SB

98

<TARGET><BILL>SB 98</BILL><SUBJECT>SB
98</SUBJECT><COMM>SSTA27</COMM></TARGET>

27-LS0014\B
Kane
3/15/11

SENATE CS FOR HOUSE BILL NO. 98(STA)

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-SEVENTH LEGISLATURE - FIRST SESSION

BY THE SENATE STATE AFFAIRS COMMITTEE

Offered:
Referred:

Sponsor(s): REPRESENTATIVES JOHNSON, Hawker, Keller, Costello, Chenault, Olson, Millett, Fairclough, Kerttula, Feige, Thomas, Peggy Wilson, Kawasaki, Johansen

SENATORS McGuire, Giessel, Meyer, Menard, Ellis, Wagoner, Egan, Dyson, Stevens

A BILL

FOR AN ACT ENTITLED

"An Act relating to display, folding, presentment, and retirement of the state flag."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:

* **Section 1.** AS 44.09.030 is amended by adding new subsections to read:

(d) When displayed horizontally in a public facility, the flag shall be positioned with the hoist on the left and the North Star in the upper right corner.

(e) When displayed vertically in a public facility, the flag shall be positioned with the hoist at the top and the North Star in the lower right corner.

* **Sec. 2.** AS 44.09 is amended by adding new sections to read:

Sec. 44.09.032. Folding and presenting the state flag. (a) When folding the state flag, the following procedure shall be followed, whenever possible:

(1) hold the flag waist-high with another person, so that the flag is parallel to the ground and the hoist is on the left;

(2) fold the flag lengthwise, with the open edge up;

(3) holding the edges securely, rotate the flag so that five stars are facing up;

(4) fold the flag lengthwise a second time, with the open edge up;

(5) holding the edges securely, rotate the flag so that two stars are facing up;

(6) fold the flag widthwise, with the North Star facing down and the hoist on the right;

(7) holding the edges securely, fold the flag widthwise a second time, with the North Star facing down and the hoist on the right;

(8) fold the flag widthwise a third time, with the North Star facing up.

(b) When presenting the folded flag to another person, the folded flag should be turned so that the North Star is nearest the receiver.

Sec. 44.09.034. Retirement of the state flag. An official flag of the state that is no longer a fitting emblem for display because it is worn, tattered, or otherwise damaged may be respectfully retired by fire in a ceremony or other dignified manner honoring the flag as a fitting emblem for the state. When practicable, retirement of the state flag should occur in a public ceremony under the direction of uniformed personnel representing a state or federal military service or a patriotic society. If a formal ceremony is not practicable, a private ceremony is acceptable.

* **Sec. 3.** AS 44.09.030(c) is repealed.

27-LS0661\M.1
Bannister
3/16/11

AMENDMENT

OFFERED IN THE SENATE BY SENATOR WIELECHOWSKI

TO: CSSB 98(STA), Draft Version "M"

Page 4, line 2:

Delete "palm print"

Insert "skin"

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

Senate Bill 98

"An Act Relating to the use of biometric information"

Sponsor Statement

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 holds great promise for fields such as medicine and law enforcement. However, this technology also holds the potential for misuse by those who would use a person's genetic data to obtain information about them that Alaskans would normally have a right to keep private.

Senate Bill 98 would update Alaska statutes to protect not only Alaskans' DNA, but all similar forms of biometric information. The term "biometric information" refers to any information about an individual based on their unique behavioral or physiological characteristics. The most commonly known forms of biometric information are a person's fingerprints and their DNA, but also includes such information as iris and retinal patterns, hand geometry, voice patterns, and facial characteristics.

Many potential uses of biometric information are still at the rudimentary stages of development. However, new technologies will soon be available that will be able to make use of this information with chilling consequences for individual privacy and civil liberties.

Examples of the potential misuse of biometric information include the collection of an individual's data by potential employers or insurers to weed out applicants that may have a genetic predisposition towards certain illnesses and the use of video surveillance enhanced by facial recognition technology to track citizens' movements without their knowledge.

Alaskans should bear in mind that one of the proposed requirements of the Federal REAL ID Act was that every Alaskan ID card contain a radio frequency identification (RFID) chip, which would allow a citizen's movements to be tracked without their knowledge.

Thankfully, the State of Alaska joined other states in refusing to submit to the REAL ID Act. The legislature should take a similar strong stand to protect Alaskans' biometric information and their constitutional right to privacy.

27-LS0661\M
Bannister
3/11/11

CS FOR SENATE BILL NO. 98(STA)

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-SEVENTH LEGISLATURE - FIRST SESSION

BY THE SENATE STATE AFFAIRS COMMITTEE

Offered:
Referred:

Sponsor(s): SENATORS WIELECHOWSKI, Coghill, Ellis, Menard, McGuire, Giessel, Egan, Paskvan, Thomas

A BILL

FOR AN ACT ENTITLED

"An Act relating to biometric information."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:

*** Section 1.** AS 18 is amended by adding a new chapter to read:

Chapter 14. Biometric Information.

Sec. 18.14.010. Biometric information consent. (a) A person may not retain or analyze, or disclose or distribute to another person, biometric information on an individual without first obtaining the informed and written consent of the individual.

(b) An individual may, at any time, revoke or amend the individual's consent provided under (a) of this section.

Sec. 18.14.020. Alternate identification. A person may not require an individual to provide biometric data to the person for the purpose of identifying the individual if the individual provides the person with a valid current

(1) United States passport; or

(2) identification card issued by a state in the United States or by a branch of the armed forces of the United States.

Sec. 18.14.030. Uniform consent form. The Department of Health and Social Services may by regulation adopt a uniform consent form to assist persons to meet the requirements for the consent required by AS 18.14.010. A person who retains or analyzes, or discloses or distributes to another person, biometric information, based on consent that is provided in a uniform consent form that has not been revoked, is exempt from civil liability under AS 18.14.060 and from criminal liability for the retention, analysis, disclosure, or distribution of the biometric information.

Sec. 18.14.040. General authorization. A general authorization for the release of medical records or medical information may not be construed to constitute the informed and written consent required by AS 18.14.010.

Sec. 18.14.050. Private right of action. An individual may bring a civil action against another person who violates AS 18.14.010 or 18.14.020. Except as provided by AS 18.14.030, a person who violates AS 18.14.010 is liable to the individual for actual damages and a penalty of $5,000, except that, if the violation resulted in profit or monetary gain to the person, the penalty is $100,000.

Sec. 18.14.060. Exemptions. This chapter does not apply to the collection, retention, analysis, disclosure, or distribution of

(1) biometric information for a law enforcement purpose, including the identification of perpetrators, the investigation of crimes, the identification of missing or unidentified persons, or the identification of human remains;

(2) biometric information when authorized by state or federal law;

(3) facial images by the Department of Administration for drivers' licenses issued under AS 28.15, for state identification cards issued under AS 18.65.310, for administering AS 28.15, or for administering AS 18.65.310; or

(4) facial images that are not used in a biometric system.

Sec. 18.14.090. Definitions. In this chapter,

(1) "biometric data" means fingerprints, handprints, voices, facial images, iris images, retinal images, vein scans, hand geometry, or finger geometry;

(2) "biometric information" means biometric data that is used in a biometric system for fingerprint recognition, hand geometry recognition, finger geometry recognition, voice recognition, facial recognition, iris scans, retinal scans, or

vein recognition;

(3) "biometric system" means an automated system capable of

(A) capturing biometric data from an individual's biometric information;

(B) extracting and processing the biometric data captured under (A) of this paragraph;

(C) storing the biometric data extracted under (B) of this paragraph;

(D) comparing the biometric data extracted under (B) of this paragraph with biometric data stored for the individual for use in future recognition of the individual; and

(E) determining how well the extracted and stored biometric data match when compared under (D) of this paragraph, and indicating whether an identification or verification of identity has been achieved;

(4) "facial recognition" means the use of an image of the visible physical structure of an individual's face for recognition purposes;

(5) "finger geometry recognition" means the use of the shape and dimensions of one or more fingers for recognition purposes;

(6) "fingerprint recognition" means the use of the physical structure of an individual's fingerprint for recognition purposes;

(7) "governmental entity" means a state agency, a municipality, and an agency of a municipality; in this paragraph, "state agency" means an agency of the executive, judicial, or legislative branch of state government;

(8) "hand geometry recognition" means the use of the physical structure of an individual's hand for recognition purposes;

(9) "iris scan" means the use of an image of the physical structure of an individual's iris for recognition purposes;

(10) "person" has the meaning given in AS 01.10.060, and includes a governmental entity;

(11) "retinal scan" means the use of the pattern of blood vessels in an individual's eye for recognition purposes;

(12) "vein recognition" means the use of the veins in an individual's palm print for recognition purposes.

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 14, 2011

SUBJECT: Sectional summary of SB 98 relating to biometric information (Work Order No. 27-LS0661\A)

TO: Senator Bill Wielechowski
Attn: Michelle Sydeman

FROM: Theresa 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 prohibits retaining, analyzing, disclosing, or distributing an individual's biometric information without obtaining the individual's consent. Allows the individual to revoke or amend the consent.

Sec. 18.14.020 prohibits a person from requiring an individual to provide biometric data for identification if the individual provides certain other identification.

Sec. 18.14.030 authorizes the Department of Health and Social Services to adopt a uniform consent form for sec. 18.14.010. If a person uses an unrevoked uniform consent form for an individual's consent, exempts the person from civil liability under sec. 18.14.060 and criminal liability for retention, analysis, disclosure, or distribution of the individual's biometric information.

Sec. 18.14.040 states that a general authorization for the release of medical information does not constitute the consent required by sec. 18.14.010.

Sec. 18.14.050 provides an individual with a private right of action for violations of secs. 18.14.010 or 18.14.020. Establishes that the violator of sec. 18.14.010 is liable to the individual for actual damages and a penalty.

Sec. 18.14.060 lists the exemptions from the chapter.

Sec. 18.14.090 defines terms for the chapter.

If I may be of further assistance, please advise.

TLB:plm
11-139.plm

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

Explanation of Changes From Original to CS, Version "M"

- **Page 1, Line 13**: The "and" has been changed to an "or," allowing a person to only present one form of identification.
- **Page 2, Line 18 and 21:** The term "biometric information" has been added to clarify.
- **Page 2, Lines 22-25:** Exemptions were clarified for the issuance of drivers' licenses, ID cards, and pictures not entered into a biometric system.
- **Page 2, Line 28:** Vein scans, hand geometry, and finger geometry were added as definitions of biometric data.
- **Page 2, Line 30:** Finger geometry recognition was included as a definition of biometric information. Its corresponding definition was added on **Page 3, Lines 17 and 18**.
- **Page 3, Line 1:** The word "palm" was removed from "palm vein recognition" in the definition of biometric information.

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

- There is a growing trend for companies and organizations to use biometric data as a means of identifying individuals. By giving personal biometric information, like fingerprints, iris scans, or facial images, a person gives away highly personal, traceable information.

- Passports, identification cards, and social security cards can be used to travel abroad, identify oneself in court, and a plethora of other activities. These should be suitable checks of identification.

- Organizations that collect biometric data routinely sell that data to third parties, without our consent.

- There is no doubt biometric data can be extremely helpful in fields such as medicine and security, but we should never be forced to give up such personal identification. This bill does not ban biometrics, but bans their use without our consent.

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.

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.

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*

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 introduce 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, Dept of Motor Vehicals	Director	Anchorage, AK	"The Alaska State Department of Motor Vehicals 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.

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—Biometric Information: What Are Other States Doing?

What are other states doing regarding the collection of biometric data?

In 2008, our office requested a research report asking which states have legislation preventing the collection of a person's biometric data, such as a fingerprints or DNA, for purposes other than law enforcement.

We received a comprehensive list of states that have laws prohibiting genetic discrimination in employment, prohibiting employers from requesting or requiring genetic information, prohibiting employers from performing genetic testing, and similar situations. In all, the researcher identified through the NCSL employment laws in 36 jurisdictions.

When it comes to non-genetic biometric information, the researcher identified 33 states which have some form of legislation, which includes a wide range of topic from prohibiting the use of lie detectors by anyone except peace officers in California, to requiring the Commissioner of Health and Social Services to examine the use of biometric identifiers for recipients of public assistance.

Among some of the more notable laws are Indiana, which prohibits the collection of personal information, including voice prints, by state agencies to that which is relevant and necessary to accomplish a statutory purpose; and New Hampshire which prohibits the collection of "biometric data" in connection with motor vehicle licensing.

Other states, such as Oregon, require those who apply for a driver's license to submit to the collection of biometric data.

Essentially, all states which have laws regarding DNA tend to protect that information at least for employment purposes, but the states vary greatly when it comes to other biometric information.

What About the Federal Government?

You will also find on Page 2 of the document in your packet titled, "Biometrics: Who's Watching You?" there is a description of some of the federal initiatives involving the biometrics. The most recent of these is the USA Patriot Act, which requires the use of biometric technology to identify foreign visitors, and the Enhanced Border and Visa Entry Reform Act of 2002, which is specific to border crossings.

LEGISLATIVE RESEARCH REPORT

NOVEMBER 20, 2008

REPORT NUMBER 09.031

STATE LAWS REGARDING BIOMETRIC PRIVACY

PREPARED FOR SENATOR BILL WIELECHOWSKI

BY ROGER WITHINGTON, LEGISLATIVE ANALYST

You asked for information regarding privacy. Specifically, you wished to know what states, if any, have laws that prohibit the collection of a person's biometric data, such as a fingerprint or deoxyribonucleic acid (DNA), for purposes other than law enforcement.

As you may know, the term "biometrics" is used for the various ways humans can be identified through unique aspects of their bodies. Fingerprints are probably the most commonly known biometric identifier. Other biometric identifiers include hand prints, vein dimensions, iris designs, blood vessels on retinas, body odor, walking characteristics, voice patterns, facial features, and genetic profile.[1]

The National Conference of State Legislatures (NCSL) collects information on actions state legislatures have taken to safeguard a persons' genetic information.[2] One common theme in state law is to protect employees and job seekers from genetic screening and discrimination. In Table 1, we provide NCSL's summary of state employment laws that pertain to a person's genetic information. As you can see from Table 1, genetic nondiscrimination in employment laws is now in place in 35 jurisdictions. In addition, laws in 19 states prohibit an employer from requesting genetic information or a genetic test from an employee; laws in 26 states prohibit an employer from requiring genetic information or a genetic test from an employee; laws in 16 states prohibit an employer from performing a genetic test on an employee; laws in 11 states prohibit an employer from obtaining an employee's genetic information or genetic test result; and laws in 14 states specify penalties for genetic discrimination in employment. As examples, we include as Attachment A genetic nondiscrimination employment laws from Arkansas, Iowa, New Hampshire, Oklahoma, and Wisconsin.

---

[1] The Privacy Rights Clearinghouse, *http://www.privacyrights.org/ar/Privacy-IssuesList.htm*.

[2] NCSL's summary of state genetic privacy laws can be found at *http://www.ncsl.org/programs/health/genetics/prt.htm*. Alaska's Genetic Privacy law can be found at AS 18.13.010 through AS 18.13.100.

Table 1: State Genetic Privacy in Employment Laws	
Provisions	**State**
Genetic discrimination prohibited in hiring, firing, and/or terms, conditions or privileges of employment	Arizona, Arkansas, California, Connecticut, Delaware, District of Columbia, Hawaii, Idaho, Illinois, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Oklahoma, Oregon, Rhode Island, South Dakota, Texas, Utah, Vermont, Virginia, Washington, Wisconsin
Employer Prohibited From Requesting Genetic Information Genetic Test	Arkansas, Connecticut, Idaho, Iowa, Kansas, Louisiana, Maryland, Massachusetts, Minnesota, Nevada, New Hampshire, New York, Oklahoma, Oregon, Rhode Island, South Dakota, Utah, Virginia, Wisconsin
Employer Prohibited From Requiring Genetic Information Genetic Test	Arkansas, Connecticut, Hawaii, Idaho, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Nebraska, Nevada, New Hampshire, New York, Oklahoma, Oregon, Rhode Island, South Dakota, Texas, Utah, Vermont, Virginia, Washington, Wisconsin
Employer Prohibited From Performing Genetic Test	California, Iowa, Louisiana, Massachusetts, Michigan, Minnesota, Nevada, New Hampshire, New York, Oklahoma, Oregon, Rhode Island, South Dakota, Vermont, Virginia, Wisconsin
Employer Prohibited From Obtaining Genetic Information Genetic Test Result	Arkansas, Idaho, Kansas, Massachusetts, Michigan, Minnesota, New York, Oklahoma, Oregon, South Dakota, Utah
Specific Penalties for Genetic Discrimination in Employment	Arkansas, Idaho, Iowa, Minnesota, Missouri, New Hampshire, New Mexico, Oklahoma, Rhode Island, South Dakota, Utah, Vermont, Virginia, Wisconsin
Notes:	Current through November 2007. Arizona Revised Statutes, §41-1463; Arkansas Code Annotated, §11-5-401 to 405; California Code Annotated, Government Code §12926 and §12940; General Statutes of Connecticut, §46a-60; Delaware Code Annotated, §19-710 to 711; District of Columbia Code, §2-1401.01; Hawaii Revised Statutes, § 378-01 to 10; Idaho Code, §39-8301 to §39-8304; Illinois Compiled Statutes, §410-513/25 and §215 ILCS 5/356v; Iowa Code, §729.6; Kansas Statutes Annotated, §44-1002, §44-1009; Louisiana Statutes, §23:302, §23:303; Maine Revised Statutes, 5 §19301 and 5 §19302; Annotated Code of Maryland, Human Relations Commission §49B-15 to 16; Massachusetts General Laws, §151B; Michigan Compiled Laws, §37.1201, §37.1202; Minnesota Statutes, §181.974; Missouri Revised Statutes, §375.1300, §375.1306; Revised Statutes of Nebraska, §48-236; Nevada Revised Statutes, §613.345; New Hampshire Revised Statutes, §141-H; New Jersey Statutes, §10:5-5, §10:5-12; New Mexico Statutes, §24-21-1 to 7; New York Consolidated Laws, Executive Code §292, §296; General Statutes of North Carolina, §95-28.1A; Oklahoma Statutes, §36-3614.2; Oregon Revised Statutes, §659A.300 to 306; General Laws of Rhode Island, §28-6.7-1; South Dakota Compiled Laws, § 60-2-20; Texas Code, Labor Code 2§21-402; Utah Code, §26-45-103; Vermont Statutes, §18-9333; Code of Virginia, §40.1-28.7:1; Revised Code of Washington, §49.44.180; Wisconsin Statutes, §111.372.
Source:	National Conference of State Legislatures, *http://www.ncsl.org/programs/health/genetics/ndiscrim.htm*.

The state laws described above do not generally extend privacy protections to non-genetic based biometric identifiers such as fingerprints. We were unable to locate a comprehensive list of state laws that prohibit the collection of a person's non-genetic biometric data. In conjunction with NCSL, we searched the statutes of each state for laws that pertain, to some degree, to an individual's non-genetic biometric data and identified 33.

Most of the laws identified by our search are quite dissimilar; they range from preventing schools from collecting the biometric information of students without the written consent of the student's parent or guardian, to establishing inmate telephone systems within state prisons that can identify inmates through biometric identifiers. None of these laws, however, appear to pertain to your

issue of expressly prohibiting employers from collecting non-genetic biometric information from their employees or prospective employees.[3] We include each of these 33 laws as Attachment B; a brief summary of each of these laws is as follows.

Arizona Revised Statutes § 15-109: Prevents schools from collecting biometric information from a pupil unless the pupil's parent or guardian gives written permission.

California Codes, Civil Code § 52.7: Except as provided in law, a person shall not require, coerce, or compel any other individual to undergo the subcutaneous implanting of an identification device.

California Codes, Financial Code § 13082: Adding tactually discernible numerical keypad, such as fingerprint biometrics, to point-of-sale devices to aid visually impaired individuals.

California Codes, Penal Code § 637.3: With the exception of peace officers carrying out his or her official duties, no person or entity shall use any system which examines or records in any manner voice prints, or other voice stress patterns of another person to determine the truth or falsity of statements made by such other person without his or her express written consent given in advance of the examination.

California Codes, Penal Code § 4017.1: Except as provided in law, any person confined in a county jail, industrial farm, road camp, or city jail who is required or permitted by an order of the board of supervisors or city council to perform work, and any person while performing community service in lieu of a fine or custody or who is assigned to work furlough, may not be employed to perform any function that provides access to personal information of private individuals, including the following: addresses; telephone numbers; health insurance, taxpayer, school, or employee identification numbers; mothers' maiden names; demand deposit account, debit card, credit card, savings account, or checking account numbers, PINs, or passwords; social security numbers; places of employment; dates of birth; state or government-issued driver's license or identification numbers; alien registration numbers; government passport numbers; unique biometric data, such as fingerprints, facial scan identifiers, voice prints, retina or iris images, or other similar identifiers; unique electronic identification numbers; address or routing codes; and telecommunication identifying information or access devices.

Connecticut General Statutes § 17b-30: Requires the Commissioner of Social Services and the Commissioner of Motor Vehicles to examine available biometric identifier systems to be used by the state's temporary family assistance program and any other program determined by the Commissioner of Social Services.

---

[3] The list does not include laws that states have adopted in relation to the National Crime Prevention and Privacy Compact or laws that refer to biometrics information in specific identity theft laws. The National Crime Prevention and Privacy Compact Act is a federal law that establishes a method by which states can exchange criminal records for noncriminal justice purposes without charging each other for the information. The URL for the Federal Bureau of Investigation's National Crime Prevention and Privacy Compact Act website is *http://www.fbi.gov/hq/cjisd/web%20page/cc.htm.*

Florida Annotated Statutes § 311.125: Establishes the Uniform Port Access Credential Card, which is required of those individuals who work at Florida's seaports. This card must include at a minimum a digital full-face photograph, a digital fingerprint, a multilayered security process, a two-dimensional barcode with technology specifications that will allow the unique biometric identifiers to reside in the barcode, a unique identifying code or number, scanning capability to compare required identifiers with information on file in the central database.

Illinois Compiled Statutes 105 ILCS 5/10-20.40 and 105 ILCS 5/34-18.34: Establishes minimum policies for school districts that collect biometric information from students.

Illinois Compiled Statutes 740 ILCS 14/1 (2008), Biometric Information Privacy Act: Relates to the retention, destruction, and privacy of an individual's biometric information. Prohibits unauthorized disclosure and exempts such information from the Freedom of Information Act. Establishes that no provision be construed to conflict with the Criminal Identification Act; the Private Detective, Alarm, Security, Fingerprint Vendor, and Locksmith Act, or another similar act.

Indiana Statutes § 4-1-6-2: Limits the collection, maintenance, and use of personal information, including voice prints, by state agencies, to that which is relevant and necessary to accomplish a statutory purpose.

Indiana Statutes § 26-2-8-116: Allows electronic signature authentication and identification to be used for certain individuals, under certain circumstances.

Louisiana Revised Statutes 37:1182: Grants the Louisiana Board of Pharmacy the authority to require applicants for any pharmacological license, registration, certificate, permit, or any other designation, to provide the information necessary to verify an applicant's identity including birth certificates, passport documents, legal status documents, and any other biometric information deemed appropriate by the board.

Nebraska Revised Statutes § 87-802: Requires that individuals be notified in the event of a security breach that compromises their personal information. Personal information is defined as a name in combination with another identifying data element, including a fingerprint, voice print, or retina or iris image, or other unique physical representation.

Nevada Revised Statutes § 639.2353: Allows a prescription to be transmitted electronically without the health care practitioner's signature if it contains a facsimile signature, security code or other unique identifier; or a voice recognition system, biometric identification technique or other approved security system is used to identify the practitioner.

New Hampshire Revised Statutes 91-A:10: Prevents the state from releasing data sets that contain biometric identifiers.

New Hampshire Revised Statutes 260: 10-b: Prohibits the collection and retention of any biometric data in connection with motor vehicle registration, operation, and driver licensing. "Biometric data" includes voice data used for comparing live speech with a previously-created speech model of a person's voice.

New Jersey Statutes § 39:2A-29: Permits the New Jersey Motor Vehicle Commission to make technological improvements including the modernization of software and hardware, the addition of surveillance cameras, alarms, and access systems, and the use of biometrics.

North Carolina General Statutes § 130A-480: Prohibits the collection of biometric identifiers, including voice prints, within statute that directs the State Health Director to develop a "syndromic" surveillance program for hospital emergency departments in order to detect and investigate public health threats resulting from a terrorist incident or epidemic.

Ohio Revised Code 3701.75: Establishes standards for using electronic signatures in health care records. One standard requires that some electronic signature systems use either a two-level access control mechanism that assigns a unique identifier to each system user or a biometric access control device.

Oregon Revised Statutes § 807.024: Requires a person who applies for issuance, renewal or replacement of a driver license, driver permit or identification card to submit to collection of biometric data by the Department of Transportation for the purpose of establishing his or her identity.

Pennsylvania Statutes § 1802: Appointees, employees and prospective employees engaged in the service of the Commissions or the Board of Gaming shall submit to fingerprinting and photographing by the Pennsylvania State Police or by a local law enforcement agency.

South Carolina Code § 30-2-10: Requires that all state agencies, boards, commissions, institutions, departments, and other state entities develop privacy policies and procedures to ensure that the collection of personal information (including biometric identifiers) pertaining to the citizens of South Carolina is limited to such personal information required by any such entity to fulfill a legitimate public purpose.

Texas Statutes, Business and Commerce Code § 35.50: Provides that biometric identifiers may not be captured for commercial purposes except with prior notification and consent. Additionally provides that once captured, the biometric information may not be sold, leased, or otherwise disclosed unless the individual consents to the disclosure; the disclosure completes a financial transaction that the individual requests or authorizes; the disclosure is required or permitted by a federal or state statute; or the disclosure is made by or to a law enforcement agency for a law enforcement purpose.

Texas Statutes, Business and Commerce Code § 503.001: Defines a "biometric identifier" as a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry. This law establishes that a person may not capture a biometric identifier of an individual for commercial purposes unless the person informs the individual before capturing the biometric identifier, and receives the individual's consent to capture the biometric identifier.

Texas Statutes, Government Code § 495.025: The State requests proposals from private vendors for a contract to provide pay telephone service to eligible inmates confined in facilities operated by the department. The telephone system must have the capacity to use a biometric identifier of the inmate making the call.

Texas Statutes, Government Code § 531.1063: The Texas Health and Human Services Commission and the Texas Department of Human Services shall develop and implement a Medicaid Fraud Pilot Program. The program must include participant smart cards and biometric readers that reside at the point of contact with Medicaid providers, recipients, participating pharmacies, hospitals, and appropriate third-party participants; and a secure finger-imaging system that is compliant with the Health Insurance Portability and Accountability Act (HIPAA).

Texas Statutes, Government Code § 560.001: Provides that a government body in possession of a biometric identifier may not sell, lease, or otherwise disclose the information unless the individual consents to the disclosure; the disclosure completes a financial transaction that the individual requests or authorizes; the disclosure is required or permitted by a federal or state statute; or the disclosure is made by or to a law enforcement agency for a law enforcement purpose.

Texas Statutes, Transportation Code § 521.032: Establishes the Enhanced Driver's License or Personal Identification Certificate which requires the applicant to submit a biometric identifier as designated by the Department of Transportation.

Vermont Statutes 23 V.S.A. § 634: Prevents the Department of Motor Vehicles from implementing any procedures or processes for identifying applicants for licenses, learner permits, or non-driver identification cards that involve the use of biometric identifiers.

Virginia Code § 2.2-3801 through § 2.2-3809: Includes voice prints in the definition of personal information. Requires that state agencies collect, maintain, use, and disseminate only that personal information permitted or required by law. This law prohibits agencies from disseminating information to another system without specifying requirements for security and usage including access limitations, and receiving reasonable assurances that those requirements and limitations will be observed.

Revised Code of Washington § 46.20.037: This law requires implementation of a voluntary biometric matching system for driver's licenses and identification cards within two years of the full implementation of the Real ID Act. This law states that the biometric matching system is to be used only to verify the identity of an applicant for a renewal or duplicate driver's license or identification card by matching a biometric identifier submitted by the applicant against the biometric identifier submitted when the license was last issued.

West Virginia Code § 17B-2-12a: Vision screening conducted as part of driver's licensure shall not be used to collect any type of personal biometric identifying information.

Included in your request was a document entitled "The Alaskan Biometric Collection Act." As you may know, within this document the author notes that the University of Alaska, Fairbanks requires individuals taking the Certified Public Accountant (CPA) examination to submit to fingerprinting before and possibly during the examination. This fingerprint condition is, however, required by the American Institute of Certified Public Accountants (AICPA), the national, professional organization for all Certified Public Accountants which sets the auditing standards and the ethical standards for all CPAs; the National Association of State Boards of Accountancy (NASBA), which

serves as a forum for the boards of accountancy throughout the United States; and Prometric, which provides testing services for those seeking to take the CPA exam.[4] According to Ken Bishop, Senior Vice President for NASBA, no state prevents Prometric—or any of its subcontractors (the UAF is one of these subcontractors)—from obtaining fingerprint data from those taking the CPA exam.[5]

I hope you find this information to be useful. Please do not hesitate to contact us if you have questions or need additional information.

[4] The URL for the American Institute of Certified Public Accountants is *http://www.aicpa.org/*. The URL for the National Association of State Boards of Accountancy is *http://www.nasba.org*. The URL for Prometric is *http://www.prometric.com/*.

[5] Ken Bishop, Senior Vice President for NASBA, can be contacted at 615-312-3755. In addition, Mr. Bishop notes that Prometric doesn't capture or retain a copy of an individual's fingerprint. Prometric captures an algorithm, or a mathematical representation, based on a person's fingerprint.

March 14, 2011

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

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

FISCAL NOTE

STATE OF ALASKA
2011 LEGISLATIVE SESSION

Fiscal Note Number
Bill Version: **SB098 \A**
() Publish Date

Identifier (file name): SB098-LAW-CIV-03-12-11
Dept. Affected: Law
Title: An Act relating to biometric information.
Appropriation: Civil
Allocation: Human Services
Sponsor: SENATOR(S) WIELECHOWSKI
Requester: (S) State Affairs
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	***	***	***	***	***	***	***
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	***	***	***	***	***	***	***

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)

Not applicable, initial version.

Prepared by: Eileen Donahue, Division Operations Manager
Phone: 465-5427
Division: Administrative Services
Date/Time: 3/12/11 2:00 PM
Approved by: John J. Burns, Attorney General
Department of Law
Date: 3/12/2011

(Revised 1/27/2011 OMB)

FISCAL NOTE

STATE OF ALASKA
2011 LEGISLATIVE SESSION

BILL NO. SB 098 \A

Analysis

This bill impacts every state governmental entity that retains, analyzes, or distributes biometric information as described in the bill to ensure that the state agencies comply with the provisions of the bill. This is a new function and will require careful review of other state and federal laws to see if an exemption applies. The Department of Law will need to work with state agencies regarding consents or other authorizations for release of medical records to be sure they comply with the provisions of the bill. This bill requires a specific release of information to use biometric information, such as fingerprints, photos, etc... Also, this bill includes a private right of action if this statute is violated. With the private right of action section, it is not clear how this will affect the state in terms of defending actions brought. The state uses biometric information in a number of instances, such as occupational licensing, back ground checks, etc...

As such, the fiscal impact of this legislation cannot be accurately determined at this time.