is still not good enough to be used as a front-line biometric technology. Simply put, voice verification systems have to account for a lot more variables than do other systems, starting with the inevitable compression of a voice captured by cheap microphones (especially those found on phone handsets), discriminating a voice from background noise and other sonic artifacts, and the human voice's tremendous variability, due to colds, aging, and simple tiredness. Also, just as a voice can be surreptitiously recorded over the telephone or face-to-face, a person's voice can be captured surreptitiously by a third party (either by tapping or bugging) and replayed, or a person's voice might be biometrically sampled remotely without consent during a fake door-to-door or telephone sales call. Because of these difficulties, commercial deployments of voice verification have been limited to "backup" status, systems in which there are other token-based methods of identification, with voice verification providing an added layer of protection.

Characterizing Different Biometrics

Different biometric features have characteristics that make them more or less useful for particular applications. Dr. James Wayman, director of the National Biometric Test Center at San Jose State University, categorizes biometric features in terms of five qualities:

- **Robustness**: repeatable, not subject to large changes.
- **Distinctiveness**: there are wide differences in the pattern among the population.
- **Accessibility**: easily presented to an imaging sensor.
- **Acceptability**: perceived as non-intrusive by the user.
- **Availability**: a user may present a number of independent measurable features.

Dr. Wayman explains these qualities by comparing fingerprinting to hand geometry.

> *"Fingerprints are extremely distinctive, but not very robust, sitting at the very end of the major appendages you use to explore the world. Damaging your fingerprints requires less than a minute of exposure to household cleaning chemicals. Many people have chronically dry skin and cannot present clear prints. Hands are very robust, but not very distinctive. To change your hand geometry, you'd have to hit your hand very hard with a hammer. However, many people (somewhat less than 1 in 100) have hands much like yours, so hand geometry is not very distinctive. Hands are easily presented without much training required, but most people initially misjudge the location of their fingerprints, assuming them to be on the tips of the fingers. Both methods require some "real-time" feedback to the user regarding proper presentation. Both fingerprints and the hand are accessible, being easily presented. In the 1990 Orkand study*, only 8% of customers at Department of Motor Vehicle offices who had just used a biometric device agreed that electronic fingerprinting "invades your privacy." Summarizing the results of a lengthy survey, the study rated the public acceptance of electronic fingerprinting at 96%. To our knowledge, there is no comparable polling of users regarding hand geometry, but we hypothesize that the figures would not be too different. With regard to availability, our studies have shown that a person can present at least 6 nearly-independent fingerprints, but only one hand geometry (your left hand may be a near mirror image of your right)."*
>
> **Orkand Corporation, "Personal Identifier Project: Final Report", April 1990, State of California Department of Motor Vehicles report DMV88-89, reprinted by the U.S. National Biometric Test Center.*

Characterizing Biometric Applications

Dr. Wayman suggests characterizing biometric applications in terms of seven variables:

- **Cooperative vs. Non-Cooperative** This refers to the behavior of the "threat" or would-be deceptive user. Is the "threat" trying to cooperate with the system? If the threat is trying to enter a restricted area, she either cooperates with the positive ID system to try to fool it into thinking she's allowed in, or deceptively tries not to cooperate with a negative ID system so as not to trigger the alarm. One implication of this variable is the scope of database search. In cooperative applications, users may first identify themselves with a card or PIN, so that the system need only match against the claimed identity's template. In non-cooperative applications, users can't be trusted to identify themselves correctly, so the entire database may need to be searched.
- **Overt vs. Covert** Is the user aware that the biometric sampling and identification is occurring?
- **Habituated vs. Non-Habituated** Is the intended user expected to be experienced in the use of the system?
- **Attended vs. Non-Attended** Will the intended user be supervised when using the system?
- **Standard vs. Non-Standard Environment** How controlled are the environmental conditions for operation?
- **Public vs. Private** Will users be customers (public) or employees (private)?
- **Open vs. Closed** Will the application be required to exchange biometric data with other systems or not?

Dr. Wayman explains that the positive biometric identification (hand geometry) of users of the Immigration and Naturalization Service's Passenger Accelerated Service System (INSPASS) for rapidly admitting frequent travelers into the United States:

> *"can be classified as a cooperative, overt, non-attended, non-habituated, standard environment, public, closed application. The system is cooperative because those wishing to defeat the system will attempt to be identified as someone already holding a pass. It will be overt because all will be aware that they are required to give a biometric measure as a condition of enrollment into this system. It will be non-attended and in a standard environment because collection of the biometric will occur near the passport inspection counter inside the airports, but not under the direct observation of an INS employee. It will be non-habituated because most international travelers use the system less than once per month. The system is public because enrollment is open to any frequent traveler into the United States. It is closed because INSPASS does not exchange biometric information with any other system." (emphases added)*

Characterizing Biometric ID Systems

Dr. Wayman suggests that biometric ID systems should be viewed in terms of a generic biometric system made up of five basic components or subsystems, depending on the application: data collection, transmission, signal processing (which comprises feature extraction, quality control, pattern matching), storage, and decision.

- **Data collection** Biometric systems involve at least two discrete data collection steps. First, any biometric system must contain a biometric characteristic deemed "true" or canonical from the system's viewpoint. The term "enrollment" or "registration" refers to the first entry of biometric data into the database. Second, the system must compare a later-submitted "sample" (often called a "live sample") to the sample in the database. (Scale is crucial to the enrollment step, sometimes for quite mundane reasons. In the context of biometric visa issuance by the State Department, for instance, the government has been looking at whether or not U.S. consulates around the world have room to handle the additional equipment and physical traffic needed for data collection.)
- **Transmission** Many biometric systems collect data at one location but store and/or process it at another. Such systems require data transmission.
- **Signal processing** Once a biometric is acquired, it must be prepared for comparison. There are three basic tasks here: feature extraction, quality control, and pattern matching. A fourth task in large-scale systems is pattern classification.
  - *Feature extraction* involves finding the true biometric pattern amid noise and signal degradation, preserving the critical information, and discarding redundant or unnecessary data. Dr. Wayman gives the example of a text-independent speaker-recognition system. A properly implemented system isolates "features that depend only on the speaker and not on the words being spoken." At the same time, the system focuses on features that do not change "even if the speaker has a cold or is not speaking directly into the microphone."
  - *Quality control* involves checking to see if the signal is of good quality. Ideally, it should be possible to make a quick determination so that another measure can be taken if the signal is inadequate.
  - *Pattern matching* involves comparing the live sample to the reference sample in the database. If the user claims to be Jane Doe, the pattern-matching process may only need to compare the sample to Jane Doe's stored template. In other situations, the sample must be compared to multiple templates. The pattern-matching process generates a quantitative "distance" measure of the comparison -- how close are they? Even for the same person, the distance is rarely if ever zero.
  - *Pattern classification* is a technique aimed at reducing the computational overhead of pattern matching. In large-scale systems, it can be computationally taxing to match each sample against all stored templates in the database. If biometric patterns can be categorized, then it may be possible to perform the match against only the stored templates in that category. This is sometimes referred to as "binning." A different technique with the same goal is "filtering," which involves partitioning the database based on information not contained in the biometric itself. If you know the person is a man, you don't need to check against women's biometrics. Both of these techniques introduce additional error possibilities; if binning or filtering is erroneous, then the true template is not used and a false non-match results.
- **Decision** This subsystem implements the biometric ID system's actual policy with regard to matching. In general, lowering the number of false non-matches raises the number of false matches, and vice versa. The signal processing subsystem yields a quantitative "distance" measure, but "how close or far is enough?" is a matter of policy. In a high-security application where the cost of a false acceptance could be high, system policy might prefer very few false acceptances and many more false rejections. In a commercial setting where the cost of a false acceptance could be small and treated as a cost of doing business, system policy might favor false acceptances in order not to falsely reject and thereby inconvenience large numbers of legitimate customers. The inevitable existence of these errors means that any biometric ID system must also have well-designed policies for exception handling.
- **Storage** Biometric reference samples must be stored somewhere for matching purposes. For systems only performing "one-to-one" matching, the database may be distributed on cards carried by each enrolled user. The user simply presents his or her biometric and the system checks to see if it matches the template stored on the card. Depending upon system policy, no central database need exist, although in this application a centralized database can be used to detect counterfeit cards or to reissue lost cards without re-collecting the biometric pattern.

  In other cases, centralized storage is necessary because the system must match the live sample to multiple templates. As the number of templates grows, speed becomes an increasingly significant issue. One technique is to partition the database (i.e., binning or filtering) so that any sample need only be matched to the templates in one partition. This increases system speed and decreases false

matches at the expense of increasing the false non-match rate owing to partitioning errors. System error rates thus change with increasing database size and ID systems do not linearly scale.

Full biometric patterns cannot be reconstructed from the stored reference samples if these are stored as templates, which reduce data richness dramatically. Templates themselves are often created using the system vendor's proprietary feature extraction algorithms. Whether stored templates themselves can be used to "spoof" the system internally is entirely dependent on the security of the system architecture.

Biometric ID systems may store not only the templates but also raw data. One reason to do so would be to allow changes to the system or to change system vendors without having to re-collect data from all enrolled users. Full raw data storage is a riskier practice in that new templates may be extracted from the data or the raw data itself may be used against the system.

The State of Scientific Testing of Biometric ID Systems

According to Dr. Wayman,

> *"Testing of biometric devices requires repeat visits with multiple human subjects. Further, the generally low error rates mean that many human subjects are required for statistical confidence. Consequently, biometric testing is extremely expensive, generally affordable only by government agencies. Few biometric technologies have undergone rigorous, developer/vendor-independent testing to establish robustness, distinctiveness, accessibility, acceptability and availability in 'real-world' (non-laboratory) applications."*

An in-depth discussion of the statistical methodology in testing biometric ID systems is beyond the scope of this discussion. We recommend Dr. Wayman's website to interested persons. Note, however, that it is very difficult to generalize from test results. At this time, scientists have no way of accurately estimating how large a test is needed to adequately characterize any biometric device in any application, even with advance knowledge of theoretical error rates.

Media Coverage/Resources

Check out this page for helpful resources including lots of media coverage and links related to the topic.

Acknowledgements:

This document was written and compiled by William Abernathy and Lee Tien with editorial assistance from Sarah Granger and technical assistance from Johnson Hor.

Want to learn how you can defend free speech, stand up for privacy, fight for government transparency, support consumer rights, and protect your right to innovation in the digital world? Visit **http://eff.org/fight** to find ways to help.

What Is Privacy in the Context of Biometrics?

The issue of privacy is central to biometrics. Critics complain that the use of biometrics poses a substantial risk to privacy rights. Proponents claim that biometrics protect privacy. Evaluating these arguments requires, in the first instance, an understanding of what privacy means. In this chapter we explore the definition of privacy in general.

Working Definition of Privacy

We all might have strong subjective ideas about what privacy is. Yet, the word "privacy" is hard to define, in part because the meaning depends greatly on the situation, culture, environment, and moment. In the immediate aftermath of September 11, for example, many Americans welcomed more intrusive governmental measures to increase public safety, even though that meant their privacy could suffer. As one New Yorker put it, "I want Big Brother on my shoulder, looking out for me." Pre-September 11, a frequent question asked at "Introduction to Biometrics" seminars was, "What about the privacy concerns?" Post-September 11, the more frequently asked question became, "What about the security aspects?"

Privacy scholar Ruth Gavison sees privacy as consisting of three parts: secrecy, anonymity, and solitude. She offers what is perhaps the extreme privacy model: "Privacy is a limitation of others' access to an individual.... In perfect privacy no one has any information about X, no one pays any attention to X, and no one has physical access to X" (Gavison 1980, 428).

Robert Ellis Smith, the editor of *Privacy Journal*, defines privacy as "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves" (Smith 2000, 6/ Smith 2002, 1–8). This definition hints at three types of privacy recognized by U.S. courts: physical, decisional, and information privacy.

Based on her survey of the extensive privacy literature, however, Professor Lillian R. Bevier concluded that "privacy is a chameleon-like word, used denotatively to designate a range of wildly disparate interests—from confidentiality of personal information to reproductive autonomy—and connotatively to generate goodwill on behalf of whatever interest is being asserted in its name" (Bevier 1995, 458).

Most important from the standpoint of biometrics, privacy includes an aspect of autonomy—as various scholars have expressed it: our control over information about ourselves, control over who can sense us, or control over the intimacies of personal identity. This control over information about us, or what is termed "information privacy" (or "informational privacy"), lies at the heart of the privacy concerns raised by this new technological reality. Individuals have an interest in determining how, when, why, and to whom information about themselves, in the form of a biometric identifier, would be disclosed.

What Privacy Concerns Does the Use of Biometrics Implicate?

With this working definition of privacy in mind, we next discuss the privacy concerns implicated by the use of biometrics. These concerns relate to identification and invasiveness.

The Individual Gives Up a Biometric Identifier

To determine the specific privacy concerns implicated by biometrics, we must first focus on what exactly is disclosed when biometric data is collected. Regardless of whether an individual voluntarily provides a biometric identifier or is forced to surrender it as part of state action or government-required scheme, he is giving up information about himself. When biometrics, like fingerprinting, iris recognition, or retinal scanning is used, he discloses robust and distinctive information about his identity. When other biometrics, such as hand or finger geometry, are used, at a minimum, he discloses accurate information about who he is. Depending on the biometric, he is giving information about himself that could be used to identify him over large-scale databases.

Invasive Aspects of the Information

Beyond this fundamental disclosure, invasive implications might also be related to privacy concerns that stem from the biometric identification information disclosed. These invasive implications for privacy are essentially three-fold:

- The invasive effects of a secondary market, defined as disclosure of the biometric identification information to third parties
- Any invasive information that might be additionally obtained as part of the biometric identifier
- The invasiveness that might be associated with actual physical harm caused by the technology

Invasive Secondary Market Effects Once a biometric identifier is captured or collected from an individual in the primary market, and even if it is captured only once, the biometric identifier could easily be replicated, copied, and otherwise shared among countless public and private sector databases. This sharing in a secondary market could conceivably take place without the individual's knowledge or consent. Indeed, biometric identifiers could be bought and sold in a secondary market much the way names and addresses on mailing lists are currently bought and sold by data merchants.

An example illustrates the secondary market effect: I give my face and fingerprints to my local sports club so I can access the club and keep better track of my workouts. I do this by presenting my face to a camera whenever I enter and by touching my finger to the computer display on the treadmill and other equipment. I get a detailed monthly fitness report. The sports club conveniently enrolled both of my index fingers so I don't even have to remember which pointer

finger to use. After a while, I start receiving marketing information telling me to show up at the local grocery store, retail outlet, and so on, because I am already preregistered and biometrically enrolled in their systems. That's because, along with my facial photograph, the sports club kept my raw data, or file images, in addition to the fingerprint templates, and sold the information to others.

Later, while shopping in the mall, sales associates insist on selling me athletic gear, protein supplements, and diet aids because their facial recognition system identified me as a failed jock from the sports club. Later, the police are confronted with the grisly homicide of the sports club manager in his office, where the only evidence is a single latent print left on the murder weapon. After no matches are made against the FBI's criminal master file, the new sports club management readily agrees to turn over the file images of fingerprints of all its members, including mine, so the latent print can be searched against them.

Particularly with respect to the private sphere, where the conduct of private actors has traditionally been given a large degree of freedom of action from government interference, few current legal limits exist in the United States on the use of biometric information held by private actors. This observation is not meant to suggest that the federal or state governments would not be able to regulate the use of biometric information held by private actors; rather, it emphasizes what the present regulatory baseline is with respect to the regulation of biometric information: Until regulatory action has been taken by government, the use of biometrics is left to the market. The legal situation is very different in the European Union, where a comprehensive privacy protection framework exists.

Invasive Information Is Obtained In addition to the identification information associated with the biometric, invasive information threatening privacy could conceivably include three other types of concerns. First, biometric identifiers could be used extensively for law enforcement purposes, as raised in the sports club example. Fingerprints have long been used by law enforcement, and electronic finger images—or what are in effect the next generation of fingerprints—are presently being used by various law enforcement agencies as part of their databases, such as the FBI's Integrated Automated Fingerprint Identification System (IAFIS).

Second, it is possible (and this point needs to be stressed: *only* possible) that some biometrics might capture more than just mere identification information. Information about a person's health and medical history might also be incidentally obtained. Recent scientific research, while the subject of controversy, suggests that fingerprints might disclose such information about a person. For example, Dr. Howard Chen, in his work on dermatoglyphics, or the study of the patterns of the ridges of the skin on parts of the hands and feet, notes that "certain chromosomal disorders are known to be associated with characteristic dermatoglyphic abnormalities," specifically citing Down syndrome, Turner syndrome, and Klinefelter syndrome as chromosomal disorders that cause unusual fingerprint patterns in a person. Certain nonchromosomal disorders, such as chronic, intestinal pseudo-obstruction (CIP) (described in the next paragraph),

leukemia, breast cancer, and Rubella syndrome, have also been implicated by certain unusual fingerprint patterns.

Dr. Marvin M. Schuster, the recently retired director of the division of digestive diseases at Johns Hopkins Bayview Medical Center, has discovered a "mysterious relationship" between an uncommon fingerprint pattern, known as a digital arch, and a medical disorder called CIP that affects 50,000 people nationwide. Based on the results of a seven-year study, Dr. Schuster found that 54 percent of CIP patients have this rare digital arch fingerprint pattern. In comparison, arch fingerprints appear in only seven percent of the general population. Schuster's discovery suggests a genetic basis to the disease. Schuster explained that in the case of CIP, "the more digital arches there are in the fingerprint, the stronger the correlation [to the condition]. The majority of CIP patients possess at least one digital arch. This discovery offers an important clue in diagnosing CIP, and it suggests that the disorder is congenital. It could potentially save people with CIP from multiple needless operations" (Hancock and Hendricks 1996).

While still extremely controversial within the scientific communities, several researchers report a link between fingerprints and homosexuality. For example, psychologists at the University of Western Ontario report that homosexual males are more likely than their heterosexual counterparts to show asymmetry in their fingerprints. "What we found is a statistically significant difference between groups of heterosexual and homosexual men," researcher Doreen Kimura said (Associated Press 1994). While this research is far from conclusive, the availability of such information with its possible links to medical and related information again raises concern about privacy and can create misperceptions.

From examining the retina or iris, an expert can determine that a patient may be suffering from common afflictions such as diabetes, arteriosclerosis, and hypertension; furthermore, a medical professional can also detect unique diseases of the iris and the retina. Moreover, the onset of certain diseases (such as diabetes) and conditions (such as pregnancy) may cause the retinal pattern to change; are the changes enough to cause a previously enrolled user to be rejected by a system because the user's biometric is no longer recognized by the system? Although both the iris and retina contain medical information, it is by no means obvious that the biometric data taken of the iris or retina implicates privacy concerns related to the disclosure of medical information. A necessary area of further technical inquiry is whether the computerized code taken of the iris or retina actually contains any medical information or if the information captured is sufficient to be used for any type of diagnostic purpose.

Much research remains to be done; however, a biometric identifier with any possible links to medical information will raise lingering questions about the privacy aspects of the information disclosed. More important, the mere perception that such sensitive information may be disclosed could dissuade people from using potentially beneficial biometric systems.

Actual Physical Harm; Physical Invasiveness Part of the "urban legend" surrounding biometrics holds that retinal scanning "shoots a laser beam into the eye." This is not the case, but urban legends die hard. Anecdotally, certain aviators, who are extremely proud of their 20/20 vision, supposedly had a hard time accepting retinal scanning devices in an experimental program because at least some of them feared the devices would adversely affect their perfect vision. Other users feared that diseases, such as conjunctivitis, may result from having to come into close proximity with a binocular-like device that strangers had touched. Some users of biometrics have complained that hand geometry systems dry their hands. Such fears, even when unfounded, can negatively affect the system because dissatisfied users will go out of their way not to cooperate with the system; some may even actively engage in acts of sabotage to prevent its use.

Documented cases of biometrics causing actual harm to a person are difficult, if not impossible, to find, but many of the technologies are fairly new. And to date, no enterprising plaintiff's attorney has brought a class-action lawsuit for personal injury on this biometrics-induced harm basis. The bottom line is that any liability resulting from any proven actual physical harm caused by biometric systems would be addressed by the individual state's tort liability regimes. On a related note, eventually, the judiciary will also have the opportunity to decide the admissibility of biometric identification as scientific evidence using the prevailing standards articulated by the Supreme Court in *Daubert v. Merrell Dow Pharmaceuticals* in 1993.

Biometrics as Privacy's Foe: Criticisms of Biometrics

This section discusses the "foe" side of the coin: the criticisms of biometrics leading to loss of anonymity and autonomy and the "Big Brother" scenario, including the danger of function creep and degradation of the individual's reasonable expectation of privacy.

The Loss of Anonymity; the Loss of Autonomy

A basic criticism of biometrics is that we, as individuals, risk losing our anonymity and autonomy whenever biometric systems are deployed. Part of controlling information about ourselves includes our ability to keep other parties from knowing things about us, like who we are. While we all know that a determined party—whether the government or a private party—can learn our identity (and much more about us), the use of biometrics makes it clear that our identity is now fully established within seconds. As Roger Clarke explains, "The need to identify oneself may be intrinsically distasteful to some people.... They may regard it as demeaning, or implicit recognition that the organization with whom they are dealing exercises power over them" (Clarke 1994).

Robert Ellis Smith agrees, noting that, "In most cases, biometric technology is impersonal" (Smith 1996). At the same time, as the technology improves, its use may become more ubiquitous, and individuals may find that they are required to provide a biometric identifier in unexpected, unwelcome, or unforeseen circumstances. Moreover, you cannot simply "make up" a biometric as you can a name, an address, or a phone number. In this sense, perhaps, the loss of anonymity leads to an inevitable loss of individual autonomy.

Biometrics should not really be blamed for the fact that there is less individual anonymity in society today than in decades or centuries past, however. Rather, far larger economic, political, and technological forces have been at work. America's transformation from an agrarian to industrial to post-industrial service (or "information age") economy, combined with the massive growth of government since the New Deal of the 1930s, have put a greater premium on the need for information about individuals and organizations. At the same time, technical advances have made it much easier and more convenient to collect, compile, and keep extensive information on individuals. This information-centric trend takes place because in the Information Age information has great value as a commodity. The computer, the enabler of "info-centrism," has helped make information a valuable commodity because it can process large amounts of personal information from large numbers of people in little time and at low cost.

While a biometric identifier is an accurate identifier, it is not the first nor the only identifier used to match or locate information about a person. Names and numerical identifiers such as social security numbers, account numbers, and military service numbers have long been used to access files with personal information. Moreover, the impressive search capabilities of computer systems with their abilities to search, for example, the full text of stored documents, make identifiers far less important for locating information about an individual.

We also should not lose sight of the fact that there is usually a good reason why individual recognition in the form of identification or verification is needed. Balancing the equities involved and depending on the case, the benefits—to the individual as well as to society—of establishing a person's identity generally outweigh the costs of losing anonymity. For example, given the massive problem of missing and abused children, many citizens would eagerly support the idea of day care providers using biometrics to make certain that our children get released at the end of the day to a parent or guardian whose identity has been verified. However, reasonable people can disagree as to the cost-benefit analysis.

Similarly, to consider a "pocketbook" example, the world's financial community has long been concerned about growing problems of ATM fraud and unauthorized account access, estimated to cost $500 million a year, check fraud at least $2 billion, and credit card fraud about $1.5 billion per year. The financial services industry believes that a significant percentage of these losses could be eliminated by the use of biometrics, by ensuring that only the authorized account

holder could access the account. MasterCard, for example, has been evaluating various biometrics since 1995 and believes fingerprint technology is the best technology to reduce credit card fraud. According to Joel Lisker, the company's senior vice president of security and risk management, "We estimate that a fingerprint system, fully implemented, could save the financial services industry billions of dollars" (Haapaniemi 1998).

Critics give too much credit to biometrics' alleged ability to erode anonymity without giving enough attention to the market's ability to protect privacy in response. It is not obvious that more anonymity will be lost when biometrics are used. Public and private sector organizations already have the ability to gather substantial amounts of information about individuals by tracking, for example, credit card use, consumer spending, and demographic factors.

A parallel to the financial services industry might be helpful. Despite the existence of many comprehensive payment systems such as credit cards, which combine extreme ease of service with extensive record-keeping, many Americans still prefer to use cash for transactions—a form of payment that leaves virtually no record. An individual who wants anonymity might have to go to greater lengths to get it in the biometric world, but the ability of the marketplace to accommodate a person's desire for anonymity should not be so readily dismissed. Moreover, as explained next, the ability of biometrics to serve as privacy enhancing technologies should not be discounted.

The Biometric-Based "Big Brother" Scenario

Aside from the alliterative qualities the phrase possesses, critics of biometrics seem to inevitably link the technology to "Big Brother." Biometrics, in combination with impressive advancements in computer and related technologies, would, its critics argue, enable the State to monitor the actions and behavior of its citizenry. In this vein, concern has been expressed that biometric identifiers will be used routinely against citizens by law enforcement agencies. As Marc Rotenberg of the Electronic Privacy Information Center has succinctly explained, "Take someone's fingerprint and you have the ability to determine if you have a match for forensic purposes" (American Banker 1996).

This "Big Brother" concern, however, goes beyond normal police work. Every time an individual used her biometric identifier to conduct a transaction, a record would be made in a database that the government, using computer technology, could then match and use against the citizen—even in ways that are not authorized or meet with our disapproval. To borrow the reasoning of a 1973 report on national identity card proposals, the biometric identifier, in ways far more effective than a numerical identifier, "could serve as the skeleton for a national dossier system to maintain information on every citizen from cradle to grave" (U.S. Department of Health, Education and Welfare 1973).

Roger Clarke has perhaps offered the best worst-case *1984*-like scenario:

> Any high-integrity identifier [such as biometrics] represents a threat to civil liberties, because it represents the basis for a ubiquitous identification scheme, and such a scheme provides enormous power over the populace. All human behavior would become transparent to the State, and the scope for nonconformism and dissent would be muted to the point envisaged by the antiutopian novelists (Clarke 1994).

At least one example exists from U.S. history of supposedly confidential records being used in ways never likely intended. In November 1941, almost two weeks before the Japanese attack on Pearl Harbor, President Franklin D. Roosevelt ordered a comprehensive list made to include the names and addresses of all foreign-born and American-born Japanese living in the United States. To compile the list, staffers used 1930 and 1940 census data. Working without the benefit of computers, staffers compiled the list in one week. Following the attack, President Roosevelt issued Executive Order 9066, authorizing military personnel to detain and relocate persons of Japanese ancestry. By the spring of 1942, the U.S. government forced persons of Japanese descent, including U.S. citizens, to relocate from their homes on the West Coast and report to relocation centers. An estimated 120,000 people, many of whom were U.S. citizens, were held without judicial review. John Miller and Stephen Moore, two libertarian scholars, contend, "The history of government programs indicates that privacy rights are violated routinely whenever expediency dictates" (Miller and Moore 1995).

Function Creep

The biometric-based "Big Brother" scenario would not happen instantly. Rather, when first deployed, biometrics would be used for limited, clearly specified, sensible purposes—to combat fraud, to improve airport security, to protect our children, and so on. But consider what Justice Louis Brandeis (of "right to privacy" fame) warned in his famous *Olmstead v. United States* dissent of 1927:

> Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding.

What would inevitably happen over time, according to civil libertarians, is a phenomenon known as "function creep" or "mission creep": identification systems incorporating biometrics would gradually spread to additional purposes not announced or not even intended when the identification systems were originally implemented.

The classic example of function creep is the use of the Social Security Number (SSN) in the United States. Originated in 1936, the SSN's sole purpose was to

facilitate record-keeping for determining the amount of Social Security taxes to credit to each contributor's account. In fact, the original Social Security cards containing the SSN bore the legend, "Not for Identification." By 1961, the Internal Revenue Service (IRS) began using the SSN for tax identification purposes. By 2002, countless transactions from credit to employment to insurance to many states' drivers licenses require a Social Security Number and countless private organizations ask for it even when it is not needed specifically for the transaction at hand. From "Not for Identification," the SSN has become virtual mandatory identification.

Moreover, given the consequences of function creep, the size, power, and scope of government will expand as all citizens get their biometric identifiers thrown into massive government databases by the "men [and women] of zeal, well-meaning but without understanding" about whom Justice Brandeis warned. In effect, an old Russian proverb aptly identifies the danger of biometrics for freedom-loving Americans: "If you are a mushroom, into the basket you must go."

Reduction of the Individual's Reasonable Expectation of Privacy

Just as function creep implies that biometrics will gradually (and innocently) grow to be used by zealous, well-meaning bureaucrats in numerous, creative ways in multiple forums, function creep will also enable the government to use the new technology of biometrics to reduce further over time the citizenry's reasonable expectations of privacy.

Analogies can be drawn from previous cases in which the government has used cutting-edge technology to intrude in an area in which the private actor had manifested a subjective expectation of privacy. For example, the Environmental Protection Agency (EPA), in an effort to investigate industrial pollution, used "the finest precision aerial camera available" mounted in an airplane flying in lawful airspace to take photographs of Dow Chemical Company's 2,000-acre Midland, Michigan, facilities. Fearful that industrial competitors might try to steal its trade secrets, Dow took elaborate precautions at its facility. Despite the precautions the company took to ensure its privacy, the Supreme Court, in a 5–4 vote handed down in 1985, found that Dow had no reasonable, legitimate, and objective expectation of privacy in the area the EPA had photographed. The dissent noted that, by basing its decision on the method of surveillance used by the government, as opposed to the company's reasonable expectation of privacy, the Court ensured that "privacy rights would be seriously at risk as technological advances become generally disseminated and available to society" (*Dow Chemical Co. v. United States*, 476 U.S. 227 (1986)).

Some contend that biometrics is precisely the kind of technological advance the *Dow* dissenters warned about. Citizens no longer would have a reasonable expectation of privacy any time they use a biometric identifier because the gov-

ernment's use of biometrics and computer matching would be merely utilizing commercially available technologies.

Cultural, Religious, and Philosophical Objections

Other criticisms of the use of biometrics originate on cultural, religious, and philosophical grounds. These objections might not be shared by large numbers of people, but to the extent those who advocate them have sincerely held beliefs, they merit discussion.

Cultural: Stigma and Dignity

Simon Davies of Privacy International notes that it is no accident that biometric systems are being tried out most aggressively with welfare recipients. The British scholar contends that they are in no position to resist the State-mandated intrusion. Interestingly, in the 1995 GAO Report on the use of biometrics to deter fraud in the nationwide Electronics Benefit Transfer (EBT) program, the U.S. Department of the Treasury expressed concern over how finger imaging would impact on the dignity of the recipients and called for more testing and study.

While stigma and dignity arguments tied to the less fortunate elements of society have a strong emotional appeal, the available empirical data from Connecticut suggests that the majority of entitlement recipients actually support the use of biometrics. Some have criticized such surveys as flawed because the recipients could be reluctant to provide their true opinions because of retaliation fears.

Religious Objections

Several religious groups criticize biometrics on the ground that individuals are forced to sacrifice a part of themselves to a godless monolith in the form of the State. For example, certain Christians interpret biometrics to be a "mark of the beast," an objection based on language in the New Testament's "Revelation":

> [The Beast] causeth all, both small and great, rich and poor, free and bond, to receive a mark in their right hand, or in their foreheads: And that no man might buy or sell, save that he had the mark, or the name of the beast, or the number of his name.... And his number is six hundred, threescore, and six (Revelation, 13:16–18).

Certain Christians consider biometrics to be the brand discussed in Revelation and biometric readers as the only means of viewing these brands. For example, stressing that "the Bible says the time is going to come when you cannot buy or sell except when a mark is placed on your head or forehead," fundamentalist Christian Pat Robertson has expressed doubts about biometrics and has noted how the technology is proceeding according to scripture. And at least one religious group has complained that the hand geometry devices used by California were making "the mark of the beast" on enrollees' hands.

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

March 14, 2011

The Honorable Bill Wielechowski, Chair
The Honorable Joe Paskvan, Vice-Chair
Senate State Affairs Committee
Alaska State Senate
Juneau, AK 99801
via email: Senator_Bill_Wielechowski@legis.state.ak.us
Senator_Joe_Paskvan@legis.state.ak.us

Re: Senate Bill 98
ACLU Statement of Support

Chair Wielechowski, Vice-Chair Paskvan:

Thank you for the opportunity to submit a written statement of support for SB 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 applauds the proactive introduction of this Bill to avoid 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 are also pleased to note that SB 98 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.

Sincerely,

Jeffrey Mittman
Executive Director
ACLU of Alaska

cc: Senator Albert Kookesh
Senator Kevin Meyer
Senator Catherine Giessel

FTC Fines ChoicePoint $15 Million for Security Breach

Los Angeles Times (LATWP News Service) (CA) - Thursday, January 26, 2006

Author: *Joseph Menn*

The Federal Trade Commission hit data broker ChoicePoint Inc. with the largest civil penalty in the agency's history Thursday for allowing sensitive information on 163,000 consumers to get into the hands of Los Angeles con artists last year.

The commission levied a $10 million penalty, on top of $5 million in restitution, making a total worth more than 10 percent of the company's profit last year. The agency declared that the company gave false assurances to the public about its security precautions while being so careless that it sold information to a purported business customer whose own ChoicePoint file identified a link to possible fraud.

Other con artists posing as customers applied for multiple accounts from the same publicly available fax machine, submitted revoked business licenses and in at least one case omitted the applicant's surname, according to the commission.

While some of the FTC's allegations were previously reported, many of the details were new, including complaints that the company failed to inquire after would-be customers applied with suspended articles of incorporation, mismatching addresses on supporting documents, and contact numbers belonging to residential or cellular phones.

Revealed because of a California disclosure law, the ChoicePoint breach launched a national debate about data security that has prompted new laws in more than a dozen states and 18 pieces of proposed federal legislation.

Most are aimed at making it harder for identity thieves to get Social Security numbers and other information that can be used to open credit accounts and make fraudulent purchases in the names of innocent consumers.

In announcing Thursday's settlement, FTC Chairwoman Deborah Platt Majoras said the commission wanted to serve notice to other businesses that consumer information must be protected.

Data security "must be a priority for financial and corporate America," she said. Signaling that the agency would continue to lead in the enforcement of identity theft, she said consumers should know that "we will make sure that your information is safeguarded and you don't have to worry that it will fall into the wrong hands and harm you."

The action generally won praise from consumer groups. Thursday's penalty "is a lot of money," even for a big company like ChoicePoint, said Chris Hoofnagle, West Coast director of the nonprofit Electronic Privacy Information Center. "It shows that the FTC is getting serious about security."

ChoicePoint still faces several private lawsuits over the data breach. The Securities and Exchange Commission also is investigating whether Chairman Derek Smith and another top executive improperly sold company shares before the breach became public.

The company was informed of the problem months earlier by investigators with the Los Angeles County Sheriff's Department. They arrested a Nigerian national, Olatunji Oluwatosin, who pleaded guilty last month to committing $2.5 million in fraud and is facing at least seven years in jail.

Beginning in January 2002, Oluwatosin used fake businesses with mail drops in Beverly Hills, Hollywood and elsewhere to set up ChoicePoint accounts and access personal information on more than 1,500 people, according to the district attorney's office. Search warrants served on ChoicePoint turned up a much wider fraud

problem.

The FTC cited ChoicePoint for violating the Fair Credit Reporting Act, which requires buyers of credit reports to have a proper purpose, and for violating basic fair-practices laws. It said ChoicePoint unfairly failed to protect consumer information and was deceptive when it made such statements as "Every ChoicePoint customer must successfully complete a rigorous credentialing process."

In legal papers filed with the settlement, the FTC said ChoicePoint improperly released nearly 10,000 credit reports and that about 800 cases of identity theft resulted. The $5 million in restitution will be distributed to those people and future victims of the data breach.

ChoicePoint didn't admit to the FTC assertions or to any wrongdoing in the settlement. It did agree to revamp its procedures in several ways, including instituting mandatory visits to many customers. It also must submit to security audits every two years through 2026.

By itself, the financial payout will do modest harm to ChoicePoint. Even after a charge for the penalty, the Alpharetta, Ga., company reported fourth-quarter earnings of $28 million Thursday on revenue of $258 million.

ChoicePoint shares dropped $3.35, or 7 percent, to $42.95 after the settlement was announced.

Section: *Financial*
Provided By: *Los Angeles Times - Washington Post News Service*
Record Number: *10F6866006A44D58*

THE WALL STREET JOURNAL.
WSJ.com

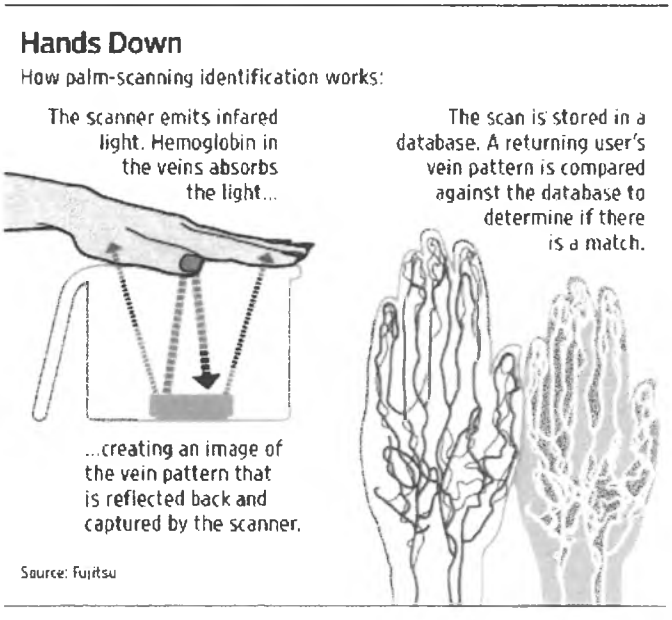
CAREERS | July 22, 2008

Business Schools Try Palm Scans To Finger Cheats

By JOHN HECHINGER

In a sign of increasing concern about cheating, the nation's top business schools will soon require a high-tech identity check for standardized admissions tests.

Aspiring corporate executives taking the Graduate Management Admission Test, or GMAT, will have to undergo a "palm vein" scan, which takes an infrared picture of the blood coursing through their hands. The image -- which resembles a highway interchange in a major city -- is unique to every individual. The scans are used widely in Japan among users of automated teller machines but only recently have appeared in the U.S.



Palm-vein scanning on GMAT test takers will begin next month in Korea and India, with U.S. centers starting as early as this fall and a world-wide rollout by May.

The technology targets "proxy" test taking, a fraud in which applicants hire high-scoring imposters to take the exam in their place. Five years ago, federal authorities broke up a ring of six fraudsters who took more than 590 exams, including GMATs, for customers who paid at least $3,000.

David Wilson, president of the Graduate Management Admission Council, which represents top business schools and oversees the test, won't disclose the level of cheating today but says the case underscored the potential. Since 2006, test takers have been required to undergo digital fingerprinting to validate their identity. They are also photographed, and videotaped taking the exam. The council says the new vein-scan technology is superior and will be more acceptable to consumers, who often associate fingerprinting with the police.

With the palm scan, students will let their hands hover for a few seconds over the device -- a roughly 1.4-inch cube -- which captures the vein patterns in their palms for an image that is archived along with test results.

Raj Nanavati, a partner at International Biometric Group, a consulting firm specializing in identity-verification technology, says vein scans are "very accurate" and "difficult to spoof," especially when compared with cheaper fingerprinting devices.

Fujitsu

Scan of a palm's vein pattern

About 4,000 business programs at 1,800 universities, including most top-ranked institutions, require the GMAT for admission. The business-school council gives 230,000 GMAT tests annually and says it won't raise the exam's $250 price. Japan's Fujitsu Ltd., which makes the scanners, says the device typically costs $1,000 or less. Including training, installation and other costs, London's Pearson PLC, which administers the business-school test for the council, expects to spend millions on the rollout of the vein-scanning technology at more than 450 test centers.

'Protecting the Integrity'

Donald L. McCabe, a Rutgers University professor of management, says it is understandable that business schools are now "protecting the integrity of their test, whatever it takes."

Professor McCabe has surveyed more than 200,000 students over 19 years and concluded that those in business school cheat more than their peers in other disciplines. He says business-school students often cite instances of corporations' "bottom-line mentality" and ethical lapses to justify their own dishonesty.

GMAT officials acknowledged that the new system would do little to deter other forms of cheating. For example, the business-school council recently won a $2.3 million judgment against the operator of a Web site called Scoretop.com, which had been selling questions from recent exams. The council took over the site and now warns visitors that cheaters will have their scores canceled, won't be allowed to take the test again, and could be subject to a civil lawsuit or criminal prosecution.

Other admissions tests employ a variety of security methods. Last year, the administrator of the Medical College Admission Test, or MCAT, began requiring digital fingerprinting. Would-be attorneys who take the Law School Admission Test, or LSAT, submit to old-fashioned ink fingerprinting. Scholars seeking a Ph.D. and sitting for the Graduate Record Examinations, or GRE, need only show a government-issued ID.

Resisting Fingerprinting

High-school students sweating the SAT and ACT, the two main college-entrance exams, don't have to submit to fingerprinting. They are required to show only standard ID. The test administrators say many parents would resist the fingerprinting of their kids, and high-tech solutions would be too costly given what families can afford. Students pay $45, less than a fifth of the cost of the business-school exam, to take the SAT.

Ray Nicosia, head of security for the Educational Testing Service, which administers the SAT, says the Princeton, N.J., nonprofit relies on several other procedures to catch cheating. ETS collects handwriting samples and relies on high-school teachers to identify test takers. Mr. Nicosia says the company also uses computer analysis to flag possible fraud, a practice also used for the ACT. He says ETS has considered more high-tech methods, but "right now, we feel like we've got the right checks and controls in place." Cheating occurs in about one-tenth of 1% of SATs, he says.

Privacy Fears

Beth Givens, director of the Privacy Rights Clearinghouse, a San Diego nonprofit, says any digital fingerprints or vein scans should be discarded after a reasonable period so that they can't be used for other purposes. Privacy advocates fear that fingerprints and other identifiers can be used improperly by authorities, catching innocents in government dragnets.

The Law School Admission Council says it discards its paper fingerprints after five years, in part because of privacy concerns. However, the business admission council says it expects to make the palm-vein scans part of students' permanent records. Joel Hagberg, a vice president at Fujitsu's computer-products division, says

students shouldn't be worried because the police can't use palm-vein scans in their investigations. "You can't leave a vein pattern at a crime scene," he says.

Write to John Hechinger at john.hechinger@wsj.com

Why I Love Biometrics

It's "liveness," not secrecy, that counts.

BY DOROTHY E. DENNING

I'm a big fan of biometrics. I'm tired of trying to remember umpteen zillion account names and passwords in order to use the computers in my office, browse my favorite Web sites and update the Web sites I manage. I long for the day when computers will automatically recognize me and handle the identification and authentication function with little effort on my part.

I make lots of security-related presentations, and when I tell all of this to an audience, someone inevitably asks, "What happens if someone snatches the biometric print used to validate you? Couldn't they just replay your biometric and pretend to be you? Wouldn't that make your biometric as good as useless?"

My response is, "No." A good biometrics system should not depend on secrecy. To understand why, think about how biometrics work in the physical world. Your friends and colleagues authenticate you by recognizing your face, voice, eyes, hands, gait and so on. None of this is secret. Anyone who interacts with you sees these characteristics. Even your fingerprints can be lifted from surfaces.

What makes biometrics successful is not secrecy, but rather the ability to determine "liveness." I can easily distinguish the living, flesh-and-blood you from a statue or photograph of you, or even someone wearing a costume and mask that looks like you. If I don't know you well, I might be fooled by a lookalike, but in the non-*Mission Impossible* real world, the system generally works. If I don't know you at all, I might ask for a photo ID. But I would use such a photo only because I lack knowledge of your appearance. I authenticate you by comparing your live face against the photo, not by comparing one photo against another. For further proof, I may watch you sign your name and compare the live signature against the one on your ID card.

The same principle applies in the digital world. Your biometric prints need not be kept secret, but the validation process must check for liveness of the readings. Many biometric products work this way, and I would like to see product surveys tell me which do and do not. The iris recognition system from **Sensar (www.sensar.com),** for example, looks for the "hippus movement" -- the constant shifting and pulse that takes place in the eye. The liveness test ensures that the reading is fresh, so an adversary can't replay a previously recorded reading.

This is the beauty of biometrics. Other forms of user authentication--including passwords, tokens and encryption--all depend on protecting a secret or device from theft. Once that secret or device is compromised, the system fails until a new one is established. Moreover, these methods

typically require users to hold a different secret with each and every device or service they use, thereby burdening the user. Imagine if every time you greeted a friend or colleague, you had to provide a different secret password!

Testing liveness is reasonably straightforward if the biometrics reader senses appropriate characteristics and is tightly coupled with the validation process and database of biometrics prints. If the reader is remote from the validation process and database, encryption can be used to provide a secure path connecting the components. The encryption system, obviously, should protect against replays. Encryption can also be used to pass credentials from one system to another. For example, once my smart card validates my fingerprint, it may use a private signature key on the card to authenticate me to services that use my public key for authentication. Of course, the encryption system itself requires secret keys, but in this context, the secrets may be less prone to compromise because they don't have to be known by humans.

Biometrics can be applied not only with human users, but also with locations. For example, technology from CyberLocator (www.cyberlocator.com) authenticates geodetic location by capturing a location signature from GPS signals in a way that ensures liveness. No secrets are required. One could imagine using biometrics to authenticate places or anything else with distinguishing characteristics that exhibit a form of liveness.

In addition to liveness, a biometrics system also depends on uniqueness. Otherwise, it may be subject to false accepts or rejects. Some forms of biometrics are better than others in this regard, iris recognition being one of the best.

Questions about privacy abuse aside, biometrics is likely to be the way of the future. I can't wait to get rid of my gazillion passwords and sticky notes.

DOROTHY E. DENNING, Ph.D., is a professor of computer science at Georgetown University and a member of *Information Security*'s Editorial Board.

http://faculty.nps.edu/dedennin/publications/biometrics.pdf

October 25, 2011

SAT Officials Vow More Security After Cheating Arrests on Long Island

By WINNIE HU and JENNY ANDERSON

FARMINGDALE, N.Y. — Stung by the arrest of seven Long Island teenagers accused of cheating on the SAT, the College Board said Tuesday that it was hiring a former F.B.I. director to review its security procedures, and that by the next exams, Nov. 5, it would begin analyzing more test scores for irregularities and increase training for test-center supervisors.

Gaston Caperton, president of the College Board and a former governor of West Virginia, said that in addition to bringing in the former F.B.I. chief, Louis J. Freeh, as a consultant, the College Board was also considering additional safeguards over the next year, including bolstering identification requirements for students taking the SAT and taking digital photographs to ensure they are who they say they are.

He announced the security measures during a State Senate hearing at Farmingdale State College here in which legislators and school officials repeatedly denounced the College Board and the Educational Testing Service, which administers the SAT test, over what they saw as glaring lapses in security for the high-stakes college-admissions exam.

Nassau County prosecutors filed criminal charges on Sept. 27 against Samuel Eshaghoff, 19, accusing him of being paid to take the SAT for six former and current students at Great Neck North High School. Prosecutors said they expected their inquiry to net more arrests involving at least two more public schools and a private school as early as next week.

"The procedures E.T.S. uses to give the test are grossly inadequate in terms of security," Bernard Kaplan, principal of Great Neck North, testified at the hearing. "Furthermore, E.T.S.'s response when the inevitable cheating occurs is grossly inadequate. Very simply, E.T.S. has made it very easy to cheat, very difficult to get caught."

While the new security measures represent a change of tone for College Board and Educational Testing Service officials who previously insisted their system was adequate, some superintendents and principals said they did not go far enough. These officials have

called for fingerprinting students, increasing stipends for proctors and imposing real consequences on those who cheat. Currently, if the testing service suspects cheating, the students' scores are canceled and they are permitted to retake the test — with no notification to either their high school or colleges where they apply.

"Actions speak louder than words, and E.T.S. needs to put some meat on the bones," said Geoffrey N. Gordon, superintendent of the Port Washington schools. "They need to partner with schools to make sure there is no cheating."

The Port Washington district, for instance, requires students to provide two forms of identification for entry to the test, instead of the one required by E.T.S.

Dr. Gordon recalled that a student from nearby Roslyn, who did not have a second form of identification, recently had to get his parents to verify his identity. The mother "chewed my head off," Dr. Gordon said, but was somewhat mollified after he explained the reason.

Kurt M. Landgraf, president and chief executive of Educational Testing Service, said at the hearing that his company already spent $25 million annually on security, about 10 percent of its overall budget for College Board programs. He said about 3,000 test scores — out of more than two million exams taken — were canceled each year, most after test-center supervisors reported irregularities or because of large jumps from a student's scores on previous tests.

Raymond Nicosia, the testing company's director of test security, said that impersonations were a small fraction of those cases, perhaps 150 a year — company officials previously said there were only a few — and that 750 people were generally turned away at test centers because of questionable identification.

"Once we have any inkling that there's anything improper, we go after them with every means available," Mr. Landgraf said.

But over more than a decade, testing officials said, about 10 cases — the ones in which money changed hands — have been referred to law enforcement nationwide.

"Sadly, the losers in this are the honest, hard-working students who play by the rules: they prepare for this like the Super Bowl," said Senator Kenneth P. LaValle, a Long Island Republican who is chairman of the Higher Education Committee in Albany. "This is something that will determine the course of their lives. And there are others, for whatever reason, who feel they can take a shortcut."

Mr. Kaplan said that since the arrests, he had sent the College Board a proposal for a pilot program in Great Neck that would require students to take the SAT in the district to limit chances of impersonation.

At a SAT exam at his high school last spring, fewer than half the test-takers were from the school, he said; the rest showed identification cards, but "any one of those could be completely made up or forged and we would have no way of knowing."

"It is ridiculously easy to take the test for someone else," Mr. Kaplan said. "That's why when E.T.S. says this kind of impersonation is a rare occurrence, you just have to laugh. How would they know? All they can say is they are unaware of a large number of impersonations. I'm sure, that's true. They are most assuredly unaware."

Testing officials said they would consider Mr. Kaplan's proposal, which also calls for increasing stipends for proctors — they are currently paid $75 for the day — and compensating the school for taking responsibility for the testing security.

Mr. Caperton pointed to the hiring of Mr. Freeh and his management company, which includes former law enforcement officials and security experts, as an indication of how seriously the College Board was taking the issue. (A College Board spokesman would not say how much it was paying him.) "We are deeply disturbed by the cases of test-taker impersonation that have recently been in the headlines and have occasioned this hearing," Mr. Caperton testified.

Mr. Landgraf said that while test security needed constant enhancement to meet new threats, he hoped that whatever measures are considered do "not unnecessarily burden test-takers or discourage any student or group of students from taking the SAT."

Winnie Hu reported from Farmingdale, and Jenny Anderson from New York.

Related Issues

Privacy, Biometrics
September 14, 2003

September 2003

Introduction

Among the many reactions to the September 11 tragedy has been a renewed attention to biometrics. The federal government has led the way with its new concern about border control. Other proposals include the use of biometrics with ID cards and in airports, e.g. video surveillance enhanced by facial-recognition technology.

The purpose of this document is to sketch out EFF's concerns about biometrics. In today's public arena, biometric technologies are being marketed as a "silver bullet" for terrorism; however, very little independent, objective scientific testing of biometrics has been done. Deploying biometric systems without sufficient attention to their dangers makes them likely to be used in a way dangerous to civil liberties. This document is very much a work in progress and we welcome comments.

What Are Biometrics?

Biometrics refers to the automatic identification or identity verification of living persons using their enduring physical or behavioral characteristics. Many body parts, personal characteristics and imaging methods have been suggested and used for biometric systems: fingers, hands, feet, faces, eyes, ears, teeth, veins, voices, signatures, typing styles, gaits and odors.

Our Major Concerns

- **Biometric technology is inherently individuating and interfaces easily to database technology, making privacy violations easier and more damaging.** If we are to deploy such systems, privacy must be designed into them from the beginning, as it is hard to retrofit complex systems for privacy.
- **Biometric systems are useless without a well-considered threat model.** Before deploying any such system on the national stage, we must have a realistic threat model, specifying the categories of people such systems are supposed to target, and the threat they pose in light of their abilities, resources, motivations and goals. Any such system will also need to map out clearly in advance how the system is to work, in both in its successes and in its failures.

- **Biometrics are no substitute for quality data about potential risks**. No matter how accurately a person is identified, identification alone reveals nothing about whether a person is a terrorist. Such information is completely external to any biometric ID system.
- **Biometric identification is only as good as the initial ID.** The quality of the initial "enrollment" or "registration" is crucial. Biometric systems are only as good as the initial identification, which in any foreseeable system will be based on exactly the document-based methods of identification upon which biometrics are supposed to be an improvement. A terrorist with a fake passport would be issued a US visa with his own biometric attached to the name on the phony passport. Unless the terrorist A) has already entered his biometrics into the database, and B) has garnered enough suspicion at the border to merit a full database search, biometrics won't stop him at the border.
- **Biometric identification is often overkill for the task at hand.** It is not necessary to identify a person (and to create a record of their presence at a certain place and time) if all you really want to know is whether they're entitled to do something or be somewhere. When in a bar, customers use IDs to prove they're old enough to drink, not to prove who they are, or to create a record of their presence.
- **Some biometric technologies are discriminatory.**A nontrivial percentage of the population cannot present suitable features to participate in certain biometric systems. Many people have fingers that simply do not "print well." Even if people with "bad prints" represent 1% of the population, this would mean massive inconvenience and suspicion for that minority. And scale matters. The INS, for example, handles about 1 billion distinct entries and exits every year. Even a seemingly low error rate of 0.1% means 1 million errors, each of which translates to INS resources lost following a false lead.
- **Biometric systems' accuracy is impossible to assess before deployment** Accuracy and error rates published by biometric technology vendors are not trustworthy, as biometric error rates are intrinsically manipulable. Biometric systems fail in two ways: false match (incorrectly matching a subject with someone else's reference sample) and false non-match (failing to match a subject with her own reference sample). There's a trade-off between these two types of error, and biometric systems may be "tuned" to favor one error type over another. When subjected to real-world testing in the proposed operating environment, biometric systems frequently fall short of the performance promised by vendors.
- **The cost of failure is high.** If you lose a credit card, you can cancel it and get a new one. If you lose a biometric, you've lost it for life. Any biometric system must be built to the highest levels of data security, including transmission that prevents

interception, storage that prevents theft, and system-wide architecture to prevent both intrusion and compromise by corrupt or deceitful agents within the organization.

Despite these concerns, political pressure for increasing use of biometrics appears to be informed and driven more by marketing from the biometrics industry than by scientists. Much federal attention is devoted to deploying biometrics for border security. This is an easy sell, because immigrants and foreigners are, politically speaking, easy targets. But once a system is created, new uses are usually found for it, and those uses will not likely stop at the border.

With biometric ID systems, as with national ID systems, we must be wary of getting the worst of both worlds: a system that enables greater social surveillance of the population in general, but does not provide increased protection against terrorists.

Some Current Biometric Initiatives

Sec. 403(c) of the **USA-PATRIOT Act** specifically requires the federal government to "develop and certify a technology standard that can be used to verify the identity of persons" applying for or seeking entry into the United States on a U.S. visa "for the purposes of conducting background checks, confirming identity, and ensuring that a person has not received a visa under a different name."

The recently enacted **Enhanced Border Security and Visa Entry Reform Act of 2002**, Sec. 303(b)(1), requires that only "machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers" shall be issued to aliens by October 26, 2004. The Immigration and Naturalization Service (INS) and the State Department currently are evaluating biometrics for use in U.S. border control pursuant to EBSVERA.

Even prior to September 11, however, large-scale civilian biometric identification systems were being pushed. Both the **Personal Responsibility and Work Opportunity Act of 1995** (PRWOA), a welfare reform law, and the **Immigration Control and Financial Responsibility Act of 1996** (ICFRA), an immigration reform law, called for the use of "technology" for identification purposes.

The PRWOA requires the states to implement an electronic benefits transfer program "using the most recent technology available . . . which may include personal identification numbers, photographic identification . . . and other measures to protect against fraud and abuse." This law covers, for example, the Food Stamps program.

The ICFRA requires the President to "develop and recommend . . . a plan for the establishment of a data system or alternative system . . . to verify eligibility for employment in the United States, and immigration status in the United States for purposes of eligibility for benefits under public assistance programs . . . or government benefits." This system "must be capable of reliably determining with respect to an individual whether . . . the individual is claiming the identity of another person."

The **Illegal Immigration Reform and Immigrant Responsibility Act of 1996** (IIRAIRA) requires the INS to include on alien border crossing cards "a biometric identifier (such as the fingerprint or handprint of the alien) that is machine readable." The State Department collects fingerprints and photographs of aliens for these cards.

The **Truck and Bus Safety and Regulatory Reform Act of 1988** (TBSRRA) requires "minimum uniform standards for the biometric identification of commercial drivers."

EFF's concerns about biometrics

Why be concerned about biometrics? Proponents argue that: A) biometrics themselves aren't dangerous because all the real dangers are associated with the database behind the biometric information, which is little different from problems of person-identifying information (PII) databases generally; B) biometrics actually promote privacy, e.g., by enabling more reliable identification and thus frustrating identity fraud.

But biometric systems have many components. Only by analyzing a system as a whole can one understand its costs and benefits. Moreover, we must understand the unspoken commitments any such system imposes.

Surveillance

The chronic, longitudinal capture of biometric data is useful for surveillance purposes. Our Surveillance Monitor page highlights some of these issues. Biometric systems entail repeat surveillance, requiring an initial capture and then later captures.

Another major issue relates to the "voluntariness" of capture. Some biometrics, like faces, voices, and fingerprints, are easily "grabbed." Other biometrics, at least under present technology, must be consciously "given." It is difficult, for instance, to capture a scan of a person's retina or to gather a hand geometry image without the subject's cooperation. Easily grabbed biometrics are a problem because people can't control when they're being put into the system or when they're being tracked. But even hard-to-grab biometrics involve a trust issue in the biometric capture device and the overall system architecture.

Databases

To be effective, a biometric system must compare captured biometric data to a biometric database. Our National ID System page highlights issues surrounding database abuse, which has both static and dynamic dimensions.

The static issues surrounding databases are mainly about safeguarding large and valuable collections of personally identifying information. If these databases are part of an important security system, then they (and the channels used to share PII) are natural targets for attack, theft, compromise, and malicious or fraudulent use.

The dynamic issues surrounding databases mainly concern the need to maintain reliable, up-to-date information. Databases that seek to maintain accurate residence information must be updated whenever one moves. Databases that are used to establish eligibility for benefits must be updated so as to exclude persons no longer eligible. The broader the function of the system, the more and broader the updating that is required, increasing the role of general social surveillance in the system.

It may seem that one of the issues that plagues token-based ID systems (like ID cards) -- the security or integrity of the token itself -- does not apply for biometric systems, because "you are your ID." But the question of the reliability of the token is really a question about trust. In an ID card system, the question is whether the system can trust the card. In biometric systems, the question is whether the individual can trust the system. If someone else captures your signature, fingerprint, or voice, for instance, what prevents it from being used by others? Any use of biometrics with a scanner run by someone else involves trusting someone's claim about what the scanner does and how the captured information will be used.

Vendors and scanner operators may say that they protect privacy in some way, perhaps by hashing the biometric data or designing the database to enforce a privacy policy. But the end user typically has no way to verify whether such technical protections are effective or implemented properly. End-users should be able to verify any such claims, and to leave the system completely if they are not satisfied. Exiting the system, of course, should at least include the expungement of the end-user's biometric data and records.

Linking

An oft-noted risk of biometric systems is the use of biometrics as a linking identifier. This risk, of course, depends to some extent on standardization. Consider, for instance, the use of the Social Security number as a linker across disparate databases. While the private sector would not have been able to develop anything like the SSN on its own, once the government created this identifier, it became a standard way of identifying individuals.

Standardization therefore creates new privacy risks because information gathered for one purpose can be used for completely unrelated, unconsented-to purposes.

Currently, Automated Fingerprint ID Systems (AFIS) are heavily used by the government in connection with law enforcement, but there is at present little standardization within the AFIS industry. If law enforcement and private industry were to unify their fingerprint databases under one common standard, such as under a national ID system, this would potentially put one's entire life history in interoperating databases that are only a fingerprint away.

Tracking

By far the most significant negative aspect of biometric ID systems is their potential to locate and track people physically. While many surveillance systems seek to locate and track, biometric systems present the greatest danger precisely because they promise extremely high accuracy. Whether a specific biometric system actually poses a risk of such tracking depends on how it is designed.

Why should we care about perfect tracking? EFF believes that perfect tracking is inimical to a free society. A society in which everyone's actions are tracked is not, in principle, free. It may be a livable society, but would not be our society.

EFF believes that perfect surveillance, even without any deliberate abuse, would have an extraordinary chilling effect on artistic and scientific inventiveness and on political expression. This concern underlies constitutional protection for anonymity, both as an aspect of First Amendment freedoms of speech and association, and as an aspect of Fourth Amendment privacy.

Implemented improperly, biometric systems could:

- increase the visibility of individual behavior. This makes it easier for measures to be taken against individuals by agents of the government, by corporations, and by our peers.
- result in politically damaging and personally embarrassing disclosures, blackmail and extortion. This hurts democracy, because it reduces the willingness of competent people to participate in public life.
- increase the 'circumstantial evidence' available for criminal prosecution. This might dramatically affect the existing balance of plausible-sounding evidence available to prosecutors, and hence increase the incidence of wrongful conviction. Many criminal cases are decided by plea bargaining, a process that is sensitive to the perceived

quality of evidence. Even ambiguous or spurious evidence generated by complex technical systems may be difficult for overburdened public defenders to challenge.

- enable the matching of people's behavior against pre-determined patterns. This could be used by the government to generate suspicion, or by the private sector to classify individuals into micro-markets, the better to manipulate consumer behavior.
- aid in repressing readily locatable and trackable individuals. While the public's concern is usually focused on the exercise of state power, these technologies may also greatly empower corporations. If proper privacy safeguards are not constructed into such systems, they would prove useful in dealing with such troublesome opponents as competitors, regulators, union organizers, whistleblowers, and lobbyists, as well as employees, consumer activists, customers and suppliers.

The Attributes of Biometric Systems

How Do Biometrics Compare to Other Types of ID?

Currently other than personally recognizing someone, or having a trusted third party personally swear to their identity, the only other technique for identifying a person is through the use of a "token." These tokens, which are in essence representations of the oath of a trusted third party, come in two basic forms:

- **Knowledge tokens**, such as passwords, secret PINs (Personal Identification Numbers), or knowledge of personal data (knowing one's mother's maiden name, e.g.), or
- **Physical tokens** such as ID cards, passports, chip cards, or plain old keys.

Token IDs offer certain advantages over biometric identification. Security against "false acceptance" of impostors can be raised by increasing the complexity of the token used for identification. Also, in the event of loss or compromise, the token, be it a password, PIN, key, or ID card, can be revoked, changed or reissued, a biometric measurement cannot.

The advantage of biometrics is that unlike tokens, biometrics cannot be lost, loaned, or forgotten. Token-based systems must verify that the presenter is the authorized user, not an unauthorized person who has come to possess the token.

Used carefully, biometrics may be combined with token-based systems to mitigate the vulnerability of ID tokens to unauthorized use.

Functions of Biometric Systems

One useful way of thinking about biometrics is that they are used for one of two purposes: A) To prove that you are who you say you are (positive ID), or B) To prove that you are not who you say you are not (negative ID).

In a positive ID situation, the subject asserts that she is Jane Doe and submits a "live" sample (a fingerprint, for example) to the system. The system then checks its database of previously enrolled or registered samples to see if the live sample matches the reference sample. A positive ID system is designed to prevent more than one person from using a single identity.

In a negative ID situation, John Roe claims *not* to be someone already known to the system. Here, the system checks its database to see that Roe is not on the watchlist of suspected criminals and terrorists, whose biometrics are already in the system. A negative ID system is designed to prevent one person from using more than one identity.

When biometrics are employed to effect negative identification, one need not be enrolled. The only persons who must be "in" the database are those whom the operator is trying to keep out or catch.

Biometrics alone cannot establish "true identity." A biometric system cannot prevent someone from furnishing fake credentials when they first enter the system. They can only prevent them from using another identity once enrolled.

Common Aspects of All Biometric Systems:

All biometric technology systems have certain aspects in common. All are dependent upon an accurate reference or "registration" sample. If a biometric system is to identify a person, it first must have this sample, positively linked to the subject, to compare against. Modern biometric identification systems, based on digital technology, analyze personal physical attributes at the time of registration and distill them into a series of numbers. Once this reference sample is in the system, future attempts to identify a person are based on a comparison of a "live" sample and the reference sample or samples.

A perfect system would recognize a person 100% of the time, and reject an impostor 100% of the time. However, biometric samples are gathered from people in environmental conditions that are uncontrollable, over equipment that may slowly be wearing out, and using technologies and methods that vary in their level of precision. Consequently, the accuracy

of biometric systems is assessed in light of these confounding variables via its tendency to experience either a "false match" (also called a "false accept") or a "false non-match" ("false reject"). The point at which these two rates intersect is called the equal error rate or crossover point.

Biometric systems may be "tuned" to diverge from the equal error rate to provide a match threshhold that satisfies the designer's requirements. If a system compares a large number of persons against a small number of samples, and the consequence of a false match is low, (for example, at a border crossing or airport that is looking for a short list of criminals) a system biased towards a higher "false accept" or "false match" rate may be desirable. The advantage to biasing a system in this manner is that it is likely to err on the side of safety, and less likely to let a criminal slip through undetected. The disadvantage is that the system will falsely associate innocent people with criminals. If other safeguards are in place and the system operators understand the system's bias towards false match, the result can be a relatively trivial loss of convenience due to increased scrutiny (extra inspection of luggage, questioning, etc.) Biasing such a system towards a high "false non-match" or "false reject" rate will result in fewer passengers slowed down at the gate, but at the cost of possibly losing the sought-after criminals.

When assessing the utility or the cost of a biometric system, it's important to bear the common features of all such systems in mind. How is the reference sample to be gathered and catalogued? How it the live sample going to be gathered? Can a live sample be captured without the subject's knowledge and cooperation? What are the implications of all four possible outcomes (true match, true non-match, false match, false non-match)? What is the value of a successful system, and what is the cost, to all parties, should it fail?

Further, we should not assess failure simply from the perspective of the core biometric technology itself. Even an ideal system can be defeated easily if it is incorporated into an insecure or poorly-designed overall system architecture. Any biometric system, especially one that involves a component of telecommunication, **must** be very carefully designed to prevent the loss or interception of user biometrics. Any

deployed system must incorporate safeguards to prevent the interception of biometric data while it is being communicated. If a user's biometric is intercepted, criminals may be able to replicate either the sample itself or the string of binary data produced by a successfully-matched sample. Armed with such intercepted biometric data, a criminal would be able to effect a potentially very damaging identity theft.

Types of Biometrics

A proper assessment is built not only on a general understanding of biometrics, but also on an understanding of specific technologies. An understanding of both biometrics in general and specific biometric technologies is a necessary condition for a solid understanding of the larger social implications of biometrics.

Signature

The biometric most familiar to us is the signature. Our ability to judge by sight if one signature matches another has made this a time-proven and legally-binding biometric. However, by sight alone, most of us cannot recognize the pressure of the pen on the paper or the speed and rhythms of its traverse of the page. Computers can do all these things, and quantify, analyze and compare each of these properties to make signature recognition a viable biometric technology. Being based on things that are not visible (pen pressure and velocity, for example), signature-based biometric technology, offers a distinct advantage over regular signature verification -- in addition to mimicking the letter forms, any potential forger has to fabricate a signature at the same speed, and with the same pen weight, as his victim.

Signature biometrics pose a couple of unique problems. The first is the comfort with which people are already willing to use their signature as a form of identification. While this high level of consumer acceptance is viewed as a strength by vendors of such systems, this bears with it a strong downside. Without proper notification, a person may sign an electronic signature pad and unwittingly also be surrendering a reference or live biometric sample. Since the custom of leaving a signature as one's "official mark" is based on the presumption of irreproducibility (i.e., that a forger would be hard-pressed to imitate a signature just by looking at

it), people are willing to provide a signature without giving its potential for reproduction a second thought. However, electronic data is easy to copy and transmit. And so, a forger posing as a delivery man might fraudulently secure a signature biometric by presenting a victim with a "gift" box, requesting a signature to confirm delivery, and making off with the victim's biometric data.

The second unique property of signature biometrics is that unlike all other biometrics, which either establish an identity (identification) or confirm an identity (authentication), a signature can convey *intent* (authorization). In other words, a traditional signature on paper is taken both to authenticate the signator, and to convey the signator's legal authority. An electronic system that solicits a user's non-signature biometric must provide a separate step to convey the user's legal authorization for any binding transaction. A signature-based biometric system could mimic our current legally customary acceptance of a signature to simultaneously convey both identity and authority.

Keystroke Dynamics

The rhythms with which one types at a keyboard are sufficiently distinctive to form the basis of the biometric technology known as keystroke dynamics. While distinct, keystroke dynamics are not sufficiently unique to provide identification, but can be used to confirm a user's identity.

Keystroke dynamics, unlike other biometric technologies, is 100% software-based, requiring no sensor more sophisticated than a home computer. Because of this, deployment is occurring in fairly low-stakes, computer-centric applications, such as content filtering (Net Nanny owns BioPassword, the leading keystroke dynamics vendor) and digital rights management, in which passwords to download music are bolstered with by keystroke dynamic verification, to prevent password-sharing. As a general rule, any method involving home or office computers is inherently insecure, as these devices leave a lot more room for experimentation than devices like ATMs or entry systems, and the information they use tends to travel over unsecured communication lines.

Hand Geometry

Perhaps the most ubiquitous electronic biometric systems are hand geometry based. Hand-geometry-based systems require the subject to place his or her hand (usually the right hand) on a plate where it is photographically captured and measured. Made of 27 bones and a complex web of interconnected joints, muscles, and tendons, the human hand presents a sufficiently peculiar conformation of anatomical features to enable authentication, but is not considered sufficiently unique to provide full identification. Further, the geometry of the hand is variable over time, as hand shape may be altered due to injury, disease, aging, or dramatic weight swings. A simple hand-geometry system will measure length and thickness of digits, width of the palm at various points, and the radius of the palm. This results in a relatively simple identification that can be expressed in a very simple, compact string of data. Efforts have been made to improve the accuracy of hand geometry, including three-dimensional sampling (i.e., a second camera measuring the thickness of the hand from the side), and a patented system (owned by the British concern, Neusciences) that measures the pattern of the veins of the hand. Neusciences claims that their system provides a high degree of accuracy and that the hand vein feature is unique and relatively invariable, changing little over a person's lifespan.

In deployment, traditional hand geometry systems have found acceptance in applications requiring verification of an identity, rather than a full proof or establishment of an identity. Airports, prisons, and factories have successfully employed hand-geometry-based systems to restrict access to runways, to prevent walk-out escapes during visits, and to ensure that time cards are being punched only by the worker, and not by that worker's pal on his or her behalf. In all these instances, the subject is attempting to prove or disprove his or her membership in a relatively small group of people (authorized runway personnel, prisoners/visiting family, factory workers). When stakes are high, these systems are not relied on exclusively to confirm identity; rather, they are used to provide an additional layer of security above and beyond that provided by existing security systems.

Since they must accommodate the largest of hands, any hand geometry or hand vein system must be somewhat bulky, and requires the user to

perform an obtrusive task (placing his or her hand on the platen for sampling). Because of this obtrusiveness, hand-based biometrics represent less of a privacy threat than some other systems: subjects cannot have their biometric features sampled without their knowledge, and the sampling method is unambiguous in its intent.

Fingerprint

Fingerprinting is a highly familiar and well-established biometric science. The traditional use of fingerprinting, of course, has been as a forensic criminological technique, used to identify perpetrators by the fingerprints they leave behind them at crime scenes. Scientists compare a latent sample left at a crime scene against a known sample taken from a suspect. This comparison uses the unique features of any given fingerprint, including its overall shape, and the pattern of ridges, valleys, and their bifurcations and terminations, to establish the identity of the perpetrator.

In the context of modern biometrics, these features, called fingerprint minutiae, can be captured, analyzed, and compared electronically, with correlations drawn between a live sample and a reference sample, as with other biometric technologies. Fingerprints offer tremendous invariability, changing only in size with age, are highly resistant to modification or injury, and very difficult to "forge" in any useful way. Although the development of some sort of surreptitious sensor is not inconceivable, the reality is that sensors remain obtrusive, requiring a willful finger pressure to gather a useful sample. Unlike other systems, based on cameras and high-tech sensors, fingerprint sampling units are compact, rugged, and inexpensive, with commercially available systems from multiple vendors offering very good accuracy. Next-generation scanners can analyze below the surface of the skin, and can add pore pattern recognition in addition to the more obvious minutia of the fingerprint.

Facial Recognition

Facial recognition sprung into the national spotlight during the 2001 Super Bowl, when Tampa police scanned the faces of game fans without their knowledge for the purpose of spotting terrorists in the crowd. While this proved a public relations nightmare in January 2001,

the use of this technology in New Orleans at the post-9/11 Super Bowl of 2002 generated little controversy. Facial recognition remains one of the more controversial biometric technologies because of its very *un*obtrusiveness. With good cameras and good lighting, a facial recognition system can sample faces from tremendous distances without the subject's knowledge or consent.

Most facial recognition technology works by one of two methods: facial geometry or eigenface comparison. Facial geometry analysis works by taking a known reference point (for example, the distance from eye to eye), and measuring the various features of the face in their distance and angles from this reference point. Eigenface comparison uses a palette of about 150 facial abstractions, and compares the captured face with these archetypal abstract faces. In laboratory settings, facial recognition results are excellent, but critics have questioned the effectiveness of the technology in real-world circumstances. Nevertheless, the accuracy of facial recognition has been good enough for casinos to have put the the technology to use since the late 1990s as a means to spot banned players. Facial recognition technology proponents claim good performance even against disguises, weight changes, aging, or changes in hairstyle or facial hair.

Eye biometrics: Iris/Retina

The human eye offers two features with excellent properties for identification. Both the iris (the colored part visible at the front of the eye) and the veins of the retina (the thin film of nerve endings inside the eyeball that capture light and send it back to your brain) provide patterns that can uniquely identify an individual. Retinal scanning is the older technology, and requires the subject to look into a reticle and focus on a visible target while the scan is completed. It's definitely one of the more intrusive biometric technologies, with some subjects reporting discomfort at the scanning method. Iris recognition has an advantage in ease of use, in that it merely requires the subject to look at a camera from a distance of three to ten inches. The iris scanner illuminates the iris with invisible infra-red light, which shows details on darker-colored eyes that are not visible to the naked eye. The pattern of lines and colors on the eye are, as with other biometrics, analyzed, digitized, and compared against a reference sample for verification.

Iridian Technologies, who hold the patents on iris recognition, claim that the iris is the most accurate and invariable of biometrics, and that their system is the most accurate form of biometric technology. Iridian's system also has the benefit of extremely swift comparisons. The compay claims that it can match an iris against a database of 100,000 reference samples in 2-3 seconds, whereas a fingerprint search against a comparable database might take 15 minutes.

Voice Verification

None of us finds it remarkable when a friend recognizes our voice on the telephone. However, what we find easy to do is still a very hard problem for computers, especially when their job is to identify someone positively. The prospect of accurate voice verification offers one great advantage, which is that it would allow a remote identification using the phone system, an infrastructure that's already been built and thus has zero client-side cost: no special reader needs to be installed in your home. Even without the phone system, the sampling apparatus, a microphone, remains far cheaper than competing, largely optically-based biometric technologies.

But voice recognition technology is still not good enough to be used as a front-line biometric technology. Simply put, voice verification systems have to account for a lot more variables than do other systems, starting with the inevitable compression of a voice captured by cheap microphones (especially those found on phone handsets), discriminating a voice from background noise and other sonic artifacts, and the human voice's tremendous variability, due to colds, aging, and simple tiredness. Also, just as a voice can be surreptitiously recorded over the telephone or face-to-face, a person's voice can be captured surreptitiously by a third party (either by tapping or bugging) and replayed, or a person's voice might be biometrically sampled remotely without consent during a fake door-to-door or telephone sales call. Because of these difficulties, commercial deployments of voice verification have been limited to "backup" status, systems in which there are other token-based methods of identification, with voice verification providing an added layer of protection.

Characterizing Different Biometrics

Different biometric features have characteristics that make them more or less useful for particular applications. Dr. James Wayman, director of the National Biometric Test Center at San Jose State University, categorizes biometric features in terms of five qualities:

- **Robustness**: repeatable, not subject to large changes.
- **Distinctiveness**: there are wide differences in the pattern among the population.
- **Accessibility**: easily presented to an imaging sensor.
- **Acceptability**: perceived as non-intrusive by the user.
- **Availability**: a user may present a number of independent measurable features.

Dr. Wayman explains these qualities by comparing fingerprinting to hand geometry.

"Fingerprints are extremely distinctive, but not very robust, sitting at the very end of the major appendages you use to explore the world. Damaging your fingerprints requires less than a minute of exposure to household cleaning chemicals. Many people have chronically dry skin and cannot present clear prints. Hands are very robust, but not very distinctive. To change your hand geometry, you'd have to hit your hand very hard with a hammer. However, many people (somewhat less than 1 in 100) have hands much like yours, so hand geometry is not very distinctive. Hands are easily presented without much training required, but most people initially misjudge the location of their fingerprints, assuming them to be on the tips of the fingers. Both methods require some "real-time" feedback to the user regarding proper presentation. Both fingerprints and the hand are accessible, being easily presented. In the 1990 Orkand study*, only 8% of customers at Department of Motor Vehicle offices who had just used a biometric device agreed that electronic fingerprinting "invades your privacy." Summarizing the results of a lengthy survey, the study rated the public acceptance of electronic fingerprinting at 96%. To our knowledge, there is no comparable polling of users regarding hand geometry, but we hypothesize that the figures would not be too different. With regard to availability, our studies have shown that a person can present at least 6 nearly-independent fingerprints, but only one hand geometry (your left hand may be a near mirror image of your right)."

*Orkand Corporation, "Personal Identifier Project: Final Report", April 1990, State of California Department of Motor Vehicles report DMV88-89, reprinted by the U.S. National Biometric Test Center.

Characterizing Biometric Applications

Dr. Wayman suggests characterizing biometric applications in terms of seven variables:

- **Cooperative vs. Non-Cooperative** This refers to the behavior of the "threat" or would-be deceptive user. Is the "threat" trying to cooperate with the system? If the threat is trying to enter a restricted area, she either cooperates with the positive ID system to try to fool it into thinking she's allowed in, or deceptively tries not to cooperate with a negative ID system so as not to trigger the alarm. One implication of this variable is the scope of database search. In cooperative applications, users may first identify themselves with a card or PIN, so that the system need only match against the claimed identity's template. In non-cooperative applications, users can't be trusted to identify themselves correctly, so the entire database may need to be searched.
- **Overt vs. Covert** Is the user aware that the biometric sampling and identification is occurring?
- **Habituated vs. Non-Habituated** Is the intended user expected to be experienced in the use of the system?
- **Attended vs. Non-Attended** Will the intended user be supervised when using the system?
- **Standard vs. Non-Standard Environment** How controlled are the environmental conditions for operation?
- **Public vs. Private** Will users be customers (public) or employees (private)?
- **Open vs. Closed** Will the application be required to exchange biometric data with other systems or not?

Dr. Wayman explains that the positive biometric identification (hand geometry) of users of the Immigration and Naturalization Service's Passenger Accelerated Service System (INSPASS) for rapidly admitting frequent travelers into the United States:

"can be classified as a cooperative, overt, non-attended, non-habituated, standard environment, public, closed application. The system is *cooperative* because those wishing to defeat the system will attempt to be identified as someone already holding a pass. It will be *overt* because all will be aware that they are required to give a biometric measure as a condition of enrollment into this system. It will be *non-attended* and in a *standard environment* because collection of the biometric will occur near the passport inspection counter inside the airports, but not under the direct observation of an INS employee. It will be *non-habituated* because most international travelers use the system less than once per month. The system is *public* because enrollment is open to any frequent traveler into the United States. It is *closed* because INSPASS does not exchange biometric information with any other system." *(emphases added)*

Characterizing Biometric ID Systems

Dr. Wayman suggests that biometric ID systems should be viewed in terms of a generic biometric system made up of five basic components or subsystems, depending on the application: data collection, transmission, signal processing (which comprises feature extraction, quality control, pattern matching), storage, and decision.

- **Data collection** Biometric systems involve at least two discrete data collection steps. First, any biometric system must contain a biometric characteristic deemed "true" or canonical from the system's viewpoint. The term "enrollment" or "registration" refers to the first entry of biometric data into the database. Second, the system must compare a later-submitted "sample" (often called a "live sample") to the sample in the database. (Scale is crucial to the enrollment step, sometimes for quite mundane reasons. In the context of biometric visa issuance by the State Department, for instance, the government has been looking at whether or not U.S. consulates around the world have room to handle the additional equipment and physical traffic needed for data collection.)
- **Transmission** Many biometric systems collect data at one location but store and/or process it at another. Such systems require data transmission.
- **Signal processing**Once a biometric is acquired, it must be prepared for comparison. There are three basic tasks here: feature extraction, quality control, and pattern matching. A fourth task in large-scale systems is pattern classification.
    - *Feature extraction* involves finding the true biometric pattern amid noise and signal degradation, preserving the critical information, and discarding redundant or unnecessary data. Dr. Wayman gives the example of a text-independent speaker-recognition system. A properly implemented system isolates "features that depend only on the speaker and not on the words being spoken." At the same time, the system focuses on features that do not change "even if the speaker has a cold or is not speaking directly into the microphone."
    - *Quality control* involves checking to see if the signal is of good quality. Ideally, it should be possible to make a quick determination so that another measure can be taken if the signal is inadequate.
    - *Pattern matching* involves comparing the live sample to the reference sample in the database. If the user claims to be Jane Doe, the pattern-matching process may only need to compare the sample to Jane Doe's stored template. In other situations, the sample must be compared to multiple templates. The pattern-matching process generates a quantitative "distance" measure of the

comparison -- how close are they? Even for the same person, the distance is rarely if ever zero.

- *Pattern classification* is a technique aimed at reducing the computational overhead of pattern matching. In large-scale systems, it can be computationally taxing to match each sample against all stored templates in the database. If biometric patterns can be categorized, then it may be possible to perform the match against only the stored templates in that category. This is sometimes referred to as "binning." A different technique with the same goal is "filtering," which involves partitioning the database based on information not contained in the biometric itself. If you know the person is a man, you don't need to check against women's biometrics. Both of these techniques introduce additional error possibilities; if binning or filtering is erroneous, then the true template is not used and a false non-match results.

- **Decision** This subsystem implements the biometric ID system's actual policy with regard to matching. In general, lowering the number of false non-matches raises the number of false matches, and vice versa. The signal processing subsystem yields a quantitative "distance" measure, but "how close or far is enough?" is a matter of policy. In a high-security application where the cost of a false acceptance could be high, system policy might prefer very few false acceptances and many more false rejections. In a commercial setting where the cost of a false acceptance could be small and treated as a cost of doing business, system policy might favor false acceptances in order not to falsely reject and thereby inconvenience large numbers of legitimate customers. The inevitable existence of these errors means that any biometric ID system must also have well-designed policies for exception handling.

- **Storage**Biometric reference samples must be stored somewhere for matching purposes. For systems only performing "one-to-one" matching, the database may be distributed on cards carried by each enrolled user. The user simply presents his or her biometric and the system checks to see if it matches the template stored on the card. Depending upon system policy, no central database need exist, although in this application a centralized database can be used to detect counterfeit cards or to reissue lost cards without re-collecting the biometric pattern.

  In other cases, centralized storage is necessary because the system must match the live sample to multiple templates. As the number of templates grows, speed becomes an increasingly significant issue. One technique is to partition the database (i.e., binning or filtering) so that any sample need only be matched to the templates in one partition. This increases system speed and decreases false

matches at the expense of increasing the false non-match rate owing to partitioning errors. System error rates thus change with increasing database size and ID systems do not linearly scale.

Full biometric patterns cannot be reconstructed from the stored reference samples if these are stored as templates, which reduce data richness dramatically. Templates themselves are often created using the system vendor's proprietary feature extraction algorithms. Whether stored templates themselves can be used to "spoof" the system internally is entirely dependent on the security of the system architecture.

Biometric ID systems may store not only the templates but also raw data. One reason to do so would be to allow changes to the system or to change system vendors without having to re-collect data from all enrolled users. Full raw data storage is a riskier practice in that new templates may be extracted from the data or the raw data itself may be used against the system.

The State of Scientific Testing of Biometric ID Systems

According to Dr. Wayman,

"Testing of biometric devices requires repeat visits with multiple human subjects. Further, the generally low error rates mean that many human subjects are required for statistical confidence. Consequently, biometric testing is extremely expensive, generally affordable only by government agencies. Few biometric technologies have undergone rigorous, developer/vendor-independent testing to establish robustness, distinctiveness, accessibility, acceptability and availability in 'real-world' (non-laboratory) applications."

An in-depth discussion of the statistical methodology in testing biometric ID systems is beyond the scope of this discussion. We recommend Dr. Wayman's website to interested persons. Note, however, that it is very difficult to generalize from test results. At this time, scientists have no way of accurately estimating how large a test is needed to adequately characterize any biometric device in any application, even with advance knowledge of theoretical error rates.

Media Coverage/Resources

Check out this page for helpful resources including
lots of media coverage and links related to the topic.

Acknowledgements:

This document was written and compiled by William Abernathy and Lee Tien with editorial assistance from Sarah Granger and technical assistance from Johnson Hor.

https://www.eff.org/wp/biometrics-whos-watching-you

March 29, 2005
TechKnowledge no. 97

techknowledge

When Data Security Regulations Fail, There Is an Alternative

by Jim Harper

Jim Harper (jharper@cato.org) is the director of Information Policy Studies at the Cato Institute in Washington, D.C. (www.cato.org/tech). To subscribe, or see a list of all previous TechKnowledge articles, visit www.cato.org/tech/tk-index.html.

Published on March 29, 2005

If you hadn't heard of ChoicePoint before, you have now. ChoicePoint is a data aggregator-a company that collects information about people, reselling it in different combinations to a variety of clients. Most of the time, data aggregation is a beneficial process. It adds brains to the economy, helping designers, makers, marketers, and sellers of goods and services do a better job for consumers. Data aggregation helps employers, insurers, and lenders make smarter decisions faster.

For good or bad, ChoicePoint has cured the data aggregation industry's obscurity problem. Headline after headline has discussed the fallout since ChoicePoint revealed that it was duped into selling sensitive information about 145,000 people to fraudsters last year. The scammers set up a series of fake businesses to appear like legitimate buyers of financial information. Their purpose was to use it in later identity frauds.

In the wake of the ChoicePoint affair came a deluge of other disclosures. Hoping to obscure their errors in the onrushing press whirl, or having quickly learned the importance of disclosure, a series of companies and institutions revealed similar breaches. Among them were payroll company PayMaxx, Bank of America, LexisNexis' Seisint, several universities, and a shoe retailer called DSW.

It would be wrong to say that the consumer data industry had been without controversy. Its well-known members, the credit bureaus, have been besieged for years by complaints about inaccuracy and unfairness. This despite the Fair Credit Reporting Act, a federal regulatory scheme imposed 30 years ago to address inaccuracy and unfairness in credit reporting. The FCRA was amended in 2003 to address inaccuracy and unfairness in credit reporting. Again.

To the extent they are known, the other data aggregators are poorly understood and mistrusted. They have no consumer face-not even the limited exposure of the credit bureaus. Little is known about what data they collect and how they get it, or to whom they sell it. Several of them, unfortunately, have engaged with the federal government, hoping to provide data mining and surveillance services.

Cued by the new press attention to data security, senators and representatives have stepped in front of earnestly scribbling reporters announcing their plans to make us safe. A variety of bills in the House and Senate would mandate "fair" information practices, require notice of breaches, and force data aggregators to provide consumers with access to personally identifiable information, plus the right to correct it. Many of these are long-dead proposals that have nothing to do with data security. Indeed, some would undermine it even further. But no matter. The American public and media are ready to be buffaloed.

The companies that allowed these data breaches are blameworthy, to be sure. Bank of America moved tapes with financial data about millions of account holders by ordinary air transport. It is surmised that the tapes were lost or that baggage handlers simply stole them.

Of carelessness like this, Sen. Patrick Leahy (D-VT) said, "I don't know what these people are thinking." It's a good rhetorical point. But it may have an equally good answer.

You see, one thing Bank of America may have been thinking about is the federal government's "Safeguards Rule." This is a data security regulation that was mandated by Congress in the 1999 Financial Services Modernization Act, also known as Gramm-Leach-Bliley. Intended to ensure the security of financial data about consumers, the regulation requires financial institutions to:

- designate one or more employees to coordinate data safeguards;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the safeguards for controlling those risks;
- design and implement a safeguards program, and regularly monitor and test it;
- select appropriate service providers and contract with them to implement safeguards; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring safeguards.

Maybe Bank of America was too focused on this federally mandated security paperwork to focus on *actual data security*. In any event, federal data security regulation did not work.

Regardless, politicians' calls for "stronger" regulation are predictable because "stronger" regulation is "better"-in a press conference. In the real world, however, regulation is no more capable of divining threats to data security than, say, a common law liability regime, or even businesses' natural interest in maintaining their operations, integrity, image, brand, and assets.

As noted, data aggregation gives our economy brains. The new regulations being proposed would put a thumb on the carotid artery of information-based businesses, making them a little woozier, a little less aware, and a little less able to serve and protect consumers.

What matters with breaches such as ChoicePoint, Bank of America, and all the rest is whether anyone was harmed. Was a data-rich computer stolen and used for target practice on a backyard shooting range or was its trove of information used in hundreds or thousands of frauds?

Rather than hurried, one-size-fits-all federal regulation, imagine a rule where negligent holders of sensitive data suffer liability for damage caused by breaches. Imagine they have to pay injured parties for the consequences. Ten thousand breaches causing $1000 damage would cost a negligent data holder $10 million, along with adverse publicity and all the rest. Under such a rule, breached companies would race to shore up the damage because further damage would create further liability.

Attractive proposals like mandatory breach notifications might be useful sometimes. Just as often, notification would be a sideshow with no role in preventing consumer harm. Occasionally, notification would tip off computer thieves to the fact that they have also stolen data they could use in identity fraud. This stiff, one-note reaction pales in comparison to the multi-faceted response that would be gotten from putting the responsible party in the financial shoes of victims. Special damages-"civil penalties" and the like-are not appropriate: The objective is proportional response, and such things would detract from that.

Data security regulation is a proven failure. There is an alternative to more of the same. But how do we create this intriguing negligence rule? What has to be done?

Nothing. Just watch and wait. The rule has already been adopted by common law courts in New Hampshire and Michigan.

Human Bar Code

by Clyde Wayne Crews Jr.

November 1, 2002

Clyde Wayne Crews Jr. is director of technology studies at the Cato Institute.

http://www.cato.org/research/articles/crews-021104.html

Stock Photo Biometric technologies - such as voice prints, retina, iris and face scanners, digitized fingerprints, even implantable chips - can benefit us. Look for the technologies in cell phones, mobile computers, cars doors, doorknobs and office keys-basically everywhere. They'll bolster online commerce, help locate a lost youngster, and transmit medical information to doctors. They promise increased privacy by preventing identity theft.

But no one wants to be treated like human bar code by the authorities.

What are the benefits and concerns surrounding the further deployment of biometric identification techniques into our lives? While they promise new levels of physical security and secure commerce, they can also threaten fundamental values of privacy and liberty. We need a framework by which to judge biometric deployment, to make distinctions appropriate and inappropriate uses. The management of databases that underlie biometric applications can impact anonymity, privacy, and even authentication technology itself.

The most pressing threat to liberty is a government-mandated database containing all of us, corresponding to a National ID with biometric identifiers. This is the Big Brother scenario that would lead to the asking for ID everywhere, and devolve into a general law enforcement tool having nothing to do with the terrorism that prompted recent calls for National IDs. National IDs threaten liberty and anonymity, and, ironically, they undermine security itself by moving the locus of technological advancement in authentication technologies out of the private sector and into government.

A less sweeping biometric database is a partial one containing criminals and suspects - but not the general population. An example would be government-run face recognition cameras deployed in public places that have garnered so much attention lately. Individuals are observed, but presumably only to see if they match a face already in the underlying database. Allegedly, the information collection - that pertaining to the criminals - has already taken place under appropriate Fourth Amendment procedures, and no data is ever collected on individuals not already in the database. Nevertheless, many properly doubt governments can be trusted to discard incidental data collected on innocents. Applications of biometrics to identify and track individuals, even in "public" places, can constitute an unreasonable search and easily be abused. Stringent safeguards are required, but they do not yet exist. This will be the locus of much of the "privacy" debate in the coming years.

Finally, private, limited applications of biometrics are less worrisome. These might constitute databases of "members," as contrasted with governmental "bad guy" databases. Such tailored solutions exist where security clearances are needed, like factories and laboratories, and can offer the opportunity for extraordinary security by preventing others from posing as us. These proclaim, in effect, "You may enter my privately owned building, airplane, parking garage, neighborhood, house, etc., but only if I know who you are."

These offerings hold the most promise in the field of biometrics. However, these applications must not be allowed access to individual data gleaned by government coercion. If that happens, they will turn society against the technology and make it impossible to defend the industry from regulation. Let's keep it self-regulated.

Biometrics offers tremendous promise, but also risk. To safeguard civil liberties, there are basically three requirements. In a nutshell: (1) avoid mandatory databases or any form of National ID; (2) Ensure Fourth Amendment protections even for public surveillance, and; (3) avoid the mixing of public and private databases as new biometrics technologies emerge and proliferate: Instead of granting the private sector the use of government-mandated information, private industry must generate its own information, for purposes limited by the market's twin engines of consumer choice - and consumer rejection. Privacy, liberty, and even authentication technology will be all the better for it.

This article originally appeared on *Tech Central Station* on November 4, 2002.

AICPA PROMETRIC NASBA
National Association of State Boards of Accountancy

July 7, 2011

Mr. Mead Treadwell
Lieutenant Governor
State of Alaska
P. O. Box 110015
Juneau, AK 99811

Mr. Mead Treadwell
Lieutenant Governor
State of Alaska
550 West 7th Avenue
Anchorage, AK 99501

Dear Lt. Governor Treadwell:

Thank you for your recent letter requesting that Mr. Jason Giamo be excused from the fingerprinting process with regard to the Uniform CPA Examination. We have been asked by our respective organizations to respond on behalf of the National Association of State Boards of Accountancy (NASBA), Prometric (a subsidiary of ETS), and the American Institute of Certified Public Accountants (AICPA). For reasons that are explained in this letter, we respectfully must decline to grant Mr. Giamo an exception from the requirement to provide fingerprint data in order to take the Uniform CPA Examination.

Pursuant to laws of each state, the Uniform CPA Examination (Exam) is required for obtaining a CPA license from the State Boards of Accountancy in all U.S. jurisdictions. In Alaska, Statute Sec. 08.04.130 mandates use of the Exam. Under the direction of a Board of Examiners, comprised of a majority of past and current state regulators, the Exam is developed and scored by the AICPA. NASBA, which is a nonprofit organization composed of all state agencies that license CPAs, issues authorizations for candidates to test in accordance with state board requirements and maintains the confidential database of all Exam candidates. In order to maintain fair testing conditions and protect the public interest, the Exam is administered securely in professional test centers operated by Prometric. Questions used on the Exam are held securely by the AICPA, and all Exam candidates commit to maintain the confidentiality of the Exam content. The obligations of Exam security are statutory as well as contractual, because the primary purpose of CPA licensing is public protection.

Threats to Exam security do exist and NABSA, AICPA, and Prometric have procedures to protect the integrity of the Exam. A high degree of Exam security is not only a contract requirement among NASBA, AICPA and Prometric, and a contract requirement between NASBA and state boards, but it is also a statutory priority. For example, Alaska's Accountancy Act has three direct references to Exam security. Thus, when new tools are developed, that can improve security and, therefore, the protection of the public interest, it makes sense to employ them. The Biometric Identification Management System (BIMS) represents one such improvement.

NASBA, AICPA and Prometric introduced the BIMS in the CPA Exam beginning January 1, 2008, after lengthy consultations with NASBA's member boards and committees. Information about BIMS was widely available well in advance of the start date and was implemented only after due discussions with, and notice to, stakeholders. State boards, state CPA societies, review course providers and 38,000 Exam candidates were notified in 2007 that biometric fingerprinting would be incorporated into the Exam registration process. The biometrics requirement is explained in the Candidate Bulletin which is available to all current and prospective candidates. In the three and a half years since we instituted the BIMS, nearly one million Exam sections have been administered. Only one person, Mr. Giamo, has declined to have his fingerprints taken.

BIMS benefits the examination process and examination-takers in several ways. For example, once a candidate has provided fingerprints the first time he or she enters a Prometric test center, BIMS will verify the candidate's identity each time that individual returns to the test center after a break or to take another Exam section. It is an efficient process and reduces waiting time for candidates. It also protects the candidate's privacy by enabling the individual

to move around the test center without having to carry and present identification documents, and it prevents fraud by detecting test-taking attempts by individuals impersonating other candidates (proxy testing).

BIMS represents a solution that balances candidate privacy, examination security and efficiency of candidate check-in. Biometrics electronically and accurately captures test-taker information from government-issued photo ID documents, and recognizes if a test-taker has enrolled and tested with Prometric previously. It also protects the value of the credentialing program, protects intellectual property, and deters proxy testing and cheating. In addition, it provides an enhanced method of identity verification and ID validation, ensures that the fingerprint data has not been previously presented under a different name (specifically for return test-takers), increases test-takers' perception of security, and improves the overall testing experience. Because BIMS keeps the test-takers' data secure, and because there are stringent security barriers, BIMS builds respect for credentials among peers and in the marketplace.

Fingerprinting is already required by law for numerous other professional licenses throughout the states. Indeed, in Alaska fingerprints are required for other occupations such as mortgage lending, collection agencies, private conservators, nurses, and insurance agents. Other means of candidate identification - such as the use of a passport - have been considered, but thus far deemed to be inadequate because a passport is not a legally "secure document." Government officials and numerous experts have noted that passport identity requirements can be easily circumvented. Indeed, there have been several cases in which applicants have found the vital statistics of a deceased child from a tombstone or obituary and applied for a duplicate birth certificate.

It is also worth noting that this issue was considered by the Alaska Board of Accountancy at its August 28-29, 2008 meeting. After discussion, the Board unanimously adopted the following resolution: "RESOLVED that the Alaska Board of Public Accountancy support NASBA, the AICPA and Prometric's security policies for the Uniform CPA Examination CBT." Further, we note that a bill was introduced in the last session of the Alaska Senate (SB 98) that would have limited the use of biometrics for examination purposes. We enclose, for your consideration, a letter that Prometric sent to the Chair of the Judiciary Committee that discusses the use of biometrics as a test security measure. SB98 did not pass out of committee.

We very much appreciate your interest in this matter; however, BIMS is central to ensuring the integrity of the examination process. We hope the information we have provided in this letter convinces you that our decision to decline Mr. Giamo's request is sound.

Sincerely,

Ken L. Bishop
Executive Vice President & COO,
National Association of State Boards of Accountancy
(NASBA)

Mark Muth
Vice President, Market Segments
Prometric

Craig Mills, Ed.D.
Vice President, Examinations and Continuing
Professional Education
AICPA

Enclosure

Acceptable SAT Photo Identification

Acceptable photo identification (government- or school-issued) in English is required for admission to the SAT test center and will also be checked during the test. Identification must be current, include a recognizable photo, bear your name and match the name shown on your SAT Admission Ticket. Unacceptable identification may result in your not being admitted to the test center or score cancellation.

Examples of acceptable IDs are:

- Driver's license
- Government-issued ID
- School identification card
- Valid passport
- Student ID form:

Your school can prepare an ID form. This form must include a recognizable photo, and the school seal must overlap the photo. Sign the ID form in the presence of your counselor or principal. You will be asked to sign the ID form again at the test center. This form is valid only in United States.

Testimony of Jim Harper
Director of Information Policy Studies
The Cato Institute
to the Health and Social Services Committee
Alaska House of Representatives
on S.B. 98, Biometric Information for ID

Executive Summary

Biometrics include a wide variety of practices and technologies. Machine-readable biometrics using digital technology are more powerful and arguably offer more security benefits, but they also have significant privacy costs. Society has yet to reconcile the costs and benefits of machine-biometrics.

The intentions animating S.B. 98 are noble, but it is not the proper role of government and it is too early to enshrine practices around biometrics into law. Many provisions in S.B. 98 would create complexity without producing consumer benefits, would fail to foster privacy as intended, and would deprive Alaskans of freedom.

A number of "lighter-touch" steps that the Alaska legislature can take would help assure privacy protection when Alaskans encounter biometrics and prevent them coming to information-age harms. The state itself should ensure that its law protects against government wrongly accessing private data, and Alaska should continue to resist the federal government's national ID programs.

Chairman Keller, Vice Chairman Dick and members of the committee:

Thank you for the opportunity to testify before you today. I am keenly interested in the subject matter of your hearing, and I hope that my testimony will shed some light on your deliberations.

My name is Jim Harper, and I am director of information policy studies at the Cato Institute in Washington, D.C. The Cato Institute is a non-profit research foundation dedicated to preserving the traditional American principles of limited government, individual liberty, free markets, and peace. In my role there, I study the unique problems in adapting law and policy to the information age, problems like privacy and security.

I was a member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee at its founding and until recently. The DHS Privacy Committee advises the DHS Privacy Office and the Secretary of Homeland Security on privacy and related issues.

In 2006, I published a book entitled *Identity Crisis: How Identification is Overused and Misunderstood.* The book articulates the mechanics of identification as a social and economic process, and it posits the government policies that will deliver consumers and citizens the fullest benefits of identification while avoiding identification policies inconsistent with American liberty.

In my testimony below, I will first discuss biometrics in general and the well-founded concerns about the rapid advance of machine-readable biometric technologies. Next, I will assess how, and how well, S.B. 98 address those concerns. Finally, I will offer the policies I recommend to you in this area.

Thank you again for the chance to address your committee. I hope you find the following material helpful.

A Brief Biometrics Primer

The term "biometrics" is formed of two Greek roots: *bios* (life) and *metron* (measure or degree). Biometrics is simply the measurement of living things. Biometric identification is the measurement of identifiers from living (and formerly living) things to distinguish them from one another.[1]

Biometrics is widely spoken of as an emerging, high-tech field, but it has been practiced since before recorded history—by human beings, animals, and even plants. When we recognize each other—when we see a friend walking down the street or hear a spouse sneezing in the kitchen—we note and compare the physical identifiers found on and about each other's bodies with identifiers we have collected before. Our observations are not recorded in millimeters, degrees, or wavelengths, of course—the process is a natural one performed in the brain—but we are just as surely measuring one another's physical characteristics.

There are two major categories of biometrics: physiological and behavioral.

Physiological biometrics measure the distinct traits that people have on their bodies. Examples of physiological biometrics are all the things we most commonly think of—hair color, eye color, sex, skin color, height, weight, and so on. They also include

[1] *See generally*, Jim Harper, IDENTITY CRISIS: HOW IDENTIFICATION IS OVERUSED AND MISUNDERSTOOD 24 (2006).

many more identifiers that will come into use with the advance of technology: retina and iris scans, facial geometry analysis, and fingerprint scanning. There are many more examples.

Behavioral biometrics measure the distinct actions that humans take, which are generally very hard to copy from one person to another. Behavioral biometrics include signatures, voice printing, and gait analysis, for example, which measure the movements of the hand, the sounds created by the voice box, and the distinct movements of a person walking. Analyzing voices and movements is easily done by humans, less easily done by machines today, but the technologies that read behavioral biometrics are improving.

The "new" field of biometrics refers to the use of machines and computers in biometric identification, an important development that has distinct consequences. A variety of machine-readable biometrics, including fingerprint scanning, iris scanning, and hand geometry appear poised for broader use.

In general, machine-readable biometric identification works by having a machine measure the relevant characteristic and compare it to earlier collected examples, thus establishing identity and "recognizing" a person. The technical ways this works vary, but typically a sensor will convert the biological observation into a mathematical description. The arches, loops, and whorls in a fingerprint, for example, will be recorded digitally along with the distances and angles among them. The digital description will then be compared to another such description (one-to-one) or to a number of them (one-to-many), producing a "match" when there is sufficient similarity between two.

Using machines to identify people can provide very highly assured comparisons between the biometric information stored in identity records and the information found on people when they present themselves to be identified. Machines do not get tired and they do not get bored. Nor are they subject to peer pressure, embarrassment, or any similar human defect. These security benefits are what advocates of biometrics put forth, and they are real.

There are important consequences when biometric identifiers are scanned by machines rather than people. Biometrics do not always work as advertised, for example, and it is important not to place too much reliance on them while they are relatively new and untested. The skin on the fingers thins as people age, making fingerprints harder to read. Manual laborers or hobbyists who work with caustic agents may burn off or thin their fingerprints. And injury can alter or remove fingerprints right along with fingers.

These issues can be ameliorated, but other concerns with machine-readable biometrics will not dissipate with time and experience. For example, a digital record of a biometric can be stored indefinitely, copied an infinite number of times, and transmitted around the globe at the speed of light. This creates security and privacy concerns cutting against the use of machine-biometrics.

For example, over a long enough time horizon, it is likely that new high-tech forms of identity fraud will emerge in the form of spoofed biometrics. False fingerprints have already been created, and research into generating fingerprints from their mathematical descriptions is ongoing. When this form of deception makes its way into practice, there is significant potential for fraud, crime, and injustice.

Some biometrics may reveal not just abstract measurements of the individual, but information about the person's health, susceptibility to disease, ancestry, race, and so on. This is most true of DNA and least true of surface measurements such as fingerprints. Future developments in medical science and biometric analysis will reveal the collateral data that biometric identification might reveal.

Machine-biometric identification has significant benefits and significant drawbacks. The stakes are high on both sides, which is why this issue is so important to examine carefully. We are at an early stage in the development of biometric identification technologies, and it is important to take great care, seeking the benefits of biometrics while avoiding their drawbacks.

How S.B. 98 Addresses Biometrics

Even if it were possible to determine how to do it at this early stage, it is not the role of government in a free society to determine how technology shall be used—even important and powerful technologies like biometrics. Rather, government's role is to prevent the infringement of rights, such as the rights to life, property, speech, conscience, and such.[2] S.B. 98 deviates from this principle rather dramatically, setting in place rules of conduct with respect to biometrics that are likely to inappropriately limit their use and prevent the security benefits of biometrics from emerging in the future.

Many of the requirements of S.B. 98 are good ideas, but it is not a good idea to mandate them top-down. In thousands of situations that will arise in the future, the rules we could come up with today are likely to result in complexity and high costs that limit the use of biometrics and the enjoyment of their benefits.

Biometrics Definitions

The definition of "biometric information" in the bill (18.14.090(2)) is both too narrow and too broad, which makes it likely to cause complexity and confusion as biometric technology develops. It is too narrow because "biometric data" (18.14.090(1)) separately defined and incorporated into "biometric information," is a listing of body parts used in biometrics currently. It is not a generic definition going to the dimension of

[2] *See generally,* Erich Weede, "Human Rights, Limited Government, and Capitalism," Cato Journal, Vol. 28, No. 1 (Winter 2008) at 35 http://www.cato.org/pubs/journal/cj28n1/cj28n1-3.pdf.

biometrics that causes concern: bodily measurements collected and stored digitally for the purpose of identifying. The bill's definition may leave some future technology outside the scope of the law though it carries all the consequences that animated the introduction of the bill.

The definition is too broad because it may reach a variety of systems that are emerging or now in use that do not animate the bill. Online social networks, for example, are experimenting with "facial mapping" to identify people in photographs, making friends easy to tag and simplifying the social experience of uploading photos. This may be concerning in terms of privacy, but such concerns are a distant relation to the concerns this bill is meant to address.

Notice and Consent

The "notice and consent" model adopted by the bill (18.14.010(a)) has been a staple of privacy regulation for years, but that model has not succeeded in protecting privacy. Because they are legally mandated and not demanded in the marketplace, privacy notices tend toward verbose legalese. Job one of regulated entities is to avoid a legally insufficient notice, and the notice required by this bill will almost certainly be unreadable by ordinary people. Consumers will then doggedly insist on *not* reading such notices, which stand in the way of their getting what they want. Instead, they will agree to whatever terms are presented to them, which is nothing like the "full consent" that the bill envisions (18.14.010(a)(2)).

If only we could make consumers privacy-aware and -protective, what a world it would be. But consumers have a variety of interests, among which privacy is only one—and they often ignore it. Under the notice-and-choice regime in the bill, consumers would collude with biometrics collectors to move forward in any given transaction, sharing whatever is necessary and doing the absolute minimum to satisfy legal requirements placed in their way.

It won't be legislation and regulation. Only experience and time will bring consumers to the awareness of biometrics and their privacy consequences that causes them to assert their interests.

Revocation and Amendment of Permission, Disposal of Data

Giving consumers a right to revoke or amend consent to use of previously shared biometric information (18.14.010(b)) may sound simple, but the technical systems that

house, back up, and use biometric data make such a right extremely complex to administer.[3]

For sound security and continuity purposes, data systems make multiple backups that come to rest in various places and forms. Secondary systems that do fraud detection, statistical analysis, marketing, and so on will multiply the number of copies further. Auditing systems may cause further rounds of copies to be made. The problems are similar with any right to require disposal of data. (18.14.050)

Removing data, altering its use, or disposing of it upon individual demand would be something like finding the molecules of gasoline that escaped your gas tank when the gas cap came off. It is certainly possible to devise a gas tank from which molecules will not escape, but that is a more complex gas tank that is more expensive to build and harder to fill. Information systems with the custom controls required by S.B. 98 would be more expensive to build and harder to operate.

Outlawed Marketing

Maybe the movie "Minority Report" inclines people against using biometrics for marketing or general surveillance purposes, but society may not always feel this way. Advertising to people using information about them is not harmful. Indeed, it tends to be more informative and less wasteful than non-targeted advertising.

The restrictions on marketing in the bill (18.14.060) appear to cover quite a bit more than the laser monitoring of our eyeballs we have seen in the movies. The way the bill is constructed, a fully informed consumer—even a biometrics and privacy expert—could not consent to receive marketing that is produced using biometric identification of the consumer.

Consider a future where grocery store payment systems use biometrics to provide security and convenience. The ban on marketing would make it illegal to give consumers a coupon at the check-out counter because biometrics are in use, or to use consumer purchase information for tailoring product ordering and store layouts.

Imagine that a web site using biometric encryption to identify users wants to provide them free, advertising-supported services. The advertising could not be tailored to the user because the user had identified him- or herself to the site using biometrics.

Aware, adult Alaskans should have the freedom to decide on their own how they interact with the variety of sites and services that will emerge in the future. The flat ban

[3] *See* Jeff Jonas blog, "How Many Copies of Your Data? Is Somewhat Like Asking: How Many Licks to the Center of the Tootsie Pop?" (August 8, 2007) http://jeffjonas.typepad.com/jeff_jonas/2007/08/how-many-copies.html.

on marketing or surveillance using biometrics may limit consumer benefits significantly if it cannot be overcome even by fully informed consumers giving their full consent.

Penalties

The private right of action created by the bill needlessly creates a "penalty" of $5,000 (and $100,000 in cases of intentionality) when violations may cause nowhere near that kind of damage to the persons the bill is intended to protect. These huge potential penalties will counsel against the use of biometrics even where they might make consumers better off overall.

And these penalties are potentially huge. Data systems tend to treat large numbers of records the same way, so even a $5,000 penalty could impose exorbitant liability reaching into the millions or billions of dollars if a biometric data collector has allowed an imperfection into the operation of its systems.

Damage awards should generally make the injured party whole. Where biometric data is misused and harm comes to a consumer, the consumer deserves compensation. But gigantic penalties will do no justice in enriching lawyers and lucky "victims."

I understand the concerns with overuse of biometrics at this early stage in their development, but the provisions of S.B. 98 overreact to those concerns. They do not seem calibrated toward balancing the costs and benefits of biometrics. The bill focuses on prescriptive regulation rather than harm-prevention. Preventing Alaskans from being harmed should be the focus, and lighter-touch legislation could do that.

Addressing Biometrics With a Lighter Touch

The concerns around biometrics are real, and there are things the state of Alaska can do to give Alaskans greater confidence they are protected—without tilting the playing field against biometrics use.

The goal is to ensure that biometrics collectors account for and prevent potential harm to Alaskans when they design and use their systems. It is not to prevent biometrics being used altogether or to constrain biometrics so much that their security benefits never materialize. To do this, the Alaska legislature should ensure that its law is prepared to address information-age challenges.

Contract and Tort Liability Clarified

Alaska law should makes biometrics collectors in Alaska liable for contract and tort violations wherever they may occur. If biometrics are collected in Alaska subject to promised limits on how they will be used, promises of timely data destruction, and so on, violations of those promises occurring anywhere should create a cause of action in

Alaska. If biometrics collected in Alaska are used negligently anywhere, allowing harm to come to the individual, this should create a cause of action in Alaska.

The legislature could similarly specify that collection of biometrics (and other personally identifiable data) creates jurisdiction in Alaska over the entity doing the collection (or for whom it is collected). This would ensure that they have remedies for wrongs committed against them by out-of-state entities using their data.

If it is not already the law, the legislature could specify that the statute of limitations on causes of action begins to run when a wrong is discovered, not when it was committed. This would protect against situations where a biometrics (or other data) collector violates a promise or obligation that goes undiscovered for years before causing harm.

If Alaska law does not already meet these recommendations, careful fixes to jurisdictional rules could ensure that Alaskans are protected from private wrongdoing. The legislature can also help protect against public entities wrongly gaining access to biometric data.

No "Third-Party" Doctrine in Alaska

The U.S. Supreme Court's "third-party doctrine" holds that information a person shares with someone else is not subject to Fourth Amendment protection by virtue of that sharing, even if the recipient is subject to privacy-protective promises or regulations.[4] State courts are free to find greater protection for their citizens' and residents' rights than are found in the federal constitution, even under similar language.[5]

The Alaska legislature could strongly signal to Alaska's courts (and federal courts applying Alaska law) that the "third-party doctrine" in federal constitutional law is not the law in Alaska. Under either the Alaska constitution's search-and-seizure clause (Art. I, sec. 14) or the right-to-privacy clause (Art. I, sec. 22), Alaska courts could find that Alaskans sharing biometric information subject to contractual privacy protections have the right to prevent government access to that data in the absence of proper suspicion, warrants, and subpoenas.

Indeed, Article I, section 22 empowers the legislature to implement the state constitutional right to privacy. It could do so consistent with limited government by

---

[4] *See,* Jim Harper, "Reforming Fourth Amendment Privacy Doctrine," 57 Am. U. L. Rev. 1381, 1401 (June 2008) http://tinyurl.com/cv223g8.

[5] The U.S. Supreme Court is the ultimate arbiter of questions of federal law but the state courts are the ultimate arbiters of the laws of each state. *See, e.g., Hortonville Joint School District No. 1. v. Hortonville Education Ass'n*, 426 U.S. 482, 488 (1976).

specifying that contractual protections for privacy preserve Alaskans search-and-seizure rights in information shared with others.

There are more "light-touch" methods of getting to the potential problem of biometrics over-use.

Avoid Occupational Cartels

The demand for biometrics in administration of the CPA exam, which motivated this bill, may or may not be excessive. One thing the legislature can do without prescriptively regulating biometrics is to ensure that occupational licensing has not created a state-sponsored cartel that can make unreasonable, privacy-invasive demands like this.

Occupational testing and certification can signal quality, but it is often used to limit access to the practice of a profession. This unnaturally drives up the salaries of providers and costs to consumers.

Alaska should eliminate any legal restrictions on entry into the profession of accounting in two ways. First, it should eliminate any legal requirement that one pass the CPA exam before providing accounting services. Those who do not wish to take the exam can seek to assure the quality of their work through their reputations and with contractual promises. Second, Alaska should eliminate any requirement that filings submitted to the state be produced by CPAs. Someone with the qualifications to act as an accountant should be able to provide those services without having taken an exam if they can assure their clients that they are good enough at doing the work.

Commit Alaska to Oppose Biometric National ID Systems

Additional measures can assure Alaskans of their protection from overweening biometrics requirements. Following up on Alaska's May 2008 rejection of the REAL ID national ID law,[6] the state should reject mandatory use of the federal E-Verify system and bar its motor vehicle bureau from sharing information wholesale with the federal government for identification purposes.

E-Verify is a federal background check system operated by the Department of Homeland Security.[7] If its advocates get their way, it will be used on every worker in the United States. Once in place, little prevents the federal government from using E-Verify

---

[6] *See,* SitNews.us "Alaska Legislature Stops Real ID Act Implementation" (April 12, 2008) http://www.sitnews.us/0408news/041208/041208_realid.html.

[7] *See generally,* Jim Harper, "Electronic Employment Eligibility Verification: Franz Kafka's Solution to Illegal Immigration," Cato Policy Analysis No. 612 (March 6, 2008) http://www.cato.org/publications/policy-analysis/electronic-employment-eligibility-verification-franz-kafkas-solution-illegal-immigration.

to control access to housing, financial services, medical care, guns, Internet access, and so on. The New Hampshire House of Representatives recently passed legislation to refuse the federal government access to state data for use in E-Verify. I commend it to your attention.[8]

There are a variety of things the Alaska legislature can do to help assure Alaskans privacy and to foster the development of biometrics technology consistent with Alaskans' interests. These are a lighter touch than the direct regulation of biometrics found in the current version of S.B. 98.

Conclusion

As a person who fights privacy battles, I have acute sympathy for the supporters of S.B. 98. One of my pet peeves is the practice in accounting departments of collecting Social Security Numbers for *all* payments, even when there is no requirement that a payment be reported to the Internal Revenue Service (non-income and income of less than $600).

I pursued this issue with the American Institute of CPAs (AICPA) in 2008, hoping that they might consider encouraging their profession to factor privacy protection over convenience in this area. I got nowhere with them. I would not call for a law barring the collection of Social Security Numbers, though. That is something for me to advocate and press for using my influence as a citizen, not using government coercion.

The direct regulation of biometrics in S.B. 98 uses too much government coercion at too early a stage in the development of these technologies. It is too blunt an instrument for figuring out how biometrics can be used. Indeed, it will be generations before all the biometric technologies, all their benefits, and all their costs are known.

There are consumer benefits to biometrics and the security they can provide. Lighter-touch actions by the Alaska legislature can help protect and assure Alaskans' privacy while encouraging all the actors in the field to seek the right balances among privacy, security, cost, and convenience in biometric technologies.

---

[8] *See* Jim Harper, "National Surveillance Programs and Their State Impediments," Cato@Liberty blog (Mar. 16, 2012) http://www.cato-at-liberty.org/national-surveillance-programs-and-their-state-impediments/.

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
Admin Reg Review

SENATOR BILL WIELECHOWSKI

January 24, 2011

The Honorable Wes Keller, Chair
House Health and Social Services Committee
State Capitol, Room 4132
Juneau, Alaska 99801

Dear Representative Keller:

I expect the following people to testify:

Jason Giaimo, Co-chair of Citizens for Privacy in Alaska
Timothy Pearson, Co-chair of Citizens for Privacy in Alaska
Horst Poepperl, CEO of Borealis Broadband

Thank you for your consideration of this request.

Sam Gottstein
Staff to Senator Wielechowski

My name is Dan Boland. I am a 21 year citizen of Anchorage Alaska.

I want it known to Alaska elected officials that I am against the collection biometric data in any form by anyone for any purpose expect in case where law enforcement concerning a felon.

I am of the opinion that the collection, storing, selling and trading biometric data of lawful citizens of the United States is a form of fascism which my father and his brothers were called to fight against in World War II.

I am outraged to learn corporation doing business in Alaska are demanding citizens to submit to surrendering their biometric data before the citizen can apply for a job or educational test that might improve their economic status. I would think a driver's license would be sufficient considering when I applied for an Alaskan driver's license I had to submit a notorized copy of my birth certificate.

If new applicants in Alaska wanting to become CPA's have to submit to biometric sampling then should not all the current Alaskan CPA's be required to submit their biometric data? What about engineers, doctors, lawyers, pipe fitters, carpenters, general contractors, most of these have to be licensed/certified to work in the State of Alaska, should they also be finger printed like criminals?

The fact that a foreign owned corporation is doing business in Alaska collecting American biometric data sounds like Hollywood action thriller movie. Who is going to regulate these companies once the biometric data is collected? How can a citizen be assured their biometric data won't be sold or traded or worse used for illegal purpose such as framing a citizen for a crime? Yes I know I sound paranoid. I have a right to be. The collection of biometric data reeks of fascism.

I have read HB 98 and found part of it lacking strength to guard against misuse of my biometric data. HB 98 needs to retain that section of the bill pertaining to Alternate identification which is Sec 18.14.040. The alternate identification needs to be spelled out as any combination of two of the following "a State Drivers license, US Passport and or copy of notarized Birth Certificate."

I also have problems with the following sections of HB 98 as following:

Sec 18.14.50 Disposal (a). The requirement of 120 days to destroy the data should be lowered to 7 days perhaps 15 at most.

Sec 18.14.50 Disposal (b). Within 30 days need to be reduced to 7 days. Why hang on to the data for 30 days if they know they don't need it.

That part that of Sec 18.14.080 Right of Action that reads "penalty of $5,000,) I believe it should be increased to $100,000.

That part of Sec 18.14.080 Right of Action (a) that reads "a penalty of $100,000" I believe it should be increased to $5,000,000.

Without the increased penalty amounts the bill has no teeth, There is no incentive for large ultra wealthy companies with unlimited cash reserves to pay attention to this law. Without the hefty penalty the large corporations once again profit at the expense of individual citizens losing their rights to privacy or worse. Please add some teeth to this bill increasing the penalties.

Thank you for your time and I hope you do what is right and just for protecting individual rights.

Dan Boland

Hi Kathy, Kelly, and Lt. Dial,

Thank you for Public Safety's willingness to be available for questions on SB 98. We will hear the bill on Tuesday March 27th from 3-5pm.

I talked with Kelly about this a couple of days ago so she should have a pretty good idea of the information we are looking for.

We are hoping you can provide some perspective on whether stolen biometric information is of any significant value or whether the fears of stolen biometrics fall within a CSI/Mission Impossible "perfect crime" scenario. Here are some of the ideas we would like considered:

1) What expertise would it take to find, steal, and replicate another person's biometric information? From a cost benefit analysis, is it worth my time to try and steal someone else's biometric info and use is for an unlawful purpose? This is a complex question. What is commonly referred to as 'fingerprints' pertains to the friction ridge structure on the end joint of the fingers and thumbs. "Friction ridges" are actually present on the entire finger, palm, toes and soles of the feet. To obtain all this data and replicate it would be quite difficult. That said, based on the documents linked to this bill, I think the fear is that someone could 'take' an electronic copy of another person's fingerprints that were recorded for a variety of purposes. It would be very difficult to take these images and change them into what appeared to be a 'latent' print. (That is the term for prints that are not generally visible to the naked eye and are processed using chemicals or other means to allow for viewing, analysis and preservation of these prints, typically left at crime scenes.)

How difficult of a process is it for law enforcement to determine if an individual's biometric information is fraudulently used by another person or entity? For example, lets say that someone manages to obtain my fingerprints, makes a usable fake copy and commits a crime in Florida. If I can prove I was in fact in Alaska and not Florida, has any harm really come to me—besides someone trying to pretend it was me? Or if someone manages wants to take enter a secure area and tries to pass off a fake copy of my fingerprint or retina scan? It seems that these scenarios depend on biometrics being the only security system being used rather than a multilayered one. Again, taking someone's electronic 'known' prints and somehow 'planting' them at the scene of a crime is probably not impossible, but highly unlikely. Because electronic fingerprints do not contain the perspiration or other substances that cause a latent impression to be left on an object that is touched, it is unlikely that a qualified latent print examiner would fail to identify the fact that the prints were 'planted'. There are other much simpler methods to obtain a person's prints surreptitiously if someone if of that mindset.

2) Is the consequences of stolen biometric information as great as the consequences of someone accessing my bank account for example? Because it is unlikely that a person would benefit from obtaining someone else's electronic fingerprints for use at a crime scene, the only practical purpose to take someone else's prints would be to obscure the identity of the person who took the prints. This could be used to hide a criminal history record, but there are processes in place through the National Crime Prevention and Privacy Compact ("Compact Council", of which Alaska is a member.) to ensure the interstate sharing of fingerprint data is done securely and respects the privacy of the contributor.
3) Is theft of biometric information a significant problem? Or are the potential consequences largely a hypothetical fear? I have never heard of a bona fide case of theft of biometric information. Identity theft is a significant issue; most often, we are able to unravel any confusion only because we have fingerprints of both the victim and the perpetrator.
4) Does the State of Alaska use biometric information for security purposes? If so, is it part of a multilayered ID verification purpose or the only means of verifying a person's ID? I know of no State of Alaska systems using biometric information for security purposes. It is an approved method for network security authentication.

As an aside; some of the documentation sites cases where private businesses might use fingerprints for security purposes. In fact, my grandchildren's day care uses fingerprint identification for drop of and retrieval of all children. I

cannot think of a way that this information could be misused by the private sector to obtain information about me that is not readily obtainable through debit cards or store 'rewards' cards.

Please let me know if I can be of further assistance. As I indicated, I will be on line today to answer any questions that may come up on this topic. I was a fingerprint examiner for almost 19 years, and have been the Chief of DPS' Criminal Records and Identification Bureau since 1995.

Kathy

Please let me know if these are issues you can provide some expertise on. If you have questions or ways to better ask the questions, please feel free to give me a call.

Thanks,

Ernest Prax
Office of Representative Wes Keller
State Capitol, Room 432
Juneau, AK 99801
Phone: 465-2186; Fax: 465-3818

SB 98 addresses very important and interesting issue... commendation – but...

Technology is making it exponentially easier to collect, store, classify PII. I grew up with key PII being my signature--- biometrics... (iris scans, voice, pictures...) digitally and ramifications are huge.

Once digitized an on-line, it is virtually impossible to ensure all erased. ----------

No decision today--- Please help me cram as many testifiers as we can so questions are on the table... then we will all process ...

UNFORTUNATELY many perspectives when coming into this discussion.. ONE is

- Personal privacy---
- Another, --- is focused on government over-regulation of business
- Security of property --- protection of sensitive/ proprietary information
- Abuses --- discrimination potential (Jews in Holocost)
- Technology focus--- every year we keep seeing unimaginable progress...

With all these perspectives, we have had some unfortunate preludes to this discussion:

- Name calling character assassinations (paranoid, corrupt,...)
- False accusations --- characterizations--- Attacks

  Business v legislature v citizens

- Overstatements exaggeration--- all sides

Try to put all away – don't spend time on apologies or continued attacks. No disrespect will be tolerated. Lets learn so we can decide...

1.5 hours--- 8-10 experts All questions on tap please—some responses may come later in letters to complete our crash course.

RESIDENT EXPERT Ernest Prax. We have spent many hours on this issue--- Ernest is a super researcher and scholar. He will be on tap in our office. Also Sam Gottstein in Sen W office...