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

Executive Summary

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

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

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

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

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

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

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

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

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

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

A Brief Biometrics Primer

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

How S.B. 98 Addresses Biometrics

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

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

Biometrics Definitions

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

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

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

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

Notice and Consent

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

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

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

Revocation and Amendment of Permission, Disposal of Data

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

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

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

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

Outlawed Marketing

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

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

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

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

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

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

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

Penalties

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

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

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

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

Addressing Biometrics With a Lighter Touch

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

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

Contract and Tort Liability Clarified

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

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

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

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

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

No "Third-Party" Doctrine in Alaska

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

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

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

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

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

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

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

Avoid Occupational Cartels

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

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

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

Commit Alaska to Oppose Biometric National ID Systems

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

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

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

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

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

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

Conclusion

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

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

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

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

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