

**SB**

**98**

<TARGET><BILL>SB 98</BILL><SUBJECT>SB  
98</SUBJECT><COMM>SJUD27</COMM></TARGET>

# ALASKA STATE LEGISLATURE

## Session

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

## Interim

716 W. 4<sup>th</sup> 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.

**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**

1 **"An Act relating to biometric information."**

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

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

4 **Chapter 14. Biometric Information.**

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

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

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

13 (1) United States passport; or

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

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 5 consent that is provided in a uniform consent form that has not been revoked, is  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

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

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

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

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

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

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

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

26           **Sec. 18.14.090. Definitions.** In this chapter,

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

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

1 vein recognition;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1  
2

(12) "vein recognition" means the use of the veins in an individual's skin 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. 4<sup>th</sup> 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 "B"

- **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. 4<sup>th</sup> 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.



## 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 threshold 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 is 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, Neosciences) that measures the pattern of the veins of the hand. Neosciences 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 *unobtrusiveness*. 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 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 company 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 "spoo" the system internally is entirely dependent on the security of the system architecture.

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

#### **The State of Scientific Testing of Biometric ID Systems**

According to Dr. Wayman,

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

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

#### **Media Coverage/Resources**

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

#### **Acknowledgements:**

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

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

## What Is Privacy in the Context of Biometrics?

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

### Working Definition of Privacy

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

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

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

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

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

Woodward, John D.; Orlans, Nicholas; Higgins, Peter T.. Biometrics. Emeryville, CA, USA: McGraw-Hill Professional Publishing, 2002. p 11g. <http://site.ebrary.com/lib/juneau/Doc?id=10153048&ppg=230>

Copyright © 2002. McGraw-Hill Professional Publishing. All rights reserved.

May not be reproduced in any form without permission from the publisher, except fair uses permitted under U.S. or applicable copyright law.

### 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),

Woodward, John D.; Orlans, Nicholas; Higgins, Peter T.. Biometrics.  
Emeryville, CA, USA: McGraw-Hill Professional Publishing, 2002. p 111.  
<http://site.ebrary.com/lib/juneau/Doc?id=10153048&ppg=232>

Copyright © 2002. McGraw-Hill Professional Publishing. All rights reserved.  
May not be reproduced in any form without permission from the publisher, except fair uses permitted under U.S. or applicable copyright law.

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.

Woodward, John D.; Orlans, Nicholas; Higgins, Peter T.. Biometrics.  
Emeryville, CA, USA: McGraw-Hill Professional Publishing, 2002. p 11j.  
<http://site.ebrary.com/lib/juneau/Doc?id=10153048&ppg=233>

Copyright © 2002. McGraw-Hill Professional Publishing. All rights reserved.  
May not be reproduced in any form without permission from the publisher, except fair uses permitted under U.S. or applicable copyright law.

**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).

Woodward, John D.; Orlans, Nicholas; Higgins, Peter T.. Biometrics.  
Emeryville, CA, USA: McGraw-Hill Professional Publishing, 2002. p 11k.  
<http://site.ebrary.com/lib/juneau/Doc?id=10153048&ppg=234>

Copyright © 2002. McGraw-Hill Professional Publishing. All rights reserved.  
May not be reproduced in any form without permission from the publisher, except fair uses permitted under U.S. or applicable copyright law.

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

Woodward, John D.; Orlans, Nicholas; Higgins, Peter T.. Biometrics.  
Emeryville, CA, USA: McGraw-Hill Professional Publishing, 2002. p 111.  
<http://site.ebrary.com/lib/juneau/Doc?id=10153048&ppg=235>

Copyright © 2002. McGraw-Hill Professional Publishing. All rights reserved.  
May not be reproduced in any form without permission from the publisher, except fair uses permitted under U.S. or applicable copyright law.

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:

Woodward, John D.; Orlans, Nicholas; Higgins, Peter T.. Biometrics.  
Emeryville, CA, USA: McGraw-Hill Professional Publishing, 2002. p 11m.  
<http://site.ebrary.com/lib/juneau/Doc?id=10153048&ppg=236>

Copyright © 2002. McGraw-Hill Professional Publishing. All rights reserved.

May not be reproduced in any form without permission from the publisher, except fair uses permitted under U.S. or applicable copyright law.

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

Woodward, John D.; Orlans, Nicholas; Higgins, Peter T.. Biometrics.  
Emeryville, CA, USA: McGraw-Hill Professional Publishing, 2002. p 11n.  
<http://site.ebrary.com/lib/juneau/Doc?id=10153048&ppg=237>

Copyright © 2002. McGraw-Hill Professional Publishing. All rights reserved.  
May not be reproduced in any form without permission from the publisher, except fair uses permitted under U.S. or applicable copyright law.

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' bands.

Woodward, John D.; Orlans, Nicholas; Higgins, Peter T.. Biometrics.  
Emeryville, CA, USA: McGraw-Hill Professional Publishing, 2002. p 11p.  
<http://site.ebrary.com/lib/juneau/Doc?id=10153048&ppg=239>

Copyright © 2002. McGraw-Hill Professional Publishing. All rights reserved.  
May not be reproduced in any form without permission from the publisher, except fair uses permitted under U.S. or applicable copyright law.

**America's Newspapers**

## **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*

*Copyright 2006, Los Angeles Times. Reproduced with the permission of Los Angeles Times - Washington Post News Service by NewsBank, inc.*

# ALASKA STATE LEGISLATURE

## Session

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

## Interim

716 W. 4<sup>th</sup> 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.<sup>1</sup>

The National Conference of State Legislatures (NCSL) collects information on actions state legislatures have taken to safeguard a persons' genetic information.<sup>2</sup> 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.

<sup>1</sup> The Privacy Rights Clearinghouse, <http://www.privacyrights.org/ar/Privacy-IssuesList.htm>.

<sup>2</sup> 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
<b>Notes:</b>	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.
<b>Source:</b>	National Conference of State Legislatures, <a href="http://www.ncsl.org/programs/health/genetics/ndiscrim.htm">http://www.ncsl.org/programs/health/genetics/ndiscrim.htm</a> .

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.<sup>3</sup> 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.

---

<sup>3</sup> 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.<sup>4</sup> 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.<sup>5</sup>

---

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

---

<sup>4</sup> 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/>.

<sup>5</sup> 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.

# Citizens for Privacy in Alaska

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

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

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



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](http://WWW.AKCLU.ORG)

**OFFICERS AND DIRECTORS**

SUSAN WINGROVE, Anchorage  
PRESIDENT

RICH CURTNER, Anchorage  
VICE PRESIDENT

LLOYD EGGAN, Anchorage  
TREASURER

TONY STRONG, Juneau  
SECRETARY

WILLIE ANDERSON, Juneau  
AFFIRMATIVE ACTION OFFICER

KIRSTEN BEY, Nome  
DONNA GOLDSMITH, Anchorage  
PAUL GRANT, Juneau  
SCOTT HENDERSON, Anchorage  
KATIE HURLEY, Wasilla  
MARJORIE KAISER, Anchorage  
MICHAEL KING, Anchorage  
KAY MARTIN, Anchorage  
CONNIE OZER, Anchorage  
GALEN PAINE, Sitka  
STEPHANIE PAWLOWSKI, Anchorage  
JUNE PINNELL-STEPHENS, Fairbanks  
NADINE WINTERS, Fairbanks

ZACH FICK, Anchorage  
STUDENT ADVISOR

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](mailto:Senator_Bill_Wielechowski@legis.state.ak.us)  
[Senator Joe Paskvan@legis.state.ak.us](mailto: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

Senate State Affairs Committee  
*ACLU Support of S.B. 98*  
March 14, 2011  
Page 2

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

**CS FOR SENATE BILL NO. 98(JUD)**

IN THE LEGISLATURE OF THE STATE OF ALASKA  
TWENTY-SEVENTH LEGISLATURE - FIRST SESSION

BY THE SENATE JUDICIARY COMMITTEE

**Offered:**  
**Referred:**

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

**A BILL**

**FOR AN ACT ENTITLED**

1 **"An Act relating to biometric information."**

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

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

4 **Chapter 14. Biometric Information.**

5 **Sec. 18.14.010. Biometric information collection.** (a) A person may not  
6 collect the biometric information of another individual unless the person first

7 (1) notifies the individual in a clear manner that the biometric  
8 information is being collected, the specific purpose for which the biometric  
9 information will be used, and how long the biometric information will be kept; and

10 (2) receives, in a written, electronic, or other form by which the  
11 consent can be documented, the individual's full consent to the collection of the  
12 biometric information, the specific purpose for which the biometric information will  
13 be used, and how long the biometric information will be kept.

14 (b) Unless the individual's biometric information was needed for a specific  
15 authorized law enforcement, security, or fraud prevention purpose, an individual may,

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

3 **Sec. 18.14.020. Disclosure of biometric information.** (a) A collector and a  
4 collector's contractor may not disclose, transfer, or distribute the biometric information  
5 of another individual, except to a contractor or to a person to authenticate the identity  
6 of the individual providing the biometric information.

7 (b) A disclosure, transfer, or distribution under (a) of this section may only be  
8 made for the original purpose for which the information was collected.

9 **Sec. 18.14.030. Sale of biometric information.** A person may not sell  
10 biometric information, except that a contractor may sell the contractor's business to  
11 another person and transfer the biometric information to the buyer.

12 **Sec. 18.14.040. Alternate identification.** If a person who administers an  
13 occupational examination requires an individual taking the examination to provide  
14 biometric information to the person for the purpose of identifying the individual taking  
15 the examination, the person may not require that the individual provide the biometric  
16 information if the individual provides the person with alternate identification  
17 acceptable to the person administering the occupational examination. In this section,  
18 "occupational examination" includes an examination required for admission to an  
19 institution of higher learning.

20 **Sec. 18.14.050. Disposal.** (a) When a collector no longer needs an individual's  
21 biometric information for the collector's original purpose, or if an individual requests  
22 in writing that the individual's biometric information be removed from all databases or  
23 other storage systems and be permanently destroyed, the collector and the collector's  
24 contractor, if any, shall, within 120 days and unless prohibited by other law, a  
25 regulation, or a court order, remove the individual's biometric information from all  
26 databases and storage systems and destroy the biometric information.

27 (b) Within 30 days after determining that the collector no longer needs an  
28 individual's biometric information for the collector's original purpose or that the  
29 individual has requested the removal and destruction, the collector shall notify the  
30 collector's contractor, if any, that the collector is to remove the individual's biometric  
31 information from all databases and storage systems and destroy the biometric

1 information.

2 **Sec. 18.14.060. Use of biometric information.** A collector may not use  
3 biometric information for marketing purposes or for general surveillance purposes, but  
4 a collector may use the biometric information for a specific authorized security or  
5 fraud prevention purpose in addition to the specific purpose for which the biometric  
6 information was collected.

7 **Sec. 18.14.070. Storage of biometric information.** A collector and a  
8 contractor shall store an individual's biometric information in a secure manner, which  
9 may include encryption or another appropriate method, to ensure that the identity of  
10 the individual who provided the biometric information is protected.

11 **Sec. 18.14.080. Right of action.** (a) Except as provided in (b) of this section,  
12 an individual may bring a civil action against a person who knowingly violates this  
13 chapter. A person who violates this chapter is liable to the individual for actual  
14 damages and a penalty of \$5,000, except that, if the violation resulted in profit or  
15 monetary gain to the person, the penalty is \$100,000. In this subsection, "knowingly"  
16 has the meaning given in AS 11.81.900.

17 (b) An action for damages, a penalty, or both may not be brought against the  
18 state, the agencies of the state, or the officers or employees of the state or the agencies  
19 of the state for violations of this chapter or for other claims arising under this chapter.

20 **Sec. 18.14.085. Exemptions.** (a) This chapter does not apply to the collection,  
21 retention, analysis, disclosure, or distribution of

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

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

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

29 (b) This chapter does not apply to the retention of voices recorded for quality  
30 assurance purposes.

31 **Sec. 18.14.090. Definitions.** In this chapter,

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

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

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

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

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

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

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

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

20 (4) "collector" means a person who collects the biometric information  
21 of another individual;

22 (5) "contractor" means a person who contracts with a collector to store  
23 the biometric information collected by the collector, and includes a person to whom  
24 the contractor sells the contractor's business and transfers the biometric information;

25 (6) "facial mapping" means the use of digital technology to measure  
26 the features of an individual's face;

27 (7) "facial recognition" means the use of facial mapping for  
28 recognition purposes;

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

31 (9) "fingerprint recognition" means the use of the physical structure of

1 an individual's fingerprint for recognition purposes;

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

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

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

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

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

13 (15) "vein recognition" means the use of the veins in an individual's  
14 skin for recognition purposes.

# ALASKA STATE LEGISLATURE

## Session

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

## Interim

716 W. 4<sup>th</sup> 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 CS, Version "B", to CS for SB 98, Version "T"

- **Sec 18.14.010:** This section now has strengthened language to further clarify consent needs to be provided for biometric information to be collected, the consent needs to be documented, and unless required for law enforcement or security purposes, the consent may be revoked at any time.
- **Sec 18.14.020:** This section now restricts the disclosure of biometric information to third parties, except to a person the collector has contracted with to the store the information. Additionally, the information may only be used for the original purpose of the collection. It no longer mandates a collector to accept an alternate ID.
- **Sec 18.14.030:** This section now says the sale of biometric information is prohibited, unless the storage entity is acquired by another storage entity. A uniform consent form to be drafted by the DHSS is no longer in the bill.
- **Sec 18.14.040:** This section now specifically says occupational examinations must allow acceptable other forms of ID to be used in lieu of biometric identification.
- **Sec 18.14.050:** This section sets time limits on how long biometric information can be stored. Biometric information will be deleted upon request of the individual or when the original reason for the collection is no longer necessary. The section allows 30 days for the collecting entity to notify the storage entity, and 120 days for the storage entity to delete the data.

- **Sec 18.14.060:** This section states that biometric information cannot be used for marketing or general surveillance purposes, but it may be used for fraud prevention.
- **Sec 18.14.070:** This section states that biometric information shall be stored in a secure manner.
- **Sec 18.14.080:** This section provides a private right of action for individuals to bring against private entities who violate this chapter. The state and its agents are exempt, but not immune to injunctions.
- **Sec 18.14.085:** This section provides exemptions for the use of biometric information without consent:
  - When used for law enforcement purposes
  - When authorized by state or federal law
  - For facial images used by the Department of Admin for drivers licenses and ID cards
  - For voice retention for quality assurance purposes
- **Sec 18.14.090:** Definitions remain unchanged

AMENDMENT #2

OFFERED IN THE SENATE

SENATOR PASKVAN

TO: CSSB 98( ), Draft Version "T"

1 Page 2, line 12:

2 Delete "If"

3 Insert "(a) Except as provided in (b) of this section, if"

4

5 Page 2, line 17, following "examination.":

6 Insert new material to read:

7 "(b) If the collection of the biometric information of an individual taking an  
8 occupational examination is legitimately necessary to establish the security of the  
9 occupational examination, the person who administers the occupational examination  
10 may collect the biometric information, but the person shall comply with the collection  
11 and other requirements of this chapter with regard to the biometric information, and  
12 the person shall require the person's contractor, if any, to agree to comply with the  
13 collection and other requirements of this chapter with regard to the biometric  
14 information.

15 (c)"

failed  
2/2

# ALASKA STATE LEGISLATURE

## Session

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

## Interim

716 W. 4<sup>th</sup> 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

### Changes in CS for SB 98 Version "E" to Version "T"

- **In Sec 18.14.040, Page 2, Lines 17-19**, a clarification has been made to ensure that exams for entrance to institutions of higher learning have been included as occupational exams.
- **In Sec 18.14.040, Page 2, Lines 17**, a clarification has been made to ensure an administer of an exam may determine what an acceptable alternate ID is.
- **In Sec 18.14.080, Page 3, Line 18**, the term "agents of the state," or what could possibly be construed as a contractor with the state, has been removed as organizations exempted from a private right of action.
- **In Sec 18.14.085, Page 3, Lines 29-30**, an exemption has been made for voice data collected for quality assurance purposes.
  - Additionally, the exemption for "facial images in a biometric system" has been removed as "facial images" have been changed to "facial mapping" under the definition of "biometric data".
- **In Sec 18.14.090, Page 3, Lines 1-2**, "facial images" have been replaced by "facial mapping" in the definitions of biometric data.
  - **Page 3, Lines 25-26**, "facial mapping" has been defined as "the use of digital technology to measure the features of an individual's face."

27-LS0661\T  
Bannister  
4/13/11

**CS FOR SENATE BILL NO. 98( )**

**IN THE LEGISLATURE OF THE STATE OF ALASKA**

**TWENTY-SEVENTH LEGISLATURE - FIRST SESSION**

**BY**

**Offered:  
Referred:**

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

**A BILL**

**FOR AN ACT ENTITLED**

1 **"An Act relating to biometric information."**

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

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

4 **Chapter 14. Biometric Information.**

5 **Sec. 18.14.010. Biometric information collection.** (a) A person may not  
6 collect the biometric information of another individual unless the person first

7 (1) notifies the individual in a clear manner that the biometric  
8 information is being collected, the specific purpose for which the biometric  
9 information will be used, and how long the biometric information will be kept; and

10 (2) receives, in a written, electronic, or other form by which the  
11 consent can be documented, the individual's full consent to the collection of the  
12 biometric information, the specific purpose for which the biometric information will  
13 be used, and how long the biometric information will be kept.

14 (b) Unless the individual's biometric information was needed for a specific  
15 authorized law enforcement, security, or fraud prevention purpose, an individual may,

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

3 **Sec. 18.14.020. Disclosure of biometric information.** (a) A collector and a  
4 collector's contractor may not disclose, transfer, or distribute the biometric information  
5 of another individual, except to a contractor or to a person to authenticate the identity  
6 of the individual providing the biometric information.

7 (b) A disclosure, transfer, or distribution under (a) of this section may only be  
8 made for the original purpose for which the information was collected.

9 **Sec. 18.14.030. Sale of biometric information.** A person may not sell  
10 biometric information, except that a contractor may sell the contractor's business to  
11 another person and transfer the biometric information to the buyer.

12 **Sec. 18.14.040. Alternate identification.** If a person who administers an  
13 occupational examination requires an individual taking the examination to provide  
14 biometric information to the person for the purpose of identifying the individual taking  
15 the examination, the person may not require that the individual provide the biometric  
16 information if the individual provides the person with alternate identification  
17 acceptable to the person administering the occupational examination. In this section,  
18 "occupational examination" includes an examination required for admission to an  
19 institution of higher learning.

20 **Sec. 18.14.050. Disposal.** (a) When a collector no longer needs an individual's  
21 biometric information for the collector's original purpose, or if an individual requests  
22 in writing that the individual's biometric information be removed from all databases or  
23 other storage systems and be permanently destroyed, the collector and the collector's  
24 contractor, if any, shall, within 120 days and unless prohibited by other law, a  
25 regulation, or a court order, remove the individual's biometric information from all  
26 databases and storage systems and destroy the biometric information.

27 (b) Within 30 days after determining that the collector no longer needs an  
28 individual's biometric information for the collector's original purpose or that the  
29 individual has requested the removal and destruction, the collector shall notify the  
30 collector's contractor, if any, that the collector is to remove the individual's biometric  
31 information from all databases and storage systems and destroy the biometric

1 information.

2 **Sec. 18.14.060. Use of biometric information.** A collector may not use  
3 biometric information for marketing purposes or for general surveillance purposes, but  
4 a collector may use the biometric information for a specific authorized security or  
5 fraud prevention purpose in addition to the specific purpose for which the biometric  
6 information was collected.

7 **Sec. 18.14.070. Storage of biometric information.** A collector and a  
8 contractor shall store an individual's biometric information in a secure manner, which  
9 may include encryption or another appropriate method, to ensure that the identity of  
10 the individual who provided the biometric information is protected.

11 **Sec. 18.14.080. Right of action.** (a) Except as provided in (b) of this section,  
12 an individual may bring a civil action against a person who knowingly violates this  
13 chapter. A person who violates this chapter is liable to the individual for actual  
14 damages and a penalty of \$5,000, except that, if the violation resulted in profit or  
15 monetary gain to the person, the penalty is \$100,000. In this subsection, "knowingly"  
16 has the meaning given in AS 11.81.900.

17 (b) An action for damages, a penalty, or both may not be brought against the  
18 state, the agencies of the state, or the officers or employees of the state or the agencies  
19 of the state for violations of this chapter or for other claims arising under this chapter.

20 **Sec. 18.14.085. Exemptions.** (a) This chapter does not apply to the collection,  
21 retention, analysis, disclosure, or distribution of

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

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

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

29 (b) This chapter does not apply to the retention of voices recorded for quality  
30 assurance purposes.

31 **Sec. 18.14.090. Definitions.** In this chapter,

- 1 (1) "biometric data" means fingerprints, handprints, voices, facial  
2 mapping, iris images, retinal images, vein scans, hand geometry, or finger geometry;
- 3 (2) "biometric information" means biometric data that is used in a  
4 biometric system for fingerprint recognition, hand geometry recognition, finger  
5 geometry recognition, voice recognition, facial recognition, iris scans, retinal scans, or  
6 vein recognition;
- 7 (3) "biometric system" means an automated system capable of
- 8 (A) capturing biometric data from an individual's biometric  
9 information;
- 10 (B) extracting and processing the biometric data captured under  
11 (A) of this paragraph;
- 12 (C) storing the biometric data extracted under (B) of this  
13 paragraph;
- 14 (D) comparing the biometric data extracted under (B) of this  
15 paragraph with biometric data stored for the individual for use in future  
16 recognition of the individual; and
- 17 (E) determining how well the extracted and stored biometric  
18 data match when compared under (D) of this paragraph, and indicating  
19 whether an identification or verification of identity has been achieved;
- 20 (4) "collector" means a person who collects the biometric information  
21 of another individual;
- 22 (5) "contractor" means a person who contracts with a collector to store  
23 the biometric information collected by the collector, and includes a person to whom  
24 the contractor sells the contractor's business and transfers the biometric information;
- 25 (6) "facial mapping" means the use of digital technology to measure  
26 the features of an individual's face;
- 27 (7) "facial recognition" means the use of facial mapping for  
28 recognition purposes;
- 29 (8) "finger geometry recognition" means the use of the shape and  
30 dimensions of one or more fingers for recognition purposes;
- 31 (9) "fingerprint recognition" means the use of the physical structure of

- 1 an individual's fingerprint for recognition purposes;
- 2 (10) "governmental entity" means a state agency, a municipality, and
- 3 an agency of a municipality; in this paragraph, "state agency" means an agency of the
- 4 executive, judicial, or legislative branch of state government;
- 5 (11) "hand geometry recognition" means the use of the physical
- 6 structure of an individual's hand for recognition purposes;
- 7 (12) "iris scan" means the use of an image of the physical structure of
- 8 an individual's iris for recognition purposes;
- 9 (13) "person" has the meaning given in AS 01.10.060, and includes a
- 10 governmental entity;
- 11 (14) "retinal scan" means the use of the pattern of blood vessels in an
- 12 individual's eye for recognition purposes;
- 13 (15) "vein recognition" means the use of the veins in an individual's
- 14 skin for recognition purposes.

# ALASKA STATE LEGISLATURE

## Session

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

## Interim

716 W. 4<sup>th</sup> 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

### **Changes from the CS for SB 98, Version “D” to the CS for SB 98, Version “E”**

**Page 2, Lines 12-16:** Section added requiring occupational exams that use biometrics as a form of ID must allow for alternate forms of ID if so desired by test takers.

**Page 3, Lines 14-17:** Subsection added that provides immunity from private rights of action towards the state and its employees.

27-LS0661\E  
Bannister  
3/31/11

**CS FOR SENATE BILL NO. 98( )**

**IN THE LEGISLATURE OF THE STATE OF ALASKA  
TWENTY-SEVENTH LEGISLATURE - FIRST SESSION**

**BY**

**Offered:  
Referred:**

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

**A BILL**

**FOR AN ACT ENTITLED**

1 **"An Act relating to biometric information."**

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

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

4 **Chapter 14. Biometric Information.**

5 **Sec. 18.14.010. Biometric information collection.** (a) A person may not  
6 collect the biometric information of another individual unless the person first

7 (1) notifies the individual in a clear manner that the biometric  
8 information is being collected, the specific purpose for which the biometric  
9 information will be used, and how long the biometric information will be kept; and

10 (2) receives, in a written, electronic, or other form by which the  
11 consent can be documented, the individual's full consent to the collection of the  
12 biometric information, the specific purpose for which the biometric information will  
13 be used, and how long the biometric information will be kept.

14 (b) Unless the individual's biometric information was needed for a specific  
15 authorized law enforcement, security, or fraud prevention purpose, an individual may,

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

3 **Sec. 18.14.020. Disclosure of biometric information.** (a) A collector and a  
4 collector's contractor may not disclose, transfer, or distribute the biometric information  
5 of another individual, except to a contractor or to a person to authenticate the identity  
6 of the individual providing the biometric information.

7 (b) A disclosure, transfer, or distribution under (a) of this section may only be  
8 made for the original purpose for which the information was collected.

9 **Sec. 18.14.030. Sale of biometric information.** A person may not sell  
10 biometric information, except that a contractor may sell the contractor's business to  
11 another person and transfer the biometric information to the buyer.

12 **Sec. 18.14.040. Alternate identification.** If a person who administers an  
13 occupational examination requires an individual taking the examination to provide  
14 biometric information to the person for the purpose of identifying the individual taking  
15 the examination, the person may not require that the individual provide the biometric  
16 information if the individual provides the person with alternate identification.

17 **Sec. 18.14.050. Disposal.** (a) When a collector no longer needs an individual's  
18 biometric information for the collector's original purpose, or if an individual requests  
19 in writing that the individual's biometric information be removed from all databases or  
20 other storage systems and be permanently destroyed, the collector and the collector's  
21 contractor, if any, shall, within 120 days and unless prohibited by other law, a  
22 regulation, or a court order, remove the individual's biometric information from all  
23 databases and storage systems and destroy the biometric information.

24 (b) Within 30 days after determining that the collector no longer needs an  
25 individual's biometric information for the collector's original purpose or that the  
26 individual has requested the removal and destruction, the collector shall notify the  
27 collector's contractor, if any, that the collector is to remove the individual's biometric  
28 information from all databases and storage systems and destroy the biometric  
29 information.

30 **Sec. 18.14.060. Use of biometric information.** A collector may not use  
31 biometric information for marketing purposes or for general surveillance purposes, but

1 a collector may use the biometric information for a specific authorized security or  
2 fraud prevention purpose in addition to the specific purpose for which the biometric  
3 information was collected.

4 **Sec. 18.14.070. Storage of biometric information.** A collector and a  
5 contractor shall store an individual's biometric information in a secure manner, which  
6 may include encryption or another appropriate method, to ensure that the identity of  
7 the individual who provided the biometric information is protected.

8 **Sec. 18.14.080. Right of action.** (a) Except as provided in (b) of this section,  
9 an individual may bring a civil action against a person who knowingly violates this  
10 chapter. A person who violates this chapter is liable to the individual for actual  
11 damages and a penalty of \$5,000, except that, if the violation resulted in profit or  
12 monetary gain to the person, the penalty is \$100,000. In this subsection, "knowingly"  
13 has the meaning given in AS 11.81.900.

14 (b) An action for damages, a penalty, or both may not be brought against the  
15 state, the agencies of the state, or the officers, employees, or agents of the state or the  
16 agencies of the state for violations of this chapter or for other claims arising under this  
17 chapter.

18 **Sec. 18.14.085. Exemptions.** This chapter does not apply to the collection,  
19 retention, analysis, disclosure, or distribution of

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

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

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

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

28 **Sec. 18.14.090. Definitions.** In this chapter,

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

31 (2) "biometric information" means biometric data that is used in a

1 biometric system for fingerprint recognition, hand geometry recognition, finger  
2 geometry recognition, voice recognition, facial recognition, iris scans, retinal scans, or  
3 vein recognition;

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

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

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

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

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

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

17 (4) "collector" means a person who collects the biometric information  
18 of another individual;

19 (5) "contractor" means a person who contracts with a collector to store  
20 the biometric information collected by the collector, and includes a person to whom  
21 the contractor sells the contractor's business and transfers the biometric information;

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

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

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

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

31 (10) "hand geometry recognition" means the use of the physical

1 structure of an individual's hand for recognition purposes;

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

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

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

8 (14) "vein recognition" means the use of the veins in an individual's  
9 skin for recognition purposes.

# ALASKA STATE LEGISLATURE

## Session

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

## Interim

716 W. 4<sup>th</sup> 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

### **Changes from the CS for SB 98, Version "D" to the CS for SB 98, Version "E"**

**Page 2, Lines 12-16:** Section added requiring occupational exams that use biometrics as a form of ID must allow for alternate forms of ID if so desired by test takers.

**Page 3, Lines 14-17:** Subsection added that provides immunity from private rights of action towards the state and its employees.

27-LS0661\D  
Bannister  
3/26/11

**CS FOR SENATE BILL NO. 98( )**  
**IN THE LEGISLATURE OF THE STATE OF ALASKA**  
**TWENTY-SEVENTH LEGISLATURE - FIRST SESSION**

**BY**

**Offered:**  
**Referred:**

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

**A BILL**  
**FOR AN ACT ENTITLED**

1 **"An Act relating to biometric information."**

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

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

4 **Chapter 14. Biometric Information.**

5 **Sec. 18.14.010. Biometric information collection.** (a) A person may not  
6 collect the biometric information of another individual unless the person first

7 (1) notifies the individual in a clear manner that the biometric  
8 information is being collected, the specific purpose for which the biometric  
9 information will be used, and how long the biometric information will be kept; and

10 (2) receives, in a written, electronic, or other form by which the  
11 consent can be documented, the individual's full consent to the collection of the  
12 biometric information, the specific purpose for which the biometric information will  
13 be used, and how long the biometric information will be kept.

14 (b) Unless the individual's biometric information was needed for a specific  
15 authorized law enforcement, security, or fraud prevention purpose, an individual may,

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

3 **Sec. 18.14.020. Disclosure of biometric information.** (a) A collector and a  
4 collector's contractor may not disclose, transfer, or distribute the biometric information  
5 of another individual, except to a contractor or to a person to authenticate the identity  
6 of the individual providing the biometric information.

7 (b) A disclosure, transfer, or distribution under (a) of this section may only be  
8 made for the original purpose for which the information was collected.

9 **Sec. 18.14.030. Sale of biometric information.** A person may not sell  
10 biometric information, except that a contractor may sell the contractor's business to  
11 another person and transfer the biometric information to the buyer.

12 **Sec. 18.14.040. Disposal.** (a) When a collector no longer needs an individual's  
13 biometric information for the collector's original purpose, or if an individual requests  
14 in writing that the individual's biometric information be removed from all databases or  
15 other storage systems and be permanently destroyed, the collector and the collector's  
16 contractor, if any, shall, within 120 days and unless prohibited by other law, a  
17 regulation, or a court order, remove the individual's biometric information from all  
18 databases and storage systems and destroy the biometric information.

19 (b) Within 30 days after determining that the collector no longer needs an  
20 individual's biometric information for the collector's original purpose or that the  
21 individual has requested the removal and destruction, the collector shall notify the  
22 collector's contractor, if any, that the collector is to remove the individual's biometric  
23 information from all databases and storage systems and destroy the biometric  
24 information.

25 **Sec. 18.14.050. Use of biometric information.** A collector may not use  
26 biometric information for marketing purposes or for general surveillance purposes, but  
27 a collector may use the biometric information for a specific authorized security or  
28 fraud prevention purpose in addition to the specific purpose for which the biometric  
29 information was collected.

30 **Sec. 18.14.060. Storage of biometric information.** A collector and a  
31 contractor shall store an individual's biometric information in a secure manner, which

1 may include encryption or another appropriate method, to ensure that the identity of  
2 the individual who provided the biometric information is protected.

3 **Sec. 18.14.070. Private right of action.** An individual may bring a civil action  
4 against a person who knowingly violates this chapter. A person who violates this  
5 chapter is liable to the individual for actual damages and a penalty of \$5,000, except  
6 that, if the violation resulted in profit or monetary gain to the person, the penalty is  
7 \$100,000. In this section, "knowingly" has the meaning given in AS 11.81.900.

8 **Sec. 18.14.080. Exemptions.** This chapter does not apply to the collection,  
9 retention, analysis, disclosure, or distribution of

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

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

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

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

18 **Sec. 18.14.090. Definitions.** In this chapter,

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

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

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

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

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

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

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

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

7 (4) "collector" means a person who collects the biometric information  
8 of another individual;

9 (5) "contractor" means a person who contracts with a collector to store  
10 the biometric information collected by the collector, and includes a person to whom  
11 the contractor sells the contractor's business and transfers the biometric information;

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

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

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

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

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

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

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

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

29 (14) "vein recognition" means the use of the veins in an individual's  
30 skin for recognition purposes.

# ALASKA STATE LEGISLATURE

## Session

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

## Interim

716 W. 4<sup>th</sup> 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 CS, Version "B", to Work Draft, Version "D"

- **Sec 18.14.010:** This section now requires a person collecting biometric information to specify a specific purpose when acquiring documented consent to collect the information.
- **Sec 18.14.020:** This section now restricts the disclosure of biometric information to third parties, except to a person the collector has contracted with to the store the information. Additionally, the information may only be used for the original purpose of the collection.
- **Sec 18.14.030:** The sale of biometric information is prohibited, unless the storage entity is acquired by another storage entity.
- **Sec 18.14.040:** This section sets time limits on how long biometric information can be stored. Biometric information will be deleted upon request of the individual or when the original reason for the collection is no longer necessary. The section allows 30 days for the collecting entity to notify the storage entity, and 120 days for the storage entity to delete the data.
- **Sec 18.14.050:** Biometric information cannot be used for marketing or general surveillance purposes, but it may be used for fraud prevention.
- **Sec 18.14.060:** Biometric information shall be stored in a secure manner.
- **Sec 18.14.070:** The word "knowingly" has been added to page 3, line 4, to ensure the party at fault is the one responsible.
- **Sec 18.14.080:** Exemptions remain unchanged

- **Sec 18.14.090:** Definitions remain unchanged

### **Key Omissions**

- **Alternate identification** in lieu of biometric identifier statute removed in **Sec 18.14.020**
- **Uniform Consent Form** removed, allowing separate organizations to draft different consent forms in **Sec 18.14.030**

## Cindy Smith

---

**From:** Tim Pearson [tim.pearson@gci.net]  
**Sent:** Monday, March 28, 2011 11:18 AM  
**To:** Sen. Hollis French  
**Cc:** Kristen Peterson; Cindy Smith; Lila Hobbs; Andy Moderow  
**Subject:** SB 98 "An Act relating to biometric information" -- please pass out of Sen. Judiciary Committee today -- a request from a resident of Senate District M

Senator French,

As a resident of Senate District M, I ask that you pass SB 98 -- "an act relating to biometric information" out of Senate Judiciary today.

I realize that the Judiciary committee meets today at 1:30 pm.

Alaskans deeply value their privacy and this bill has broad bipartisan support.

SB 98 does not affect law enforcement and the only opponents are the data mining companies who profit from collecting the personal information of Alaskans.

Collecting biometric data is also a poor security practice. Once collected (even if by an employer for security purposes), and stolen, biometric data can not be replaced -- a person cannot get a new set of fingerprints. They will have live for the rest of their lives with the issues of a compromised identity -- always questioned, always in fear of how it might be misused.

Security experts recommend other techniques, like multifactor authentication, to establish database, computer, and building security.

(Multifactor authentication is an electronic token carried by a user that repeatedly generates a time-based number that must be appended to a password when a person logs in.)

Please pass SB 98 today so that it can come to a floor vote.

Thank you for your efforts to protect Alaskan's privacy as quickly as possible.

All the best,

Tim

Tim Pearson  
3941 Starburst Circle  
Anchorage, AK 99517  
(907) 952-3948 c  
[tim.pearson@gci.net](mailto:tim.pearson@gci.net)



March 21, 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](http://WWW.AKCLU.ORG)

OFFICERS AND DIRECTORS  
SUSAN WINGROVE, Anchorage  
PRESIDENT

RICH CURTNER, Anchorage  
VICE PRESIDENT

LLOYD EGGAN, Anchorage  
TREASURER

TONY STRONG, Juneau  
SECRETARY

WILLIE ANDERSON, Juneau  
AFFIRMATIVE ACTION OFFICER

KIRSTEN BEY, Nome  
DONNA GOLDSMITH, Anchorage  
PAUL GRANT, Juneau  
SCOTT HENDERSON, Anchorage  
KATIE HURLEY, Wasilla  
MARJORIE KAISER, Anchorage  
MICHAEL KING, Anchorage  
KAY MARTIN, Anchorage  
CONNIE OZER, Anchorage  
GALEN PAINE, Sitka  
STEPHANIE PAWLOWSKI, Anchorage  
JUNE PINNELL-STEPHENS, Fairbanks  
NADINE WINTERS, Fairbanks

ZACH FICK, Anchorage  
STUDENT ADVISOR

The Honorable Hollis French, Chair  
The Honorable Bill Wielechowski, Vice-Chair  
Senate Judiciary Committee  
Alaska State Senate  
Juneau, AK 99801-1182  
via email: [Senator Hollis French@legis.state.ak.us](mailto:Senator_Hollis_French@legis.state.ak.us)  
[Senator Bill Wielechowski@legis.state.ak.us](mailto:Senator_Bill_Wielechowski@legis.state.ak.us)

Re: **CS Senate Bill 98 (STA)**  
**ACLU Statement of Support**

Chair French, Vice-Chair Wielechowski:

Thank you for the opportunity to submit a written statement of support for the Senate State Affairs Committee Substitute for Senate Bill 98.

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

From a constitutional rights and privacy perspective, **the ACLU of Alaska endorses protections for individuals' personal biometric information, and 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. CS for SB 98 (STA) 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 the Committee Substitute for SB 98 is intended to protect against coerced “consent.”

**For the above reasons, the ACLU is pleased to support SB 98, and thanks Senator Wielechowski for sponsoring this legislation to protect privacy rights.**

Please feel free to contact the undersigned should you require any additional information. We are happy to reply to any questions which Members of the Committee may have. Thank you again for the opportunity to share our support of this bill.

Sincerely,



Jeffrey Mittman  
Executive Director  
ACLU of Alaska

cc: Senator Joe Paskvan, [Senator\\_Joe\\_Paskvan@legis.state.ak.us](mailto:Senator_Joe_Paskvan@legis.state.ak.us)  
Senator Lesil McGuire, [Senator\\_Lesil\\_McGuire@legis.state.ak.us](mailto:Senator_Lesil_McGuire@legis.state.ak.us)  
Senator John Coghill, [Senator\\_John\\_Coghill@legis.state.ak.us](mailto:Senator_John_Coghill@legis.state.ak.us)

## Cindy Smith

---

**From:** Sheela Tallman [Sheela.Tallman@PREMERA.com]  
**Sent:** Monday, April 11, 2011 7:21 PM  
**To:** Cindy Smith  
**Subject:** RE: SB98

**Follow Up Flag:** Follow up  
**Flag Status:** Flagged

That would be great, thank you.

---

**From:** Cindy Smith [[mailto:Cindy\\_Smith@legis.state.ak.us](mailto:Cindy_Smith@legis.state.ak.us)]  
**Sent:** Monday, April 11, 2011 4:34 PM  
**To:** Sheela Tallman  
**Subject:** RE: SB98

I did! I am providing a copy to the bill's sponsor, Sen. Wielechowski. I know that his office is working on that bill and we do not have another hearing on it scheduled at this time, but I can let you know if it is scheduled in the next few days (our session ends on Sunday).

Cindy Smith  
Office of Senator Hollis French  
(907) 465-3892  
[www.senate.org](http://www.senate.org)

---

**From:** Sheela Tallman [<mailto:Sheela.Tallman@PREMERA.com>]  
**Sent:** Monday, April 11, 2011 1:50 PM  
**To:** Cindy Smith  
**Subject:** RE: SB98

Hello, I wanted to reach out and make sure you received a copy of our letter and see if you had any questions. I am happy to talk with you about the bill at your convenience.

Thanks,  
Sheela

Sent from my Windows Mobile® phone.

---

**From:** Cindy Smith <[Cindy\\_Smith@legis.state.ak.us](mailto:Cindy_Smith@legis.state.ak.us)>  
**Sent:** Monday, April 11, 2011 1:36 PM  
**To:** Sheela Tallman <[Sheela.Tallman@PREMERA.com](mailto:Sheela.Tallman@PREMERA.com)>  
**Subject:** SB98

Hi,

I am away from my desk a lot in this last week of the session so I thought I'd see if you can let me know by email what your questions/concerns with SB98 are –

Cindy Smith  
Office of Senator Hollis French  
(907) 465-3892  
[www.senate.org](http://www.senate.org)

April 4<sup>st</sup>, 2011

Dear Senator:

My name is Herbert Eckmann, a voter from Anchorage and very concerned citizen of this great State.

I URGE YOU to stand up for ALL Alaskans privacy. Pass a strong Biometric Privacy law this session that includes an opt-out for ALL ALASKANS who show a driver's license or passport as ID. I agree with Citizens for Privacy in Alaska; we need a privacy law that:

"makes 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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,

**Herbert Eckmann**

A concerned Alaskan Voter

[Kmal2@gci.net](mailto:Kmal2@gci.net)

April 2<sup>st</sup>, 2011

Dear Senator:

**My name is Eileen Becker, Chairman of the Alaska Republican Party Region 7, and my personal view is that you should STRONGLY support biometric privacy legislation that protects ALL Alaskans from being fingerprinted for ID purposes.**

I support Citizens for Privacy in Alaska in their goal below:

**"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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.**

Sincerely,

**Eileen Becker**

Chairman, Alaska Republican Party, Region 7  
Homer, AK  
[district35republican@webtv.net](mailto:district35republican@webtv.net)

April 3<sup>st</sup>, 2011

Dear Senator:

My name is Joe Dirksen, a voter, a long-time Alaskan, a member of the Alaska National Guard and, like most Alaskans, I am a strong supporter of privacy rights. My personal view is that **you should strongly support the new biometric privacy bill...** if it says that no fingerprinting of innocent Alaskans for ID should be required, as noted below:

"**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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Will you stand up for our privacy rights?

Sincerely,

**Joe Dirksen**

Anchorage voter

South Anchorage, 99507

[jldirksen@acsalaska.net](mailto:jldirksen@acsalaska.net)

April 3<sup>rd</sup>, 2011

Dear Senator:

Please support REAL biometric privacy legislation that would 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.

Thank you,

Elizabeth Merrill  
A Concerned Alaskan VOTER  
[Elizabeth\\_merrill@hotmail.com](mailto:Elizabeth_merrill@hotmail.com)

(I have updated my comments on this bill)

April 4<sup>st</sup>, 2011

Dear Senator:

**My name is Eileen Becker, from Homer.** I support SB 98 (THE BIOMETRIC PRIVACY BILL) because too many of our rights to privacy are being sold to the highest bidder.

**It is time to say NO and protect ourselves and our families. PROTECT ALL ALASKANS.**

Thank you,

Eileen Becker

Owner of Peninsula Communications, Inc, privately owned radio stations here in Alaska

Mother of 5 children and 8 grandchildren

Alaska resident since 1973

DISTRICT35REPUBLICAN@WEBTV.NET

ALASKAN VOTER, REPUBLICAN PARTY

**"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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

April 2<sup>st</sup>, 2011

Dear Senator:

I'm an Anchorage voter and resident named Cindy Baldwin, and I am writing to you to urge you to stand up for ALASKAN'S privacy.

As for my personal view, I **support** the new biometric privacy bill and I **STRONGLY** support Citizens for Privacy in Alaska's position that no fingerprinting of innocent Alaskans for ID should be required. Please don't water this one down; we all need this protection.

Sincerely,

*Cindy*

Cindy Baldwin

Anchorage voter

[cindyb.alaska@gmail.com](mailto:cindyb.alaska@gmail.com)

April 2<sup>st</sup>, 2011

Dear Senator:

As a dedicated member of Alaska's Republican Party, I would like to ask you to support the Wielechowski/Coghill "biometric privacy bill" (and its House companion bill) so long as it protects ALL Alaskan's from being forced into being fingerprinted for ID purposes.

"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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,

**Jerad McClure**

Member, Alaska Republican Party

[jaredlainak@gmail.com](mailto:jaredlainak@gmail.com)

April 2<sup>st</sup>, 2011

Dear Senator:

We vote...the data-miner's lobbyists don't. Please stand up for ALASKANS and our privacy, and **support** the new biometric privacy bill... if it says that no fingerprinting of innocent Alaskans for ID should be required.

My name is Laura Dirksen, a school teacher and resident of south Anchorage. Having taught for nearly 20 years at an Anchorage Christian school – I AGREE that our privacy laws need to be updated to *prevent* fingerprint collection “as ID.”

I urge your support for protecting the biometric privacy of Alaskans. Passports and driver's licenses are sufficient identification.

"**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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,

*Laura Dirksen*

Laura Dirksen  
Christian school teacher, and a voter  
Anchorage  
[jldirksen@acsalaska.net](mailto:jldirksen@acsalaska.net)

04/01/2011

Dear Senator:

My name is Dr. Frank Jeffries, Assistant Professor of Business and Public Policy at UAA.

I recently learned of a grass-roots group of Alaskan voters called the "Citizens for Privacy in Alaska" and of their courageous support for a MUCH NEEDED privacy bill. Although this is my personal view, I urge you to support it.

**I strongly support a biometric privacy bill that:**

"makes 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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,  
Dr. Frank Jeffries  
Assistant Professor of Business and Public Policy  
University of Alaska, Anchorage  
[taikodad@gci.net](mailto:taikodad@gci.net)

04/01/2011

Dear Senator:

**As Director of the Maserculiq Village Corporation in Marshall, Alaska** – I can tell you that I am a very strong supporter of privacy. I hope you will show us that you are as well, but supporting the Biometric Privacy Bill when it comes before you.

**I support real protection that:**

"makes 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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,  
George Owletuck  
Director, Maserculiq Village Corporation  
Marshall, Alaska  
[George.owletuck@gmail.com](mailto:George.owletuck@gmail.com)

PS This is my personal position

March 31, 2011

Dear Senator:

My name is Eunice Trask – a long time resident (and voter) from Anchorage. I'm a member of Citizens for Privacy in Alaska, and I've heard you are standing up for Alaskans privacy against Outside dataminer-lobbyists. GOOD FOR YOU! I SUPPORT THE BIOMETRIC PRIVACY BILL and I hope you will too.

**"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."

Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates

**We Alaskans should lead the country in standing up for privacy and in a return to dignity of the individual.** Please stand up for our privacy – innocent people shouldn't be compelled to give fingerprints as ID! Isn't the right to privacy guaranteed in our State Constitution?

Sincerely,

Eunice Trask

**Registered Voter...and I will**  
Anchorage

Dear Senator:

My name is JP Godfrey, a Management Consultant in private practice in Anchorage.

I have to say, what Citizens for Privacy in Alaska is doing is astonishing – and I strongly support them and **I strongly support this privacy bill!** Don't let the lobbyists water it down, we need REAL protection.

**"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."

Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates

Sincerely,  
JP Godfrey  
CEO, Management Consultant  
Anchorage, AK  
[jpgod@aci.net](mailto:jpgod@aci.net)

PS. I vote

March 31, 2011

Dear Senator:

My name is Mark V. Johnson, Business Development Manager for GCI Industrial Telecom in Anchorage. Today I became aware of what the Citizens for Privacy in Alaska group is doing – and I SUPPORT THEM IN STANDING UP FOR ALASKAN'S PRIVACY. I hope you will too.

**"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."**  
*Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates*

Sincerely,

*Mark*

Mark V. Johnson  
Business Development Manager,  
GCI Industrial Telecom  
Anchorage, AK  
[mjohnson@gci.com](mailto:mjohnson@gci.com)

March 31, 2011

Dear Senator:

As owner and President of Pacific Rim Media – I can tell you that I am a strong supporter of the Citizens for Privacy in Alaska. They are standing up for our privacy and I hope you will too.

**"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."

Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates

Sincerely,

*Russel*

Russell Pounds  
President, Pacific Rim Media  
Anchorage, AK  
[Russell@prmalaska.com](mailto:Russell@prmalaska.com)  
[www.prgalaska.com](http://www.prgalaska.com)

March 31, 2011

Dear Senator:

My name is Anna von Reitz, a technology analyst, author and President of the Gas for Alaskan's Association – and I support what Citizens for Privacy in Alaska is doing.

Please stand with them on this, this issue cuts across all party lines.

**"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."**  
Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates

Sincerely,  
Anna von Reitz  
President, Gas for Alaskan  
Big Lake, AK  
[avannavon@gmail.com](mailto:avannavon@gmail.com)

March 31, 2011

Dear Senator:

I'm writing to ask to you support the STRONGEST version of SB 98 **which would prevent anyone from ever collecting** or disseminating biometric data. As an Alaskan I value my privacy greatly as well as that of my clients.

The gradual degradation of our privacy over the last few years is deeply troubling to me – it is now impossible to know who has our data and what they are doing with it. But, at least one has protections using credit cards and the like – you may get dinged but you are covered. And if your email gets targeted by the advertisers, drug purveyors and sexual enhancement folks (and yes, my mother gets those too) you have recourse.

On the other hand, if our biometric information gets loose into cyberspace all hell can break loose if your prints, or mine, get used by an unscrupulous person, much less a terrorist.

**Now is the time to draw the line, hard and fast. This is no time to become spineless and give into lobbyists who have many assurances of safety, but no guarantees and no accountability when this data gets loose – and you all know that it will.**

**Please a support meaningful, strong SB 98. The “Alternative ID” section must stay.**

Thanks. Ken.

---

Kenneth G. Robertson  
Robertson Law Office  
310 K Street, Suite 200  
Anchorage, Alaska 99501  
(907) 278-5657  
(907) 346-2810 Fax  
[www.robertsonlaw.net](http://www.robertsonlaw.net)

April 1<sup>st</sup>, 2011

Dear Senator:

My name is Tim Pearson, an Anchorage business professional and Co-Chairman of the Citizens for Privacy in Alaska. I urge your support for protecting the biometric privacy of Alaskans.

Please remember that unlike credit cards, stolen or lost fingerprints and biometric information cannot be replaced. Innocent Alaskans *deserve the option* of not being forced to provide their fingerprints. Passports and driver's licenses are sufficient identification.

Alaskan businesses do not want to take on the **legal liability** of losing the irreplaceable data of their employees or customers. There is no way to make people whole again.

"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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

**PLEASE stand up for our privacy -- and pass a strong Biometric Privacy law this session that includes the "Alternative ID" provision (ie. allows an opt-out for people who show a driver's license or passport as ID).**

Sincerely,

**Tim Pearson**

President, Pearson Consulting  
Graduate of Harvard University  
Fmr Vice President of Human Resources, GCI  
[tim@timpearson.net](mailto:tim@timpearson.net)  
952-3498

April 1<sup>st</sup>, 2011

Dear Senator:

As an attorney and Principal at my firm, Woelber and Jacobson, LLC, I can tell you that I am a STRONG SUPPORTER OF PRIVACY. I learned about Citizens for Privacy in Alaska today, and I urge your support for a biometric privacy bill...but only one that offers the safeguards below:

**"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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,

**Tonja Woelber**

Attorney, Principal at  
Woelber & Jacobson, LLC  
Anchorage, AK  
[twoelber@alaska.net](mailto:twoelber@alaska.net)

04/01/2011

Dear Senator:

My name is James MacKenzie, Director of the Food Bank of Alaska. I learned that you were planning to stand up for our privacy rights through a friend today, and I STRONGLY urge your support of the new Biometric Privacy Rights bill – so long as it contains REAL protection as noted below.

"**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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,

**James MacKenzie**  
Director, Food Bank of Alaska  
Anchorage, AK  
[mackenzie.jamesa@gmail.com](mailto:mackenzie.jamesa@gmail.com)

PS note that this is my personal position on this subject

Dear Senator:

I am a past President of Alaska Chapter of the Institute of Management Accountants (IMA) and have been employed in mostly accounting and/or financial positions over my work life.

From the financial side, the people who typically steal large amounts of money from businesses or non-profits are well thought of or even "Pillars of the Community" --- before the disgracing headline hits. Collecting biometric data will do nothing to reduce the amount of criminal activity within financial circles.

**A passport or a driver's license is adequate identification for test taking purposes. AS A MEMBER OF THE ANCHORAGE BUSINESS COMMUNITY – I URGE YOU TO SUPPORT THE NEW BIOMETRIC PRIVACY BILL.**

I am also a member of Citizens for Privacy in Alaska, and we are all watching this bill closely. "**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."

Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates

Thank you for your consideration.

Sincerely  
Tim A. Wiepking  
Anchorage, 99508  
529-0766

March 31, 2011

Dear Alaska Legislators:

My name is Taylor Ridgeway. I am a strong supporter of Citizens for Privacy in Alaska, and I URGE you to stand up for Alaska's privacy rights against the data-miner's lobby! All of these oppressive encroachments are whittling away at the average Americans ability to engage in free commerce. These practices are unconstitutional...this has got to stop!

**"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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates

Sincerely

Taylor Ridgeway

Taylor.ridgeway@gmail.com

March 31, 2011

Dear Alaska Legislators:

My name is Kelly Mazzei, a voter from Anchorage. **You must stand up to these Outside data-miner lobbyists and support our privacy rights!** I am also a member of 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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates**

Sincerely

*Kelly Mazzei*

A REGISTERED VOTER

Anchorage

kamazzei@gmail.com

Dear Senators and Representatives:

My name Barbara Brown, resident of Anchorage, and I urge your support for protecting the biometric privacy of Alaskans. I am also a member of 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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates

Will you stand up for Alaskans and support this bill?

Barbara Brown  
4071 MacInnes St.  
Anchorage, AK 99508  
[cloudy@acsalaska.net](mailto:cloudy@acsalaska.net)

March 30, 2011

Dear Senator / Representative:

As an Alaskan voter, small business owner and accountant, I **urge you to support and pass biometric privacy legislation *this session***.

I am also a member of Citizens for Privacy in Alaska, and we are all watching this bill closely.

**"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."

Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates

Karen Demichelis, Principal  
Demichelis & Associates  
karen.demichelis@gmail.com  
tel: 907-360-2661

Dear Senator:

March 30, 2011

As the owner and President of a small business, I **have no need for fingerprint “biometric” security systems and I never will.**

The ABSOLUTE LAST thing I would want would be to be legally liable for a data breach involving my employee’s fingerprints! *Their privacy would be compromised for the rest of their lives* because fingerprints are like passwords that you can never change. I would be responsible for that...I can only imagine the lawsuits! **Alaskan businesses are NOT interested the risky proposition of fingerprint security systems.**

I strongly support the bi-partisan bill to protect our private biometric data (SB 98), and URGE you to pass it into law *this session* with the “Alternative ID” section intact.

We Alaskans have entrusted YOU to stand up for our privacy rights against Federal intrusion and corporate special interests...and we are all watching this bill closely.

Global data-miner ChoicePoint/LexisNexis/Reed Elsevier, has NO legitimate voice in this process, please don’t even grant them a meeting. They have flown a team of east coast lobbyists to Juneau to “influence” you -- and will attempt to scare you with a bunch of nonsense because **they profit by exploiting Alaskan’s loss of privacy.**

If they weren’t making money off collecting and trafficking our private information, why would they be here?

Who will you stand with?

Regards,  
Jason Giaimo  
Anchorage Real Estate Investor, Accountant, Small business owner  
(907) 602-9250  
[Giaimo1@aol.com](mailto:Giaimo1@aol.com)

Dear Senator:

My name is Allan R. Johnston, Vice President of Wedbush Morgan Securities. I am a member of Citizens for Privacy in Alaska....and I urge you to **support this biometric privacy bill!**

"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."

Allan R Johnston

Vice President and Regional Manager

Wedbush Morgan Securities

101 West Benson Blvd, Ste 500

Anchorage, AK 99503

[allanrjohnston@gmail.com](mailto:allanrjohnston@gmail.com)

Dear Senator:

My name is Tyler Arnold, Founder and CEO of **TylerSystems, Inc.** a rapidly growing global technology firm based in Anchorage. I urge your support for protecting the biometric privacy of Alaskans. I am also a member of Citizens for Privacy in Alaska, and we are watching this bill closely.

**"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."

Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates

PLEASE stand up for our privacy -- and support this bill.

Tyler Arnold  
CEO, TylerSystems, Inc.  
227-9541  
[tyler@tylersystems.com](mailto:tyler@tylersystems.com)

March 30, 2011

Dear Senator:

As a small business owner, I write this email to you with great concern over the future of freedom in this country. Alaska has always been at the heart of cherishing individual freedom. Right now there are very wealthy forces from outside this country that are plotting to take away "our" freedom of privacy.

If you have an ounce of respect for our forefathers who died to provide us with some small degree of human dignity, I implore you to join in the battle to defend these rights. To put it bluntly, tells these foreign data-mining companies (Lexis Nexis/Reed Elsevier) to go to hell!

I am not sure if you feel it like I do, but there is revolution in the air throughout the world. You need to make a choice and decide if you are going to sell out your family's freedoms and privacy to the corporate interests, or take a stand and let freedom ring. I hope you will make the right choice.

Sincerely,

*Andrew*

Andrew Wilkins

Small business owner  
aawilkens@yahoo.com

March 30, 2011

Senator:

Please support REAL biometric privacy legislation that would 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 (the "Alternative Identification" provision).

Please do not let Choice Point (LexisNexis/ReedElsevier) or any other company or corporation gut this bill. Please protect Alaskans from privacy intrusions by passing Senate Bill 98 in the format of the original intent as requested by Citizens for Privacy in Alaska – with the "Alternative ID" section in-tact.

Thank you.

*Daniel*

Daniel Boland

**Registered Alaskan Voter**

8231 Kip Court

Anchorage AK 99507

[Mt1dan@gci.net](mailto:Mt1dan@gci.net)

March 29<sup>th</sup> 2011

Dear Senator Hollis French:

We are a group of Alaskan voters who strongly support the need for stronger privacy legislation. **Specifically, we are *Citizens for Privacy in Alaska*, and we urge you to support and pass the new Alaskan Biometric Privacy Legislation SB-98 this session.**

All Alaskans cherish their privacy - it's even guaranteed by our State Constitution. As with opposing REAL ID, we Alaskans look to YOU, our representatives to stand up for our privacy rights against the Federal Government and corporate intrusion.

This privacy bill is supported by nearly everyone - from Libertarians to liberal Democrats, from conservative Republicans to the ACLU; from school teachers to military families, to CEOs, IT experts and oil company managers. Not surprisingly, only the lobbyists for the global data-mining firms seem to object (ChoicePoint/LexisNexis) because *this bill threatens their ability to profit from the exploitation of Alaskan's loss of privacy.*

SB-98 says essentially that biometrics (fingerprints etc) should not be required as identification when a valid driver's license or US passport is presented (this bill would not affect fingerprints taken for background checks and it would not affect law enforcement in any way).

As you may know, NY Senator Chuck Schumer and SC Senator Lindsey Graham have proposed as "the cornerstone" of their immigration Reform a Federal Government plan to FINGERPRINT ALL AMERICANS under a new biometric National (work) ID Card program. A city in Arizona is right now considering mandating all customers of the local pharmacy be fingerprinted in order to pick up their prescriptions...those who object will be *denied their medicine*. With this rapidly deteriorating national privacy climate, Alaskans urgently need strong biometric privacy legislation now.

As you know, there are *very few issues* on which Alaskans from across the political spectrum agree. *The urgent need to protect our privacy* from constant and increasing Federal Government and corporate intrusion is one of them. Please do all you can to support the Biometric Privacy bill and pass it into law this session.

*Signed,*

*Citizens for Privacy in Alaska*

Co-chair: Tim Pearson – business owner

Co-chair: Jason Giaimo, business owner

Gretchen Guess: Alaskan voter, former Senator

Horst Poepperl: CEO and IT data privacy expert, Borealis Broadband Corporation

**Mark Lerner:** President, Stop REAL ID National Coalition

**Jason Dowell:** Libertarian Party Alaska, member

**Cindy Miller:** Former CFO of Unocal Alaska

**Joe Dirksen:** Resident, Alaska, Alaskan Voter, military family

**Eunice Trask:** Alaskan voter

**Laura Dirksen:** 20 year teacher at an Anchorage Christian School. Alaskan Voter

**Barbara Brown:** Alaskan Voter

**Dan Boland:** State of Alaska, Audit Division, Alaskan Voter

**Arzu Smith:** CPA candidate

**Tom Gill:** UAA, formerly with BP, Alaskan Voter

**Tim Wiepking:** Institute of Management Accountants, former President, Alaskan Voter

**George Ascott:** Alaska resident, Alaskan Voter

**Ralph Taylor:** Taylor Consultants, President

**Allan Johnston:** Wedbush Morgan Securities, Alaskan Voter

**Angela Gill:** Alaskan Voter, medical professional

**Andrew Blackman, CPA:** Partner with Shapiro Lobel LLP

**Karen Demichelis:** President, Accountant, Demichelis & Associates, Alaskan Voter

Tyler Arnold: TylerSystems Inc. CEO, Alaskan Voter

Joel Smith: Former President of the Institute of Management Accountants, SF chapter

Tim Pearson: Pearson Consulting, Alaskan Voter

Jason Giaimo: Net Gain Business Consultants of Alaska, Alaskan Voter

Jack-Taylor Ridgeway: Privacy Rights supporter, advocate

Patrick Lorenz: Management, Analyst, British Petroleum, Alaskan Voter

Dianne Kelly: CPA, State of New Jersey

Chuck Kaucic: Alaskan voter, Wasilla

Chris Brownwell: Resident, Alaska, noted author, Alaskan Voter, military family

Hetal Giaimo: Alaskan Voter

Dawn Brownwell: Alaska Voter, military family

Kelly Mazzei: Alaskan Voter

Andrew Wilkins: IT expert at a large national bank.

Bruce Sollenberger: Alaskan Voters

Wendi Sollenberger: Alaskan Voters

Jeffrey Mittman: Executive Director, ACLU - Alaska

*...this is only a partial list of voters and supporters who are watching this bill*

ALASKA SENATE and ALASKA HOUSE SUPPORT INCLUDES:

**Bill sponsor: Senator Bill Wielechowski**

**Co-sponsor: Senator Coghill**

**Co-sponsor : Senator Kevin Meyer**

**Co-sponsor: Senator Johnny Ellis**

**Will be a bill sponsor or co-sponsor: Representative Berta Gardner**

**Co-sponsor: Representative Allan Dick**

**Co-sponsor: Representative Wes Keller**

**Does not oppose: Whitney Brewster Alaska State Director, Division of Motor Vehicles**

**Does not oppose: Alaska Department of Health and Social Services**

**Reviewed SB190 (previous version of SB-98): previous Alaska Attorney General**

**Supported SB190 (previous version of SB-98) in committee: Senator Kookesh**

**Supported SB190 (previous version of SB-98) in committee: Senator Egan**

**Supported SB190 (previous version of SB-98) in committee: Senator French**

**Supported SB190 (previous version of SB-98) in committee: Senator McGuire**

**Supported SB190 (previous version of SB-98) in committee: Senator Paskvan**

**Co-sponsoring SB-98: Senator Cathy Giessel**

Co-sponsoring SB-98: Senator Linda Menard

Will co-sponsor: Representative Tammie Wilson

Will co-sponsor: Representative Chris Tuck

Will co-sponsor: Representative Sharon Cissna

Will co-sponsor "very probably" Representative Mark Neuman



April 4, 2011

The Honorable Hollis French  
Chairman  
Senate Judiciary Committee  
Alaska State Senate

Re: Alaska SB 0098A

Dear Chairman French:

I am writing to present information regarding the use of biometrics as a test security measure. Attached to this letter is a fact sheet which provides relevant data regarding biometrics as implemented by Prometric on behalf of its testing clients.

Prometric is the largest provider of integrated testing services in the world. Prometric's test administration services include the development of test content, the administration of tests via test center based services, internet based testing services, and paper based testing services and test result and data management services. Prometric administers over 9 million tests per year.

As the leading global provider of test services, Prometric, in concert with its clients, is responsible for the security and integrity of testing services. This includes protecting the content of the examinations which we administer and to make certain that testing and evaluation of candidates is valid and fair.

#### Why Biometrics

There are numerous methods by which individuals can threaten the integrity of the testing process. One such method involves the impersonation of a test taker or candidate by another individual. There are at least three reasons why such impersonation or proxy testing occurs. The first is the simple substitution of one person for a real candidate for the purpose of providing that candidate an advantage. This is usually distinguished by two individuals conspiring without necessarily a profit motive as in a friend or relative substitutes to obtain a higher score.

The second reason for proxy testing is a variant of the first, however, in this case the motivation is a professional test taker who takes tests for any individual willing to pay the price.

The third reason for proxy testing is by a professional test taker for the purpose of stealing test content. The content is then used to provide gray market study materials or to provide real content for the purpose of memorization.

In each case the public is harmed because candidates without valid criteria are permitted to practice a profession, exercise a certification, enter an institution of higher education, or display a credential that they are not entitled to and did not earn.

1501 South Clinton Street  
Baltimore, Maryland 21224  
USA

443 455 8000 PHONE  
866 PROMETRIC TOLL FREE  
866 776 6387 TOLL FREE

[www.prometric.com](http://www.prometric.com)



### Examples

Prometric tracks many security statistics across a wide variety of misconduct. For a nine month period in 2010 ending in September, Prometric undertook 329 proxy testing investigations.

There have been significant and high profile proxy testing cases over the last several years involving Prometric and its clients in which proxy testing was an issue. In each case cited below, the incidents are documented, however, Prometric's internal privacy protection policies prohibit identifying the individuals or the programs.

a. The first example, which was one of the factors involved in Prometric looking at implementing a biometric solution world wide, involved a massive proxy testing scheme involving 600 candidates in 10 US states. The client is a large testing organization which provides its own examinations and which acts as an aggregator providing testing for other organizations. The examinations were major large volume exams for admission to US educational institutions. In the summer of 2004 Prometric assisted this client along with law enforcement in investigating the matter. We discovered during the course of the investigation that the following activities were occurring:

- Chinese examinees were paying \$3000.00 each to the conspirators for professional test takers to take one of the three academic tests involved.
- The professional test takers were armed with high quality forged identification documentation including passports so that the documentation presented would pass any test center scrutiny of the credentials.
- Analysis of credit card data and digital photos after the fact demonstrated that the 600 tests were in fact taken by a small number of professional test takers and that candidate fees were paid using a small pool of credit cards.
- The ring had been operating for at least 3 years, was discovered through a tip to the client, and required more than 600 schools and individuals to be notified the scores were obtained fraudulently.

b. In 2007 and 2008, Prometric assisted a large medical client in investigating a ring of individuals who were using false candidate profiles to capture exam content. In this case the individuals obtained seemingly legitimate credentials from a school which credentials were used by the client to create test eligibility files. This ring of professional test takers then took examinations in at least two US states and 3 foreign countries in order to capture content on behalf of a test preparation company. Our belief is that this was a small group of professional test takers, registering under a number of different identities, and having appropriate forged ID documents. Prometric and the client identified at least 8 different individuals that may have been part of the ring through credit card usage. Our strong belief is that had the client been using biometrics, an earlier flag would have been thrown that showed a suspicious pattern of test taking resulting in prevention of the ring from accessing future tests and attempting to capture content.

c. In 2009, through a tip from a Prometric employee, Prometric discovered a professional test taker who was taking entry level work safety examinations on behalf of an immigrant community in the UK. In this case, Prometric operates a number of mobile test vehicles, essentially complete

1501 South Clinton Street  
Baltimore, Maryland 21224  
USA

443 455 8000 PHONE  
866 PROMETRIC TOLL FREE  
866 776 6387 TOLL FREE

[www.prometric.com](http://www.prometric.com)



test centers in the back of tractor trailers in the UK. The client was not using biometrics although the technology was available for use. In at least 10 cases, the professional test taker arrived in place of the real candidate, using a different mobile location each time and with false identification documents that passed inspection by the test center administrators. Prometric caught the professional test taker because the individual attempted to employ a Prometric employee in the scam to avoid having to travel to numerous locations. Had the professional test taker simply continued to travel to multiple locations and use false identification, we might not have caught the individual as quickly. Had biometrics been used with this client, we would have caught the individual on the second attempt.

d. In October 2010, Prometric performed a surprise audit at a test center in India and discovered that individuals were present at the site and sitting US academic entry examinations on behalf of other individuals. While an investigation is still ongoing, we were by virtue of examination of the records able to determine that proxy testing was occurring. This involved a number of candidates present at the site although an exact count is not available until completion of the investigation.

e. In 2008 Prometric caught two sisters impersonating each other for the purpose of taking a higher education entrance examination for a health profession. The sisters were similar enough in appearance that average scrutiny of real US state drivers licenses did not reveal the false identity. In this case one sister traveled across the border from New York to Canada in an attempt to impersonate the other and obtain higher scores on her behalf. We were able to identify the impersonation because biometrics was in operation for this program in both New York and Canada.

f. In 2010, based on a tip through a security hotline, Prometric was made aware that a candidate for an association certification exam claimed that another individual associated with the test center, had taken the exam on her behalf. Prometric and the client began an investigation and based on a review of exam performance determined that the point gain from first attempt to second attempt indicated that someone did take the exam as a proxy for the candidate. The test center was located in Ontario Canada and we terminated the center's contract with Prometric over the issue and the client will discipline the candidate.

#### Use of Government Identification

In most if not all of these cases, Prometric has determined that government quality false identification documents were used by the proxy testers. In the first example this occurred at least 600 times. This is a large problem in the testing industry. A casual review of the internet, without any attempt to do more than a brief search, reveals at least 15 websites offering false ID documents. Most of these sites offer US and Canadian identity documents. The use of a website to acquire fake ID is not uncommon and computer technology enables sophisticated IDs difficult to detect for the average person. The criminal test takers in the case of the Chinese students likely had access to professional criminals capable of producing identification documents that are not discernible from real ID documents by anyone other than a professional. While Prometric and clients are working on technology that will enable better detection of false identity documents, biometrics is an equally effective and safe means of combating test fraud.

1501 South Clinton Street  
Baltimore, Maryland 21224  
USA

443 455 8000 PHONE  
866 PROMETRIC TOLL FREE  
866 776 6387 TOLL FREE

[www.prometric.com](http://www.prometric.com)



What is clear for each of the examples set out above is that biometrics would have stopped each of these incidents within 2 or 3 tests at the most. The trend we believe is toward greater use of biometrics as a fraud deterrent.

Websites offering false identification documents: (Note: the safety of any of these sites has not been verified. Prometric suggests that only an IT professional verify the site.)

[www.theidshop.com](http://www.theidshop.com)  
[www.photoidcards.com](http://www.photoidcards.com)  
[www.howtochangeyouridentity.info](http://www.howtochangeyouridentity.info)  
[www.fake-id.de](http://www.fake-id.de)  
[www.buyfakeidonline.com](http://www.buyfakeidonline.com)  
[www.newidcards.com](http://www.newidcards.com)  
[www.newid.com](http://www.newid.com)  
[www.fluxcard.com](http://www.fluxcard.com)  
[www.myfakeid.co.uk](http://www.myfakeid.co.uk)  
[www.nextdayid.co.uk](http://www.nextdayid.co.uk)  
[www.fakepassportsale.cc](http://www.fakepassportsale.cc)  
[www.fakeidfree.com](http://www.fakeidfree.com)  
[www.marketingoazis.hu](http://www.marketingoazis.hu)  
[www.developersdex.com](http://www.developersdex.com)  
[www.topix.com](http://www.topix.com)

## Use of Biometrics by Prometric

Prometric's biometric program is characterized by integrity, security, and adherence to privacy principles. The attached fact sheet contains additional information regarding our program, but I highlight here our adherence to strict privacy obligations.

1. Biometrics is used only to ensure the integrity of testing programs. Prometric does not and will not sell biometric information and we adhere to the highest standards of data privacy. Prometric uses the services of LexisNexis for processing the biometric data. Our contract with LexisNexis requires that the data be used solely for the detection of fraud and protecting the integrity of testing programs. LexisNexis is prohibited from any use of the biometric and demographic data except as permitted by Prometric in writing.
2. The biometric data and demographic data is securely stored and protected with stringent security measures. The data is segregated from all other LexisNexis data and LexisNexis programs. Prometric and LexisNexis meet or exceed current industry best practices for computer system and data center protections. Prometric regularly audits LexisNexis compliance and clients have also audited them.
3. Prometric collects only the information necessary to implement a test integrity program. All data is deleted within a reasonable time after the reason for collection is fulfilled. Prometric does not retain biometric data beyond such period of time as is necessary to fulfill the underlying program integrity needs.

1501 South Clinton Street  
Baltimore, Maryland 21224  
USA

443 455 8000 PHONE  
866 PROMETRIC TOLL FREE  
866 776 6387 TOLL FREE

[www.prometric.com](http://www.prometric.com)



4. Prometric adheres to the US Department of Commerce Safe Harbor regime for meeting strict European Union data protection requirements. Prometric and its clients routinely manage consent rules and varied data privacy requirements.

I trust that this information is of assistance in your consideration of a bill regulating biometric practices. Should you have additional questions, feel free to contact me per the below contact information.

Sincerely,

Anthony R. Scicchitano  
SVP and General Counsel  
443-455-8493 Direct  
443-455-6481 Fax  
[anthony.scicchitano@prometric.com](mailto:anthony.scicchitano@prometric.com)

cc: Honorable Bill Wielechowski

1501 South Clinton Street  
Baltimore, Maryland 21224  
USA

443 455 8000 PHONE  
866 PROMETRIC TOLL FREE  
866 776 6387 TOLL FREE

[www.prometric.com](http://www.prometric.com)

## **Identity Management – Biometric Check-in Fact Sheet**

### **Advantages to Testing Sponsors and Test Takers:**

- ID management and biometrics verify test taker information at the time of check-in, during breaks, and when returning to test at a later date. These procedures attempt to deter proxy testing, cheating and collaboration by test takers and testing proctors.
  - Example: In 2008 two sisters testing for a medical exam, attempted to test for one another. The first sister took the exam at a testing center in the United States and passed. Several months later the same sister crossed the country border into Canada and presented the ID of her sister attempting to test for the same exam under her sister's name. Although she had presented a new ID, her fingerprints matched that of her real ID. This was enough evidence to use for investigative purposes and identify this as a true proxy testing incident.
- Biometrics:
  - Electronically and accurately captures test taker information from government-issued photo ID documents, and recognizes if a test taker has enrolled and tested with Prometric previously
  - Protects the value of the credentialing program; credentials facilitate public trust, help support the economy, and enable individuals to contribute to society
  - Protects intellectual property
  - Deters proxy testing
  - Provides an enhanced method of identity verification to validate ID and fingerprint data has not been previously presented under a different name
  - Increases test takers perception of security and increases deterrence of cheating
  - Improves overall testing experience, specifically for return test takers
  - Keeps the test taker's data secure
  - Stringent security barriers build respect for credentials among peers and in marketplace

### **Prometric's Implementation Methods:**

- Biometric check-in is combined with several other standard security procedures in Prometric Test Centers worldwide including, digital video recording (DVR) monitoring, and protocol that prevents test taker's to bring items into the testing room during the examination.
- Biometric Consent Tool – a consent form is presented to the test taker during the scheduling and registration process asking the test taker to agree to the use of biometrics during check-in.
  - Dependent upon the location of the testing center and the laws within that country, the test taker will be presented with the appropriate consent form. There is a form for each of the following possible scenarios: fingerprinting is prohibited, the country has no laws against the use of fingerprints, consent is required, or consent is implied.
  - This feature acts as a means of preparing the test taker, prior to arriving at the test center, for what to expect during the biometric check-in process. This is expected to further minimize anything unexpected on the part of the test taker.
- Prometric works with each testing sponsor/organization to include information regarding biometric check-in within the sponsors test taker materials, including the sponsor's website and candidate bulletins.

URGENT FAX;

April 7, 2011

WE DEMAND REAL BIOMETRIC PRIVACY PROTECTION FOR ALL ALASKANS

Dear Senator:

**My name is Horst Poepperl, CEO of Borealis Broadband Inc.** I've already sent several emails in support of SB-98, but as I understand it, the current version has been watered down significantly with exemptions.

First of all, I do want to say that I appreciate and am grateful for those senators and representatives who have already taken a public stand for personal privacy, like our founding fathers intended. Especially those of you who have taken the time to respond to my emails personally. You have my heartfelt gratitude and support. The rest of this email might be informational for you but otherwise redundant.

For the rest of you:

How utterly disappointing and what a dangerous game to play with our personal information.

I would like to go on record AGAIN as OPPOSING the watering down of this privacy legislation and SUPPORTING strong privacy protections. If it continues as is, then you are making a very serious mistake regarding the privacy of your fellow Alaskans. It is much more prudent to pass strong privacy legislation and, if necessary, loosen it up on a case-by-case basis later. Doing the reverse and tightening up the legislation later is completely useless - your fellow Alaskans will already have their biometrics floating around cyberspace waiting to be sold to whomever...or lost to hackers.

In February of 2010 it was revealed that Israel had stolen biometric information from the passports of visitors to the country. Innocent and unsuspecting citizens of many countries were affected when the Mossad used their biometric information to fake passports and commit an assassination. [http://www.timesonline.co.uk/tol/news/world/middle\\_east/article7029553.ece](http://www.timesonline.co.uk/tol/news/world/middle_east/article7029553.ece)

Go ahead and take some time to read the article and see how that affected those people. Some of these people had to literally hide in their houses for a while and could no longer travel to entire parts of the world until the deception had been made public. Even today, they have to look over their shoulders for the rest of their lives in case some extremist didn't get the memo.

CEO of Borealis Broadband Inc p.2

Yes, it's an extreme example, but the point is, IT'S ALREADY HAPPENED. More than once. It's hard to think of an even more egregious use of stolen personal data, but I'm sure someone will figure out how to top that one at some point in the future.

Maybe next time, they'll just buy the information like everyone else and crank out fake passports to their hearts' content. Maybe they'll buy it from Choicepoint. Maybe that technique will become all the rage for other countries, hackers or criminals. Maybe some Alaskans' biometric data will be used because you didn't take the privacy issue seriously.

In my personal opinion, and saying this with all due respect, you DO NOT need to entertain Choicepoint or any data mining company. To me, the very idea that you would seriously entertain the wants of a foreign (or domestic) company of data snitches is just putrageous. What the hell for? Why give even one iota of leeway to a company that makes its money ratting out your personal information to the highest bidder? A new market for them, at our expense?

As far as other companies are concerned, you need to ask yourself; "what did they do before fingerprint readers were introduced commercially?" Suddenly we should believe that fingerprints are critical for their security procedures? Really? Fingerprint readers aren't even in widespread use yet as the consumer version of that technology has not yet fully matured. I think they just want to keep the door open and that's not nearly a good enough reason to sacrifice more of my privacy.

*As a career professional in the IT industry for the past 27 years, it just boggles my mind that we would even consider releasing more privacy information in light of all the historical abuse already.* To me, with what I've seen, experienced and know about this issue, it is just mind-numbingly dumb to even contemplate releasing additional information into this cesspool that the data-miners and other companies have created. Much less something as personal and unchangeable as fingerprints.

In the words of one of my buddies from my military days, "That can't get nuttin' but ugly." He said that every time he was looking at a problem that had no upside. Allowing the release of fingerprint biometrics has no upside. Period. Even for the National Security argument; no nation has ever been made more secure by ratting out its citizens.

Or maybe you need a reminder of how often data is stolen or lost:

<http://www.privacyrights.org/data-breach/new> That link will take you to a site that lists data breaches in chronological order. Be prepared for a long list.

CEO of Borealis Broadband Inc, p.3

I've already been notified that various pieces of my personal data were lost or stolen four times in the space of just six years. Once even by the Veteran's Administration, who, incidentally, probably has my fingerprints. Where is my compensation for creating all that work, stress and hassle for me for something that didn't have to be? I saw plenty of finger pointing but no one taking responsibility.

That's my skin in this game. I'm not at all interested in having you expose me to even more abuse and I will strongly resent it if you do. If a person wants to willingly give up their biometrics, then fine, let them. But never, ever, create or allow the conditions that FORCE us to.

I urge you to strengthen the privacy legislation as tight as you possibly can AND PROTECT ALL ALASKANS WITH IT. Making it airtight with the commitment to review on a case-by-case basis in the future would be acceptable for now. You will never go wrong with protecting our privacy and passing strong privacy legislation is the lowest risk path to take, not to mention the right thing to do by any measuring stick, no matter how much the lobbyists try to muddy the water for you. But you will most definitely screw up badly if you allow the release of our biometrics and force Alaskans to give up their fingerprints with weak legislation. You won't be able to correct that mistake later - once the data is out, it's out.

Best regards,

**Horst Poepperl**

CEO

Borealis Broadband, Inc.

Professional Quality Internet Service

# FAX

April 8, 2011

Dear Senator:

**My name is Gretchen Guess**, I am a former Senator, a former member of the Alaska State House of Representatives, and a resident of Anchorage. I fully support a ban on the compulsory fingerprinting of innocent Alaskans for ID purposes, and I urge you to pass a strong privacy law this session that:

"makes 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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,

**Gretchen Guess**

Anchorage

[guessak@gmail.com](mailto:guessak@gmail.com)

# FAX

April 8, 2011

Dear Senator:

**My name is Eric Britten, former Chairman of the Anchorage Chamber of Commerce and Past Chair of the Alaska State Chamber of Commerce.**

I am writing to you in support of a ban on compelling law-abiding Alaskans to be fingerprinted for ID purposes. I urge you to pass a strong privacy law *this session* that:

"makes 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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,

**Eric Britten**

Former Chairman of the Anchorage Chamber of Commerce

Past Chair of the Alaska State Chamber of Commerce

[eric@brittenassociates.com](mailto:eric@brittenassociates.com)

(907) 440-8181

April 7<sup>st</sup>, 2011

Dear Senator:

My name is Ted McMillan, a resident of Anchorage. I fully support NOT fingerprinting innocent Alaskans-for-ID, as described in the "Our goal" statement below.

Privacy rights are a basic freedom of every law abiding citizen. There's just some things you shouldn't do... involuntarily tracking law abiding citizens is one of them.

Having a company lobby to protect its revenue stream is almost immoral.

**"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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,  
Ted McMillan  
Anchorage  
[tmcmillan@gci.com](mailto:tmcmillan@gci.com)

April 5, 2011

Senator Hollis French  
Alaska State Legislature  
State Capitol Room 417  
Juneau, AK 99801-1182



Jack C. McRae  
Senior Vice President

RE: CSSB 98 Biometric information

Dear Senator French:

I am writing on behalf of Premera Blue Cross Blue Shield of Alaska to express concern about CSSB98(STA), "an Act relating to biometric information."

Under proposed new Section 1, new Sec. 18.14.090 Definitions, "biometric data" includes "voices" and "biometric system" means "an automated system capable of capturing biometric data from an individual's biometric information...storing the biometric data extracted... and comparing the biometric data extracted...with biometric data stored for the individual for use in future recognition of the individual..."

Proposed new section Sec 18.14.060 Exemptions sets forth exemptions to the collection, retention, analysis, disclosure or distribution of biometric information, but there is no exemption for quality control purposes.

Premera, as well as many other organizations, records telephone calls in our Customer Service department strictly for quality assurance purposes in order to provide quality and valued service to our customers.

We do not believe that regulating the recording of voices for this purpose is intended by this legislation and suggest that a related exemption be included in the legislation for clarity. Therefore, we request that the following language be added to CSSB98 (STA) to Section 1. Chapter 14 Biometric Information, under Sec. 18.14.060 Exemptions on page 2 after line 25: "(5) voices when used for quality assurance purposes."

Thank you for your consideration of this request. Please let me know if you have questions or would like to discuss this matter further.

Sincerely,

A handwritten signature in black ink that reads "Jack C. McRae".

Jack C. McRae  
Senior Vice President



Michael W. DePasquale  
Chief Executive Officer

March 25, 2011

Honorable Hollis S. French II  
Chair, Senate Judiciary Committee  
State Capitol, Room 205  
Juneau, AK 99801-1182

RE: SB 98

Dear Senator French:

On behalf of BIO-key International, I write to respectfully oppose SB 98, which would require prior written consent for the use of biometric technology in identity applications, and force any person, government agency, or business wishing to use a biometric as part of their business process to accept a photo ID as an valid alternative to doing so. In short, a photo ID check does not provide the same anti-fraud benefits as a biometric does, and is not an equivalent substitute. It does not address the problems of "identity theft with cooperation" and "one person having multiple identities" (aliases), which are central to so many identity theft and fraud scenarios, and can only be detected and prevented using biometrics.

BIO-key International develops and delivers advanced identification solutions to commercial and government enterprises who otherwise struggle with managing identity. Our finger identification technology accurately identifies and authenticates users, patients and customers in some of the world's largest identification deployments to improve security, guarantee identity, and help prevent identity theft. In fact, in part as a response to the FBI's misidentification problems such as those cited by Senator Wielechowski, our technology has been added to the FBI's recently deployed Next Generation Identification System, significantly improving the accuracy of that system.

It is noteworthy that the driver of the bus involved in the gruesome accident in New York City, killing 15 passengers, had his license suspended under several aliases, but was never detected, because the names didn't match. He was employed because his current photo ID driving record was clean. See <http://www.nbcnewyork.com/news/local/Crash-Driver-Used-Alias-118194134.html>. Without biometrics, how can a business needing to know who it is dealing with stop a person from either shedding their existing ID to assume a new one, or, as is the case in the exam fraud that the IACPA seeks to prevent, sharing it with a paid proxy to go take the exam for them?

Additionally, many commercial applications of biometrics are for safety, not just security - to automate the process of positive ID, without requiring an individual to carry an identification card. Hospitals, Blood Centers, and other beneficial entities rely on BIO-key to make a positive identification of their patients and donors in order to properly associate that person with their medical history, or to prevent prescription or medical ID fraud. In many of these cases, a misidentification can have deadly

consequences, as with the case of a blood transfusion to the wrong patient, or misidentification of surgery patient. A photo ID check only validates the name of a person, and does not ensure that it is the same individual, even if the name matches.

A search of the Houston (TX) County Hospital records found that they had 2500 or more "Maria Garcia's" in their records, and found that there had been three in the hospital at the same time! Biometrics are introduced to automate the positive ID of an individual, not just confirm that they have a particular name.

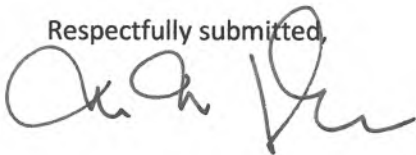
SB 98 assumes that the goal of a biometric system is simply to ensure that someone is matching the name that they say they are, and correctly envisions that a photo ID check is sufficient to achieve that goal. However, because there are so many people with the same name, and because people move over time, this is not a sufficient means to assure a consistent identity of a single individual over time. Even the government, with its immense access to information on individuals, uses biometrics in public assistance programs to prevent double dipping on benefits, and in law enforcement, because they recognize the failures of photo ID checks to determine if someone is a first time applicant for assistance or has a past criminal record that they might want to hide. Businesses struggle with the same issues, with much less access to data, as part of trying to prevent fraud and identity theft. Don't private entities have the right to know who they are trusting or doing business with, and to know that the Alaska laws support their using proven tools to assure the identity of those people?

Protecting individual privacy is important, but in the case of biometrics, the majority of people actually prefer the convenience and ID-Theft resistance of biometrics. Twice a year, Unisys Corporation commissions a recurring, statistical measure of consumer concern about four areas of security: national, financial, Internet and personal safety. The Unisys Security Index tracks trends in consumer perception of pressing security issues. Their objective findings inform the conversation about personal security and the use of biometrics.

The most recent Security Index was issued in October 2010 and can be downloaded in its entirety from <http://www.unisyssecurityindex.com/>. The study found that Americans are seriously concerned about identity theft and bankcard fraud. A 2009 study focused on biometrics for personal identification. It found that 73% of Americans are willing to use fingerprint identification to verify their identity with banks, government agencies and other organizations to prevent fraudulent misuse of their personal information.

I ask that full consideration be given to the many beneficial uses of biometric technology, and not focus on a small area of potential abuse in order to cut off this valuable and cost-saving means to prevent fraud and assure identity. Please vote no on SB 98.

Respectfully submitted,



Michael W. DePasquale

March 29<sup>th</sup> 2011

Dear Senator Hollis French:

We are a group of Alaskan voters who strongly support the need for stronger privacy legislation. **Specifically, we are *Citizens for Privacy in Alaska*, and we urge you to support and pass the new Alaskan Biometric Privacy Legislation SB-98 this session.**

All Alaskans cherish their privacy - it's even guaranteed by our State Constitution. As with opposing REAL ID, we Alaskans look to YOU, our representatives to stand up for our privacy rights against the Federal Government and corporate intrusion.

This privacy bill is supported by nearly everyone - from Libertarians to liberal Democrats, from conservative Republicans to the ACLU; from school teachers to military families, to CEOs, IT experts and oil company managers. Not surprisingly, only the lobbyists for the global data-mining firms seem to object (ChoicePoint/LexisNexis) because *this bill threatens their ability to profit from the exploitation of Alaskan's loss of privacy.*

SB-98 says essentially that biometrics (fingerprints etc) should not be required as identification when a valid driver's license or US passport is presented (this bill would not affect fingerprints taken for background checks and it would not affect law enforcement in any way).

As you may know, NY Senator Chuck Schumer and SC Senator Lindsey Graham have proposed as "the cornerstone" of their Immigration Reform a Federal Government plan to FINGERPRINT ALL AMERICANS under a new biometric National (work) ID Card program. A city in Arizona is right now considering mandating all customers of the local pharmacy be fingerprinted in order to pick up their prescriptions...those who object will be *denied their medicine*. With this rapidly deteriorating national privacy climate, Alaskans urgently need strong biometric privacy legislation now.

As you know, there are *very few issues* on which Alaskans from across the political spectrum agree. *The urgent need to protect our privacy* from constant and increasing Federal Government and corporate intrusion is one of them. Please do all you can to support the Biometric Privacy bill and pass it into law this session.

*Signed,*

*Citizens for Privacy in Alaska*

Co-chair: Tim Pearson – business owner

Co-chair: Jason Giaimo, business owner

Gretchen Guess: Alaskan voter, former Senator

Horst Poepperl: CEO and IT data privacy expert, Borealis Broadband Corporation

Mark Lerner: President, Stop REAL ID National Coalition

Jason Dowell: Libertarian Party Alaska, member

Cindy Miller: Former CFO of Unocal Alaska

Joe Dirksen: Resident, Alaska, Alaskan Voter, military family

Eunice Trask: Alaskan voter

Laura Dirksen: 20 year teacher at an Anchorage Christian School. Alaskan Voter

Barbara Brown: Alaskan Voter

Dan Bolland: State of Alaska, Audit Division, Alaskan Voter

Arzu Smith: CPA candidate

Tom Gill: UAA, formerly with BP, Alaskan Voter

Tim Wiepking: Institute of Management Accountants, former President, Alaskan Voter

George Ascott: Alaska resident, Alaskan Voter

Ralph Taylor: Taylor Consultants, President

Allan Johnston: Wedbush Morgan Securities, Alaskan Voter

Angela Gill: Alaskan Voter, medical professional

Andrew Blackman, CPA: Partner with Shapiro Lobel LLP

Karen Demichelis: President, Accountant, Demichelis & Associates, Alaskan Voter

Tyler Arnold: TylerSystems Inc. CEO, Alaskan Voter

Joel Smith: Former President of the Institute of Management Accountants, SF chapter

Tim Pearson: Pearson Consulting, Alaskan Voter

Jason Giaimo: Net Gain Business Consultants of Alaska, Alaskan Voter

Jack-Taylor Ridgeway: Privacy Rights supporter, advocate

Patrick Lorenz: Management, Analyst, British Petroleum, Alaskan Voter

Dianne Kelly: CPA, State of New Jersey

Chuck Kaucic: Alaskan voter, Wasilla

Chris Brownwell: Resident, Alaska, noted author, Alaskan Voter, military family

Hetal Giaimo: Alaskan Voter

Dawn Brownwell: Alaska Voter, military family

Kelly Mazzei: Alaskan Voter

Andrew Wilkins: IT expert at a large national bank.

Bruce Sollenberger: Alaskan Voters

Wendi Sollenberger: Alaskan Voters

Jeffrey Mittman: Executive Director, ACLU - Alaska

*...this is only a partial list of voters and supporters who are watching this bill*

ALASKA SENATE and ALASKA HOUSE SUPPORT INCLUDES:

**Bill sponsor: Senator Bill Wielechowski**

**Co-sponsor: Senator Coghill**

**Co-sponsor : Senator Kevin Meyer**

**Co-sponsor: Senator Johnny Ellis**

Will be a bill sponsor or co-sponsor: **Representative Berta Gardner**

Co-sponsor: Representative Allan Dick

Co-sponsor: Representative Wes Keller

Does not oppose: Whitney Brewster Alaska State Director, Division of Motor Vehicles

Does not oppose: Alaska Department of Health and Social Services

Reviewed SB190 (previous version of SB-98): previous Alaska Attorney General

Supported SB190 (previous version of SB-98) in committee: Senator Kookesh

Supported SB190 (previous version of SB-98) in committee: Senator Egan

Supported SB190 (previous version of SB-98) in committee: Senator French

Supported SB190 (previous version of SB-98) in committee: Senator McGuire

Supported SB190 (previous version of SB-98) in committee: Senator Paskvan

Co-sponsoring SB-98: Senator Cathy Giessel

Co-sponsoring SB-98: Senator Linda Menard

Will co-sponsor: Representative Tammie Wilson

Will co-sponsor: Representative Chris Tuck

Will co-sponsor: Representative Sharon Cissna

Will co-sponsor "very probably" Representative Mark Neuman

***FAX***

April 13, 2011

Dear Senator French:

My name is Tyler Arnold, Founder and CEO of **TylerSystems, Inc.** a rapidly growing global technology firm based in Anchorage. I urge your support for protecting the biometric privacy of Alaskans. I am also a member of Citizens for Privacy in Alaska, and we are watching this bill closely.

**"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."

Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates

PLEASE stand up for our privacy -- and support this bill.

Tyler Arnold  
CEO, TylerSystems, Inc.  
227-9541  
[tyler@tylersystems.com](mailto:tyler@tylersystems.com)

April 13, 2011

Dear Senator French:

**I am writing in support of protecting biometric data.** I am a past President of Alaska Chapter of the Institute of Management Accountants (IMA) and have been employed in mostly accounting and/or financial positions over my work life.

From the financial side, the people who typically steal large amounts of money from businesses or non-profits are well thought of or even "Pillars of the Community" --- before the disgracing headline hits.

Collecting biometric data will do nothing to reduce the amount of criminal activity within financial circles.

**A passport or a driver's license is adequate identification for test taking purposes. SUPPORT THE NEW BIOMETRIC PRIVACY BILL**

Thank you for your consideration.

Sincerely  
Tim A. Wiepking  
Anchorage, 99508  
529-0766

04/ 13/2011

Dear Senator French:

My name is Dr. Frank Jeffries, an Assistant Professor of Business and Public Policy at a major educational institution in Alaska. This is my personal view.

I recently learned of a grass-roots group of Alaskan voters called the "Citizens for Privacy in Alaska" and of their courageous support for a MUCH NEEDED privacy bill. Although this is my personal view, I urge you to support it.

**I strongly support a biometric privacy bill that:**

"makes 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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,

**Dr. Frank Jeffries**

Assistant Professor of Business and Public Policy

Anchorage

[taikodad@gci.net](mailto:taikodad@gci.net)

April 13<sup>st</sup>, 2011

Senator French:

My name is Kathryn Eckmann, a voter and very concerned citizen of this great State.

**Stand up for ALL Alaskans privacy!** Pass a strong Biometric Privacy law this session that protects ALL Alaskans...not just a select few. I agree with Citizens for Privacy in Alaska; we need a privacy law that:

"makes 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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,

*Kathryn*

Kathryn Eckmann

A concerned Alaskan Voter

[Kmal2@gci.net](mailto:Kmal2@gci.net)

April 13, 2011

FAX

Dear Senator French:

My name is Kelly Mazzei, from Anchorage. I strongly support the Biometric Privacy Bill, and I hope that you will also. Alaskans are at risk and we need this to pass this session!

I support and agree with Citizens for Privacy in Alaska that we need 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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,

**Kelly Mazzei**

Anchorage Voter

[kamazzei@gmail.com](mailto:kamazzei@gmail.com)

April 13<sup>st</sup>, 2011

Dear Senator French:

**My name is Eileen Becker, from Homer.** I support SB 98 (THE BIOMETRIC PRIVACY BILL) because too many of our rights to privacy are being sold to the highest bidder.

**It is time to say NO and protect ourselves and our families. PROTECT ALL ALASKANS.**

Thank you,

Eileen Becker

Owner of Peninsula Communications, Inc, privately owned radio stations here in Alaska

Mother of 5 children and 8 grandchildren

Alaska resident since 1973

[DISTRICT35REPUBLICAN@WEBTV.NET](mailto:DISTRICT35REPUBLICAN@WEBTV.NET)

ALASKAN VOTER, REPUBLICAN PARTY

**"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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.**

April 13<sup>st</sup>, 2011

Dear Senator French:

My name is Tim Pearson, an Anchorage business professional and Co-Chairman of the Citizens for Privacy in Alaska. I urge your support for protecting the biometric privacy of Alaskans, PLEASE PASS SOMETHING THIS SESSION!

Please remember that unlike credit cards, stolen or lost fingerprints and biometric information cannot be replaced. Innocent Alaskans *deserve the option* of not being forced to provide their fingerprints. Passports and driver's licenses are sufficient identification.

Alaskan businesses do not want to take on the **legal liability** of losing the irreplaceable data of their employees or customers. There is no way to make people whole again.

"**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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

**PLEASE stand up for our privacy -- and pass a strong Biometric Privacy law this session that includes the "Alternative ID" provision (ie. allows an opt-out for people who show a driver's license or passport as ID).**

Sincerely,

**Tim Pearson**

President, Pearson Consulting  
Graduate of Harvard University  
Fmr Vice President of Human Resources, GCI  
[tim@timpearson.net](mailto:tim@timpearson.net)  
952-3498

April 13<sup>st</sup>, 2011

Dear Senator French:

My name is Joe Dirksen, a voter, a long-time Alaskan, a member of the Alaska National Guard and, like most Alaskans, I am a strong supporter of privacy rights. My personal view is that **you should strongly support the new biometric privacy bill...** if it says that no fingerprinting of innocent Alaskans for ID should be required, as noted below:

**"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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Will you stand up for our privacy rights?

Sincerely,

**Joe Dirksen**

Anchorage voter

South Anchorage, 99507

[jldirksen@acsalaska.net](mailto:jldirksen@acsalaska.net)

04/ 13/2011

FAX

Dear Senator French:

**As Director of a Village Corporation in Marshall, Alaska** – I can tell you that I am a very strong supporter of privacy. I hope you will show us that you are as well, but supporting the Biometric Privacy Bill when it comes before you.

**I support real protection that:**

"makes 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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,  
George Owletuck  
Director, a native Village Corporation  
Marshall, Alaska  
[George.owletuck@gmail.com](mailto:George.owletuck@gmail.com)

PS This is my personal position

# FAX

April 13, 2011

Dear Senator French:

**My name is Gretchen Guess**, I am a former Senator, a former member of the Alaska State House of Representatives, and a resident of Anchorage. I fully support a ban on the compulsory fingerprinting of innocent Alaskans for ID purposes, and I urge you to pass a strong privacy law this session that:

"makes 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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,

**Gretchen Guess**

Anchorage

[guessak@gmail.com](mailto:guessak@gmail.com)

April 13<sup>st</sup>, 2011

Dear Senator French:

My name is Herbert Eckmann, a voter from Anchorage and very concerned citizen of this great State.

I URGE YOU to stand up for ALL Alaskans privacy. Pass a strong Biometric Privacy law this session that includes an opt-out for ALL ALASKANS who show a driver's license or passport as ID. I agree with Citizens for Privacy in Alaska; we need a privacy law that:

"makes 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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,

**Herbert Eckmann**

A concerned Alaskan Voter

[Kmal2@gci.net](mailto:Kmal2@gci.net)

URGENT FAX;

April 13, 2011

PASS BIOMETRIC PRIVACY PROTECTION FOR ALL ALASKANS THIS SESSION!

Dear Senator French:

**My name is Horst Poepperl, CEO of Borealis Broadband Inc.** I've already sent several emails in support of SB-98, but as I understand it, the current version has been watered down significantly with exemptions.

First of all, I do want to say that I appreciate and am grateful for those senators and representatives who have already taken a public stand for personal privacy, like our founding fathers intended. Especially those of you who have taken the time to respond to my emails personally. You have my heartfelt gratitude and support. The rest of this email might be informational for you but otherwise redundant.

For the rest of you:

How utterly disappointing and what a dangerous game to play with our personal information.

I would like to go on record AGAIN as OPPOSING the watering down of this privacy legislation and SUPPORTING strong privacy protections. If it continues as is, then you are making a very serious mistake regarding the privacy of your fellow Alaskans. It is much more prudent to pass strong privacy legislation and, if necessary, loosen it up on a case-by-case basis later. Doing the reverse and tightening up the legislation later is completely useless - your fellow Alaskans will already have their biometrics floating around cyberspace waiting to be sold to whomever...or lost to hackers.

In February of 2010 it was revealed that Israel had stolen biometric information from the passports of visitors to the country. Innocent and unsuspecting citizens of many countries were affected when the Mossad used their biometric information to fake passports and commit an assassination. [http://www.timesonline.co.uk/tol/news/world/middle\\_east/article7029553.ece](http://www.timesonline.co.uk/tol/news/world/middle_east/article7029553.ece)

Go ahead and take some time to read the article and see how that affected those people. Some of these people had to literally hide in their houses for a while and could no longer travel to entire parts of the world until the deception had been made public. Even today, they have to look over their shoulders for the rest of their lives in case some extremist didn't get the memo.

CEO of Borealis Broadband Inc p.2

Yes, it's an extreme example, but the point is, IT'S ALREADY HAPPENED. More than once. It's hard to think of an even more egregious use of stolen personal data, but I'm sure someone will figure out how to top that one at some point in the future.

Maybe next time, they'll just buy the information like everyone else and crank out fake passports to their hearts' content. Maybe they'll buy it from Choicepoint. Maybe that technique will become all the rage for other countries, hackers or criminals. Maybe some Alaskans' biometric data will be used because you didn't take the privacy issue seriously.

In my personal opinion, and saying this with all due respect, you DO NOT need to entertain Choicepoint or any data mining company. To me, the very idea that you would seriously entertain the wants of a foreign (or domestic) company of data snitches is just outrageous. What the hell for? Why give even one iota of leeway to a company that makes its money ratting out your personal information to the highest bidder? A new market for them, at our expense?

As far as other companies are concerned, you need to ask yourself; "what did they do before fingerprint readers were introduced commercially?" Suddenly we should believe that fingerprints are critical for their security procedures? Really? Fingerprint readers aren't even in widespread use yet as the consumer version of that technology has not yet fully matured. I think they just want to keep the door open and that's not nearly a good enough reason to sacrifice more of my privacy.

*As a career professional in the IT industry for the past 27 years, it just boggles my mind that we would even consider releasing more privacy information in light of all the historical abuse already.* To me, with what I've seen, experienced and know about this issue, it is just mind-numbingly dumb to even contemplate releasing additional information into this cesspool that the data-miners and other companies have created. Much less something as personal and unchangeable as fingerprints.

In the words of one of my buddies from my military days, "That can't get nuttin' but ugly." He said that every time he was looking at a problem that had no upside. Allowing the release of fingerprint biometrics has no upside. Period. Even for the National Security argument; no nation has ever been made more secure by ratting out its citizens.

Or maybe you need a reminder of how often data is stolen or lost:

<http://www.privacyrights.org/data-breach/new> That link will take you to a site that lists data breaches in chronological order. Be prepared for a long list.

CEO of Borealis Broadband Inc, p.3

I've already been notified that various pieces of my personal data were lost or stolen four times in the space of just six years. Once even by the Veteran's Administration, who, incidentally, probably has my fingerprints. Where is my compensation for creating all that work, stress and hassle for me for something that didn't have to be? I saw plenty of finger pointing but no one taking responsibility.

That's my skin in this game. I'm not at all interested in having you expose me to even more abuse and I will strongly resent it if you do. If a person wants to willingly give up their biometrics, then fine, let them. But never, ever, create or allow the conditions that FORCE us to.

I urge you to strengthen the privacy legislation as tight as you possibly can AND PROTECT ALL ALASKANS WITH IT. Making it airtight with the commitment to review on a case-by-case basis in the future would be acceptable for now. You will never go wrong with protecting our privacy and passing strong privacy legislation is the lowest risk path to take, not to mention the right thing to do by any measuring stick, no matter how much the lobbyists try to muddy the water for you. But you will most definitely screw up badly if you allow the release of our biometrics and force Alaskans to give up their fingerprints with weak legislation. You won't be able to correct that mistake later - once the data is out, it's out.

Best regards,

**Horst Poepperl**

CEO

Borealis Broadband, Inc.

Professional Quality Internet Service

Dear Senator French:

April 13, 2011

As the owner and President of a small business, I have no need for fingerprint "biometric" security systems and I never will.

The ABSOLUTE LAST thing I would want would be to be legally liable for a data breach involving my employee's fingerprints! *Their privacy would be compromised for the rest of their lives* because fingerprints are like passwords that you can never change. I would be responsible for that...I can only imagine the lawsuits! **Alaskan businesses are NOT interested the risky proposition of fingerprint security systems.**

I strongly support the bi-partisan bill to protect our private biometric data (SB 98), and URGE you to pass it into law *this session* with the "Alternative ID" section intact.

We Alaskans have entrusted YOU to stand up for our privacy rights against Federal intrusion and corporate special interests...and we are all watching this bill closely.

Global data-miner ChoicePoint/LexisNexis/Reed Elsevier, has NO legitimate voice in this process, please don't even grant them a meeting. They have flown a team of east coast lobbyists to Juneau to "influence" you -- and will attempt to scare you with a bunch of nonsense because **they profit by exploiting Alaskan's loss of privacy.**

If they weren't making money off collecting and trafficking our private information, why would they be here?

Who will you stand with?

Regards,  
Jason Giaimo  
Anchorage Real Estate Investor, Accountant, Small business owner  
(907) 602-9250  
[Giaimo1@aol.com](mailto:Giaimo1@aol.com)

April 13, 2011

**URGENT FAX:**

**SUBJECT: PLEASE DON'T PUT ALASKANS AT RISK FOR ANOTHER YEAR-  
PASS THE PRIVACY BILL (SB-98) THIS SESSION**

Dear Senator French:

Last week, data-miner Epsilon may have exposed your family's personal data to criminal hackers during a massive data-breach, as reported in the Wall Street Journal. About a dozen of my Alaskan friends also received notices that their secure data was accessed by criminals. Epsilon stores private data for customers of firms like Citibank, JP Morgan, Disney etc.

What if you or your children had been forced to give this data-miner fingerprints-for-ID? Might it be possible for a criminal hacker to place your children's fingerprints at a crime scene? (that's easy to do). Would you be able to prove their innocence?

If this sounds theoretical, look up Mr. Brandon Mayfield. He's an attorney from Oregon who was jailed because his fingerprints were *thought* to be on a bomb that blew up a train in Madrid in 2004 (there are hundreds of other examples). Will the Federal Government (or a foreign data-mining corporation) abide by an Alaskan law that says they can't sell the info once collected? Would we ever know if they breached this law?

In March, RSA Security, one of the world's most secure networks was hacked, with criminals gaining access to its corporate network and stealing information about its SecurID two-factor authentication products.

If you ask data-security experts (and I encourage you to do so), to a person they will tell you that **the only way to be 100% sure information will not be lost, stolen or accessed...is not to collect it in the first place.**

**Please take a bold stand for real biometric privacy. Alaskan's are demanding it.**  
Ban fingerprints-as-ID mandates for all law-abiding Alaskans.

Jason Giaimo  
Founder, Co-Chairman  
Citizens for Privacy in Alaska  
907 602 9250  
(Go to [www.PrivacyNowAK.org](http://www.PrivacyNowAK.org) you will be shocked by what you find)

**FAX**

April 13<sup>st</sup>, 2011

Dear Senator French:

As a dedicated member of Alaska's Republican Party, I would like to ask you to support the Wielechowski/Coghill "biometric privacy bill" (and its House companion bill) so long as it protects ALL Alaskan's from being forced into being fingerprinted for ID purposes.

Sincerely,

**Jerad McClure**

Member, Alaska Republican Party

[jaredlainak@gmail.com](mailto:jaredlainak@gmail.com)

04/13/2011

Dear Senator French:

My name is James MacKenzie, Director of a major non-profit firm in Anchorage. I learned that you were planning to stand up for our privacy rights through a friend today, and I STRONGLY urge your support of the new Biometric Privacy Rights bill – so long as it contains REAL protection as noted below.

"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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,

**James MacKenzie**  
Director, Anchorage Voter  
Anchorage, AK  
[mackenzie.jamesa@gmail.com](mailto:mackenzie.jamesa@gmail.com)

PS note that this is my personal position on this subject

Dear Senator French:

April 13, 2011

My name is JP Godfrey, a Management Consultant in private practice in Anchorage.

I have to say, what Citizens for Privacy in Alaska is doing is astonishing – and I strongly support them and **I strongly support this privacy bill!** Don't let the lobbyists water it down, we need REAL protection.

**"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."**

Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates

Sincerely,  
JP Godfrey  
CEO, Management Consultant  
Anchorage, AK  
[jpgod@gci.net](mailto:jpgod@gci.net)

# FAX

April 13, 2011

Dear Senator French:

As an Alaskan voter, small business owner and accountant, **I urge you to support and pass biometric privacy legislation *this session*.**

I am also a member of Citizens for Privacy in Alaska, and we are all watching this bill closely.

**"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."**

Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates

Karen Demichelis, Principal  
Demichelis & Associates  
karen.demichelis@gmail.com  
tel: 907-360-2661

April 13, 2011

Dear Senator French:

I'm writing to ask to you support the STRONGEST version of SB 98 **which would prevent anyone from ever collecting** or disseminating biometric data. As an Alaskan I value my privacy greatly as well as that of my clients.

The gradual degradation of our privacy over the last few years is deeply troubling to me – it is now impossible to know who has our data and what they are doing with it. But, at least one has protections using credit cards and the like – you may get dinged but you are covered. And if your email gets targeted by the advertisers, drug purveyors and sexual enhancement folks (and yes, my mother gets those too) you have recourse.

On the other hand, if our biometric information gets loose into cyberspace all hell can break loose if your prints, or mine, get used by an unscrupulous person, much less a terrorist.

**Now is the time to draw the line, hard and fast. This is no time to become spineless and give into lobbyists who have many assurances of safety, but no guarantees and no accountability when this data gets loose – and you all know that it will.**

**Please a support meaningful, strong SB 98. The “Alternative ID” section must stay.**

Thanks. Ken.

---

Kenneth G. Robertson  
Robertson Law Office  
310 K Street, Suite 200  
Anchorage, Alaska 99501  
(907) 278-5657  
(907) 346-2810 Fax  
[www.robertsonlaw.net](http://www.robertsonlaw.net)

April 13, 2011

Dear Senator French:

My name is Kelly Mazzei, a voter from Anchorage. **You must stand up to these Outside data-miner lobbyists and support our privacy rights!** I am also a member of 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."** Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates

Sincerely

*Kelly Mazzei*

A REGISTERED VOTER

Anchorage

kamazzei@gmail.com

April 13<sup>st</sup>, 2011

Dear Senator French:

We vote...the data-miner's lobbyists don't. Please stand up for ALASKANS and our privacy, and **support** the new biometric privacy bill... if it says that no fingerprinting of innocent Alaskans for ID should be required.

My name is Laura Dirksen, a school teacher and resident of south Anchorage. Having taught for nearly 20 years at an Anchorage Christian school – I AGREE that our privacy laws need to be updated to *prevent* fingerprint collection “as ID.”

I urge your support for protecting the biometric privacy of Alaskans. Passports and driver's licenses are sufficient identification.

"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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates.

Sincerely,

*Laura Dirksen*

Laura Dirksen  
Christian school teacher, and a voter  
Anchorage  
[jldirksen@acsalaska.net](mailto:jldirksen@acsalaska.net)

April 13, 2011

Dear Senator French:

As owner and President of Pacific Rim Media – I can tell you that I am a strong supporter of the Citizens for Privacy in Alaska. They are standing up for our privacy and I hope you will too.

**"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."

Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates

Sincerely,

*Russel*

Russell Pounds  
President, Pacific Rim Media  
Anchorage, AK  
[Russell@prmalaska.com](mailto:Russell@prmalaska.com)  
[www.prgalaska.com](http://www.prgalaska.com)

## IMPORTANT FAX

April 13, 2011

Dear Senator French:

My name is Taylor Ridgeway. I am a strong supporter of Citizens for Privacy in Alaska, and I URGE you to stand up for Alaska's privacy rights against the data-miner's lobby! All of these oppressive encroachments are whittling away at the average Americans ability to engage in free commerce. These practices are unconstitutional...this has got to stop!

"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." Note that criminal background checks or law enforcement will not be affected by this legislation. This is specifically focused on biometrics-as-ID mandates

Sincerely

*Taylor Ridgeway*

Taylor.ridgeway@gmail.com