SB 190

26-LS0332\W
Bannister
4/7/10

CS FOR SENATE BILL NO. 190( )

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-SIXTH LEGISLATURE - SECOND SESSION

BY

Offered:
Referred:

Sponsor(s): SENATORS WIELECHOWSKI, Ellis

A BILL

FOR AN ACT ENTITLED

"An Act relating to biometric information."

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

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

Chapter 14. Biometric Information.

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

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

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

(1) United States passport; and

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

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to another person, biometric information, based on consent that is provided in a uniform consent form that has not been revoked, is exempt from civil liability under AS 18.14.060 and from criminal liability for the retention, analysis, disclosure, or distribution of the biometric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

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

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

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

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

(2) when authorized by state or federal law.

Sec. 18.14.090. Definitions. In this chapter,

(1) "biometric data" means fingerprints, handprints, voices, facial images, iris images, or retinal images;

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

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

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

(B) extracting and processing the biometric data captured under

(A) of this paragraph;

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

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

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

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

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

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

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

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

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

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

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

ALASKA STATE LEGISLATURE

Session
State Capitol, Rm. 115
Juneau, AK 99801
(907) 465-2435
Fax: (907) 465-6615

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

Senator_Bill_Wielechowski@legis.state.ak.us

Co-chair
Joint Armed Services Committee
Resources Committee

Member
Energy Committee
Judiciary Committee
World Trade Committee

SENATOR BILL WIELECHOWSKI

Draft CS for SB 190(JUD) – Proposed Changes

The following changes are proposed for Senate Bill 190 in the Senate Judiciary Committee and can be found in the attached version 26-LS0332\W:

1. A new chapter entitled "Biometric Information" is created for this provision of the law.

Discussion: This was done at the recommendation of the Attorney General's office because SB 190 is substantially different from the chapter in which it was originally contained titled "Genetic Privacy."

Location: Page 1, lines 3 and 4.

2. The term "collect" is removed from the bill.

Discussion: Both the Attorney General's office and committee members expressed concern that the term "collect" might prevent legitimate social and economic practices from taking place.

Location: Page 1, lines 5-7; page 2, lines 3-4; page 2, lines 16-17.

3. Clarification was made that there is an exception for the retention, analysis, disclosure, or distribution of biometric information for law enforcement purposes, or when authorized by state or federal law.

Discussion: This is based on suggested language from the Attorney General's office and is intended to clarify that private investigations into such crimes as fraud or arson are legal, and that biometric information can continue to be collected for criminal background checks.

Location: Page 2, lines 16-21.

4. The word "willing" is removed from the "informed and written consent" found in the previous version.

Discussion: This language now mirrors that which is found in the current Genetic Privacy statute.

Location: Page 1, line 7; page 2, lines 9 and 10.

5. Biometric data cannot be required for personal identification if the person to be identified can provide a valid current United States Passport and valid state or military ID.

Discussion: Since biometric data, such as a fingerprint, is only as good as the initial ID with which it is presented, it would seem that there is no valid reason to collect this data identification purposes.

Location: Page 1, lines 10-15.

6. The definitions section has been greatly expanded and clarified. A distinction has been made between "biometric information," "biometric data," and a "biometric system." The "biometric information" referenced in this bill is now defined as "biometric data" that has been used in an automated system capable of capturing, extracting, and processing biometric data. Further, the system must be capable of storing the data, comparing the data with other stored data, and indicating whether an indication or verification of identity has been achieved.

   This section also provides clear definitions for the specific forms of biometric information referenced in this bill—using definitions from the National Science and Technology Council to the extent practicable.

Location: Page 2, lines 22-31; and page 3, lines 1-26.

ALASKA STATE LEGISLATURE

Session
State Capitol, Rm. 115
Juneau, AK 99801
(907) 465-2435
Fax: (907) 465-6615

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

Senator_Bill_Wielechowski@legis.state.ak.us

Co-chair
Joint Armed Services Committee
Resources Committee

Member
Energy Committee
Judiciary Committee
World Trade Committee

SENATOR BILL WIELECHOWSKI

Senate Bill 190

"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; but also holds the potential for misuse by those who would use a person's genetic data to obtain information about them that they would normally have an express right to keep private.

Senate Bill 190 would update this legislation 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 include such information as iris and retinal patterns, hand geometry, voice patterns, and facial characteristics.

At this time, 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 DNA 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 has 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.

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 February 22, 2010

SUBJECT: SB 190 relating to biometric information
(Work Order No. 26-LS0332\P)

TO: Senator Bill Wielechowski
Attn: George Ascott

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. Expands AS 18.13.010(a), which currently deals with DNA information, to prohibit collecting other biometric information from a person, retaining other biometric information, and disclosing the results of other biometric information without the required consent. Makes the other biometric information the exclusive property of the person who was the source of the biometric information.

Section 2. Amends AS 18.13.010(b), which lists the situations to which (a) does not apply. Expands the subsection to indicate that the listed situations cover "other biometric information collected" as well as DNA. Adds to the list an exception for background checks as required or permitted by state or federal law.

Section 3. Amends AS 18.13.020, which provides a private right of action for violations. Adds the biometric information prohibitions to the violations for which a person has a right of action.

Section 4. Amends AS 18.13.030(a), which sets a criminal penalty for violations, to include violations of the biometric information prohibitions. Removes governmental entities from the subsection.

Section 5. Amends AS 18.13.030(c), which makes the crime a class A misdemeanor. Conforms the name of the violation to the name of the crime established in (a).

Section 6. Amends AS 18.13.100, the definition section for AS 18.13. Adds definitions for "biometric information," "governmental entity," and "person."

If I may be of further assistance, please advise.

TLB:ljw
10-123.ljw

Science News

Facial Biometrics System Capable of Creating a Facial 'DNA'

ScienceDaily (Nov. 16, 2009) — Research into techniques of facial biometrics, carried out by scientists at Universidad Carlos III de Madrid (UC3M), has resulted in a system that is able to recognize the facial "DNA" of every individual by determining his/her most noteworthy facial traits, with a of 95% rate of precision.

A new facial biometrics system that is able to recognize the facial "DNA" of every individual by determining his/her most noteworthy facial traits. (Credit: Image courtesy of Universidad Carlos III de Madrid - Oficina de Información Científica)

See also:

Computers & Math
- Mathematics
- Artificial Intelligence
- Computer Modeling
- Computer Programming
- Information Technology
- Mathematical Modeling

Reference
- Speech recognition
- Computational genomics
- Mathematical model
- Computer vision

Recognition techniques based on facial features, known as facial biometrics, is usually based on the search for those traits which make one face different from another. The research carried out by this team, in contrast, approaches the issue from a slightly different point of view.

"The difference between our work and the majority of the others that are found in this field is the idea of individualized models," explains one of the study's authors, mathematician David Delgado Gomez from the UC3M Statistics Department. "Our objective," he continued, "is to create a model for each person which highlights the most distinguishing features of each face, as a sort of facial 'DNA'."

The researchers had this idea when they were imagining the situation of a crowded room where someone comes in asking for one of them. "Our way to describe a person is through some traits that the others don't have, such as the tall woman with blue eyes, or the bald guy with a beard. We try to apply this idea to our algorithm," remarked Professor Delgado, who has been carrying out this research with Federico Sukno, Kaushik Pavani and Alejandro Frangi from the CISTIB Group of *Universidad Pompeu Fabra* of Barcelona, and Bjarne Ersboll and Jens Fagertun from the mathematical modelling group of Technical University of Denmark, which has recently published an article entitled "Similarity-based Fisherfaces," with some of their research results appearing in the scientific journal *Pattern Recognition Letters*.

Basic elements

A facial biometrics system is normally made up of three components. First, a camera is necessary to record an image; secondly, a software program is needed which determines if there is a face in that image, locating among other things, the facial geometry (the placement of the eyes, nose, mouth, etc.); and thirdly, a system that is capable of classifying all those elements to differentiate between them and those of other persons. The most complicated part, according to the researchers was combining the facial geometry and facial texture.

"With only the geometric information, very low classifications are obtained, which is why we combine this information with that of facial texture to obtain a more robust model, and a statistical way of combining them occurred to us, which offered very good results.," Delgado pointed out. The researchers have shown that when this system is used in a controlled environment, it can achieve a 95% rate of precision.

The main complication occurring when using this type of systems is the lighting, which can change the color of the face. Another challenge is the passage of time, because as a person ages, his/her face undergoes changes as it becomes heavier, thinner, or more wrinkled, which can then fool the classifiers. On the other hand, the researchers add, it does have a significant advantage when compared to other biometric systems: it doesn't need direct interaction with a person as do fingerprinting or iris recognition, for example.

Adapted from materials provided by Universidad Carlos III de Madrid - Oficina de Información Científica, via AlphaGalileo.

Mayachitra imago
Bioimage management and analysis software. Free trial is available.
www.mayachitra.com/imago

Related Stories

Improving Security With Face Recognition Technology (Nov. 15, 2009) — A number of US states now use facial recognition technology when issuing drivers licenses. Similar methods are also used to grant access to buildings and to verify the identities of international ... > *read more*

New Image Processing System Detects Moods (Dec. 4, 2008) — Researchers are developing a computer image processing system that detects and classifies human facial expressions. The aim of this system is to take and analyze photos of individuals, potentially in ... > *read more*

New Step Taken Towards A Machine Capable Of Face Recognition (Feb. 20, 2007) — A recent study shows that facial recognition through machine vision is technically possible. This raises interesting prospects for future machine vision ... > *read more*

Saying 'Cheese' For More Effective Border Security (Dec. 3, 2008) — Researchers have found that several simple steps can significantly improve the quality of facial images that are acquired at border entry points such as airports and ... > *read more*

Intelligent System To Help Autistic Children Recognize Emotions (Oct. 19, 2009) — Computer scientists are working on the development of an efficient and intelligent facial expression recognition system. The system is capable of locating the face region using derivative-based ... > *read more*

Number of stories in archives: 77,634

Special investigation: How my genome was hacked

25 March 2009 by Peter Aldhous and Michael Reilly
Magazine issue 2701. Subscribe and get 4 free issues.
For similar stories, visit the Genetics Topic Guide

Editorial: *Time for laws on genome spies*

This man's genome has hacked. That was for work purposes. You may not be so lucky (Image: Mark Richards)

1 more image

INTIMATE secrets hidden in your DNA could be stolen without you even realising. By taking a glass from which you have drunk, a "genome hacker" could obtain a comprehensive scan of your genome, revealing DNA variants that help determine your susceptibility to a wide range of diseases, from a common form of blindness to Alzheimer's disease.

That's the disturbing finding of a *New Scientist* investigation, in which one of us - Michael Reilly - "hacked" the genome of the other - Peter Aldhous - armed with only a credit card, a private email account and a home address.

You might have thought that genome hacking requires specialist skills, and personal access to sophisticated equipment. But in recent years, some companies have started to offer personal genome scans to the public over the internet. Other firms routinely analyse genomes on behalf of scientists involved in human genetics research. In theory, both types of service are vulnerable to abuse by a genome hacker determined to submit someone else's DNA for covert analysis.

Until our investigation, it was not clear whether this would be possible in practice. Could a hacker with no access to a genetics lab take an item carrying another person's DNA and obtain a sample that companies would accept for scanning? Would the sample be of high enough quality to yield accurate results? And would genome analysis companies have procedures in place to identify and refuse suspicious orders?

We decided to find out. Rather like computer security researchers who expose vulnerabilities in software code so that they can be "patched" to guard against malicious hackers, our goal was to uncover vulnerabilities in the way companies offering genome scans operate, so that they can be fixed.

Our investigation uncovered some loopholes that might be closed to help thwart genome thieves. The findings also strengthen the case for additional laws to protect the information contained in the DNA that we all shed continually and leave lying around.

"Just as we have a right to expect that relatives, neighbours, or even strangers can't poke through our medical records without our permission, we should have a right to expect that people can't snoop through our genes," says Kathy Hudson, who heads the Genetics and Public Policy Center in Washington DC.

We should have a right to expect that people can't snoop through our genes

Our experimental genome hack began like this: Peter drank water from a glass, which he handed to Michael. Michael's first task was to get Peter's DNA off the glass and turn it into a sample that he could submit to a genome-scanning company.

Michael approached several firms that ordinarily extract DNA from items like drinking glasses and match this DNA against particular individuals, on behalf of the police, private detectives or citizens pursuing their own investigations. He said nothing about his intentions, but soon found a company that would extract the DNA without performing any DNA matches. Some weeks later a vial containing a solution of Peter's DNA turned up at Michael's home.

DNA boosters

Companies that perform genome scans use DNA "chips" that test for the presence of hundreds of thousands of DNA variants known as single nucleotide polymorphisms, or SNPs - some of which have been associated with susceptibility to various diseases. As these chips require more DNA than came from our drinking glass, Michael's next challenge was to duplicate Peter's DNA to get a large enough sample.

This procedure, called "whole genome amplification", is offered to scientists and could, for instance, be used to amplify DNA from small clinical samples in studies investigating the genetic origins of disease. Geneticists often place orders involving large numbers of samples, but Michael found a lab services firm that was willing to amplify our single sample to produce more than enough DNA to run on a SNP chip. He did not say why he wanted this done.

Next we had to choose a company to perform the genome scan itself. Lab services companies, such as the one that performed our amplification, often offer this service to scientists as well. But they do not provide an interpretation of the scans in terms of health risks and other traits - something a genome hacker is likely to want. So this wasn't our first port of call. Instead, we looked at the personal genomics services offered to members of the public by companies such as Decode Genetics of Reykjavik, Iceland, and the Californian firms 23andMe of Mountain View and Navigenics, based in Foster City.

Swab spiker

To gather the DNA provided by their customers, 23andMe and Navigenics use a collection tube into which you must spit about 2 millilitres of saliva. We decided that it would be hard to convert Peter's amplified DNA sample into a form that closely mimicked saliva. So we chose to use Decode's service, branded deCODEme, which instead collects DNA using swabs consisting of a piece of filter paper on a plastic handle that customers are supposed to rub against the inside of their cheek. We reasoned that Michael might be able to "spike" these swabs with Peter's amplified DNA without Decode noticing.

The terms and conditions for the deCODEme service state that someone submitting DNA must have the legal authority to do so, and that the sample must be taken from the cheek. We wanted to test whether deCODEme is vulnerable to abuse from someone prepared to ignore these terms, so Michael pipetted some of Peter's DNA onto deCODEme's swabs and sent them off for analysis under his own name. As far as Decode was concerned, it was a sample of Michael's DNA taken by swabbing his own cheek.

This is when we hit our only real obstacle. A few weeks later, Michael was told that the sample had not processed successfully. This is possibly because Decode uses a chip that isn't designed to work with amplified DNA.

We had two contingency plans, however. First, Michael contacted our original lab services company again and asked it to analyse the remainder of our amplified sample using a different type of chip to the one that Decode uses. This company also has terms and conditions specifying that customers must have the necessary consents and approvals to submit samples. Mimicking a hacker who would be willing to ignore these terms, Michael submitted the amplified DNA for scanning.

Second, we made use of the replacement cheek swabs sent to deCODEme customers when a sample fails to process. We wanted to test the swabs' vulnerability to being spiked with a different source of "abandoned" DNA that might be taken by a genome hacker - semen from a used condom. Peter sealed

the replacement swabs, spiked with his semen, in an envelope, which Michael sent back to Decode.

Both of these back-up plans worked. For the sample of DNA taken from the drinking glass and analysed by the lab services company we obtained a read-out of about a million of Peter's SNPs. To interpret this information, we used a computer program called Promethease, which can be downloaded for free from the genomics website SNPedia.com.

SNPedia contains information contributed by genomics enthusiasts on the diseases and traits linked to particular SNPs, mostly drawn from scientific papers. Promethease is a tool intended for legitimate customers of personal genomics companies that takes the raw data from an individual's genome scan and relates it to the information in SNPedia, highlighting those SNPs that seem to reveal the most interesting things about the person concerned.

For the semen sample submitted to Decode, we obtained the company's own interpretation of Peter's lifetime risks of developing a range of diseases, in addition to a full download of the raw data, again documenting about a million SNPs.

So what would a hacker who had taken Peter's DNA have learned about him? For the DNA taken from the drinking glass, Promethease highlighted a range of SNPs, including those conferring increased risks of baldness, the skin disease psoriasis, and a form of blindness called exfoliation glaucoma. Decode's interpretation of the semen sample was rather different. For instance, it decided from an analysis of eight different SNPs that Peter's risk of developing psoriasis is very low (see table). And while Promethease and Decode both concluded that Peter is more likely than a typical person to develop Alzheimer's disease, they disagreed on the size of his risk (see "A short-lived Alzheimer's scare").

In part, these confusing results reflect current limits to geneticists' knowledge of how individual variations in DNA sequences influence health. But the science is advancing quickly, so there is no room for complacency about the ease with which a genome can be hacked.

Motives for such hacking are not hard to find. In the wake of the US presidential election, Robert Green and George Annas of Boston University speculated that future campaigns could be blighted by the sneaky analysis of a candidate's DNA by political opponents who hope to reveal looming health problems (*The New England Journal of Medicine*, vol 359, p 2192).

For people who are not politicians or celebrities, the most obvious threat comes from unscrupulous employers or insurers - and many countries have already restricted their use of genetic information. But private citizens may also have motives to pry into one another's DNA. A newly engaged person might want to know whether their future spouse carries genes making them vulnerable to dementia, for example. Or a childless couple could simply wipe a dribbling baby's mouth to investigate the child's genetic heritage and traits before deciding whether to adopt.

> An engaged person might want to know if their future spouse is vulnerable to dementia

Cost is not a huge obstacle, as the sums we spent would not deter a wealthy snoop. Decode's analysis of Peter's semen cost $985, while the total price for extracting his DNA from a drinking glass and then getting it amplified and analysed by the lab services company was about $1700. Genomic analysis is only going to get cheaper, and more powerful. "The plummeting costs of genome profiling and sequencing make it all too tempting to snoop around in other people's genomes," says Hudson.

Still, the results of our investigation suggest steps that companies could take to help protect people's privacy, and *New Scientist* has informed firms that run SNP analyses of our findings.

For companies selling genetic analyses to the public, verifying the origin of samples will always be difficult unless sample collection is supervised by a medical professional or some other official witness. It is possible to run lab tests that distinguish saliva and swabs taken from inside the cheek from other biological samples, however.

Companies offering services to research scientists, meanwhile, might consider running some checks to try to confirm that customers are legitimate. Such checks may not be completely hacker-proof, but had Michael been asked for evidence of affiliation to a scientific institution, he would not have been able to provide it legitimately.

Following our investigation, the company that amplified and analysed the sample from the drinking glass is now considering whether it could introduce further checks without obstructing legitimate orders. "Clearly we do not want to process samples where the proper consent has not been obtained," says the firm's operations director. "It's a question of how to achieve that goal without impeding the research of legitimate scientists."

Thwarting genome hackers may also require new laws to protect privacy. One approach would be for other countries to follow the UK, which has made it a crime to have someone else's DNA with the intent of analysing it without consent. "Although we are not aware of any instances of this in personal genome analysis, there is a clear rationale for making it illegal to analyse an individual's DNA without their knowledge and consent," says Decode spokesman Edward Farmer. Such laws are difficult to enforce, however, as an earlier *New Scientist* investigation revealed (31 January, p 6).

Another approach, which could be tried in parallel, would be to make it illegal for companies to extract and analyse DNA left on everyday items, except under specific circumstances. "There's no good reason, unless you are a police officer investigating a crime, to be doing DNA analysis on a sample from a drinking glass," argues Mark Rothstein, director of the Institute for Bioethics, Health Policy and Law at the University of Louisville in Kentucky.

One thing is clear: if lawmakers fail to rise to the challenge posed by genome hacking, we all have reason to fear for the security of our DNA.

Editorial: *Time for laws on genome spies*

A short-lived alzheimer's scare

We have shown that a genome hacker could take someone's DNA and obtain scans that reveal their risks of certain diseases (see main story). But how accurate are these scans, and how meaningful are the interpretations drawn from them?

To get an idea, we compared the scan results for three samples of DNA taken from our reporter Peter Aldhous. One scan was obtained legitimately by Peter submitting a sample of his saliva to the personal genomics firm 23andMe; the other two were from simulated genome "hacks". The first of these hacked samples was semen from a condom, submitted to a rival service provided by Decode Genetics; the second consisted of DNA extracted from a drinking glass, which was then amplified and scanned by a lab services company.

The raw data from these scans, which document DNA variants known as SNPs, were reasonably consistent, according to an analysis performed for *New Scientist* by Kevin Jacobs, who runs Bioinformed Consulting Services in Gaithersburg, Maryland.

The raw data for the hacked semen sample were the same as for the legitimate saliva control for 99.996 per cent of the SNPs recorded in both cases. Meanwhile, the SNP data for the DNA taken from the drinking glass diverged a little from the results coming from the semen sample and the control, agreeing about 93 per cent of the time in each case. Why the glass sample gave slightly different results is unclear, but it might be due to degradation or contamination of the DNA, or artefacts introduced during its amplification.

Interpretations of the raw SNP data varied much more widely, however (see table). Most confusing - and initially rather scary - were the suggestions about Peter's risk of developing Alzheimer's disease.

Look again

Alzheimer's risk is determined partly by variants of a gene called *APOE*. 23andMe provides no information on these variants, and for the other two samples we received conflicting interpretations.

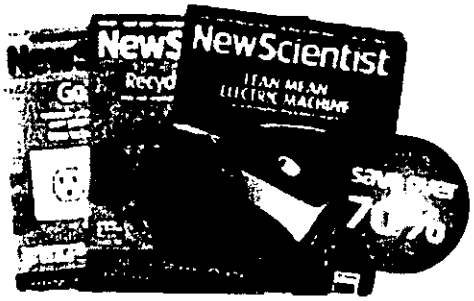
For the DNA sample taken from the drinking glass, the software that we used to interpret the scan, called Promethease, highlighted a rare form of one SNP, which nestles close to *APOE* and tends to be inherited along with two copies of the risky variant of the gene, known as epsilon 4. Based on this, Promethease suggested Peter's risk of developing Alzheimer's disease was between 15 and 25 times that of an average person.

It all seemed very worrying, until we looked at Decode's analysis. The raw data confirmed that Peter does carry this rare SNP, but Decode does not assess *APOE* in the indirect way that Promethease does. Instead, it analyses two SNPs in the *APOE* gene itself that define how many copies of the risky variant are actually present. This revealed that Peter has just one copy of epsilon 4, and one of the common variant, epsilon 3. On this basis, Decode concluded that he is only twice as likely to develop Alzheimer's as a typical person - a moderate risk that Peter shares with about 1 in 5 people of European descent.

So while the raw data from genome scans - legitimately obtained or not - are reasonably accurate, determining what they mean is another matter entirely.

Back to article

PRINT SEND SHARE



Fingerprinting program threatens privacy for CPAs, accountants

By Jason Giaimo
Publication Date: 04/27/08

Accountants and certified public accountants are in an uproar over a new program instituted by the American Institute of Certified Public Accountants that forces those seeking certification to be fingerprinted.

Worse still, fingerprints will be stored by a soon-to-be foreign corporation.

For the first time in its 121-year history, the venerable American Institute of Certified Public Accountants (AICPA) is forcing examinees across the country to either submit to being fingerprinted or be barred from the exam process, regardless of other identification presented.

Accountants should think twice before taking the CPA exam until this program is rescinded. I am challenging the national accounting board over its new forced fingerprint collection program, and I am far from alone.

We have surrendered enough of our privacy. This illogical, un-American and Orwellian obsession with collecting innocent people's fingerprints must end now.

It's hard to understand the business case for this type of application. I offered to show my U.S. passport, driver's license, social security card, even my original birth certificate, but was still barred from completing my remaining CPA exams due to "insufficient identification." I was two days away from completion when the new program went into effect.

How can a passport be sufficient identification to travel the world and enter the USA, but not to sit for the CPA exam? This is clearly not about identification, but about data collection. It's shameful and it needs to stop.

CPAs across the nation, including the Alaska State Board of Accountancy, staunchly oppose the new national forced fingerprinting program. The AICPA has agreed to put the program on the agenda for review at its May 19 national meeting, according to national accounting board official Pat Hartman.

The Institute of Management Accountants (IMA), another group that offers certifications, said it does not plan to require fingerprinting for their exams.

Some believe fingerprints are necessary for identity validation. Others say it's too risky. Risky indeed.

According to the National Association of State Boards of Accountancy executives, the new CPA fingerprint database will be stored by ChoicePoint Corp., the same data broker that was recently fined a whopping $15 million

by the Federal Trade Commission - the largest civil penalty in FTC history - for "making false and misleading statements about its privacy policies, violating consumer's privacy rights, and for violating numerous federal laws," according to the FTC Web site.

ChoicePoint was also accused of selling highly confidential financial information to Nigerians involved in crime operation.

Currently, the company maintains more than 17 billion records of individuals and businesses, which it sells to an estimated 100,000 clients, including the Department of Homeland Security, law enforcement agencies and the FBI. Worse still, ChoicePoint recently announced that it is being acquired by foreign corporation ReedElsevier, which privacy advocates maintain will make it even less subject to U.S. regulatory and legal control.

Why should innocent Americans object to having their fingerprints taken?

When you submit to being fingerprinted for "routine" background checks, your prints are compared against the FBI's database of more than 55 million sets of fingerprints, and then (supposedly) purged.

However, according to a Dec. 23, 2007, article in the Washington Post, the FBI is initiating a new program called "rap-back," which will allow the FBI to retain and add the fingerprints from "routine" background checks on innocent Americans to their massive tracking database.

Your fingerprints will then be subject to "electronic line-ups" whenever the law enforcement database is queried for terrorism, murder or other criminal activities.

Mistakes do happen. People have been falsely imprisoned by errors in fingerprint matching. Just Google U.S. attorney Brandon Mayfield for one such example. His prints initially came back a "100 percent perfect match" to a terrorist bombing, according to FBI fingerprint experts.

I remain an optimist. The AICPA is responsive to public comment and has top-notch leadership. While this unfortunate misstep puts CPAs at risk and hurts the profession, I'm confident the organization will rectify the situation by shutting down this program at its May 19 meeting. My hope is that the public and CPAs will e-mail the AICPA to share their views about this program.

The e-mail addresses of key AICPA/NASBA executives can be found on my Web site at www.NetGainConsultants.com or on the AICPA's site at www.aicpa.org.

Jason Giaimo is a privacy rights advocate and the owner of Net Gain Business Consultants, a professional business and accounting consulting firm, that operates in Alaska, California and New York.
Click here to return to story:
http://www.alaskajournal.com/stories/042708/hom_20080427039.shtml

ELECTRONIC FRONTIER FOUNDATION

Biometrics: Who's Watching You?

Introduction

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

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

What Are Biometrics?

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

Our Major Concerns

- **Biometric technology is inherently individuating and interfaces easily to database technology, making privacy violations easier and more damaging.** If we are to deploy such systems, privacy must be designed into them from the beginning, as it is hard to retrofit complex systems for privacy.
- **Biometric systems are useless without a well-considered threat model.** Before deploying any such system on the national stage, we must have a realistic threat model, specifying the categories of people such systems are supposed to target, and the threat they pose in light of their abilities, resources, motivations and goals. Any such system will also need to map out clearly in advance how the system is to work, in both in its successes and in its failures.
- **Biometrics are no substitute for quality data about potential risks**. No matter how accurately a person is identified, identification alone reveals nothing about whether a person is a terrorist. Such information is completely external to any biometric ID system.
- **Biometric identification is only as good as the initial ID.** The quality of the initial "enrollment" or "registration" is crucial. Biometric systems are only as good as the initial identification, which in any foreseeable system will be based on exactly the document-based methods of identification upon which biometrics are supposed to be an improvement. A terrorist with a fake passport would be issued a US visa with his own biometric attached to the name on the phony passport. Unless the terrorist A) has already entered his biometrics into the database, and B) has garnered enough suspicion at the border to merit a full database search, biometrics won't stop him at the border.
- **Biometric identification is often overkill for the task at hand.** It is not necessary to identify a person (and to create a record of their presence at a certain place and time) if all you really want to know is whether they're entitled to do something or be somewhere. When in a bar, customers use IDs to prove they're old enough to drink, not to prove who they are, or to create a record of their presence.
- **Some biometric technologies are discriminatory.**A nontrivial percentage of the population cannot present suitable features to participate in certain biometric systems. Many people have fingers that

simply do not "print well." Even if people with "bad prints" represent 1% of the population, this would mean massive inconvenience and suspicion for that minority. And scale matters. The INS, for example, handles about 1 billion distinct entries and exits every year. Even a seemingly low error rate of 0.1% means 1 million errors, each of which translates to INS resources lost following a false lead.

- **Biometric systems' accuracy is impossible to assess before deployment** Accuracy and error rates published by biometric technology vendors are not trustworthy, as biometric error rates are intrinsically manipulable. Biometric systems fail in two ways: false match (incorrectly matching a subject with someone else's reference sample) and false non-match (failing to match a subject with her own reference sample). There's a trade-off between these two types of error, and biometric systems may be "tuned" to favor one error type over another. When subjected to real-world testing in the proposed operating environment, biometric systems frequently fall short of the performance promised by vendors.
- **The cost of failure is high.** If you lose a credit card, you can cancel it and get a new one. If you lose a biometric, you've lost it for life. Any biometric system must be built to the highest levels of data security, including transmission that prevents interception, storage that prevents theft, and system-wide architecture to prevent both intrusion and compromise by corrupt or deceitful agents within the organization.

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

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

Some Current Biometric Initiatives

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

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

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

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

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

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

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

EFF's concerns about biometrics

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

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

Surveillance

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

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

Databases

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

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

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

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

what the scanner does and how the captured information will be used.

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

Linking

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

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

Tracking

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

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

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

Implemented improperly, biometric systems could:

- increase the visibility of individual behavior. This makes it easier for measures to be taken against individuals by agents of the government, by corporations, and by our peers.
- result in politically damaging and personally embarrassing disclosures, blackmail and extortion. This hurts democracy, because it reduces the willingness of competent people to participate in public life.
- increase the 'circumstantial evidence' available for criminal prosecution. This might dramatically affect the existing balance of plausible-sounding evidence available to prosecutors, and hence increase the incidence of wrongful conviction. Many criminal cases are decided by plea bargaining, a process that is sensitive to the perceived quality of evidence. Even ambiguous or spurious evidence generated by complex technical systems may be difficult for overburdened public defenders to challenge.
- enable the matching of people's behavior against pre-determined patterns. This could be used by the government to generate suspicion, or by the private sector to classify individuals into micro-markets, the better to manipulate consumer behavior.
- aid in repressing readily locatable and trackable individuals. While the public's concern is usually focused

on the exercise of state power, these technologies may also greatly empower corporations. If proper privacy safeguards are not constructed into such systems, they would prove useful in dealing with such troublesome opponents as competitors, regulators, union organizers, whistleblowers, and lobbyists, as well as employees, consumer activists, customers and suppliers.

The Attributes of Biometric Systems

How Do Biometrics Compare to Other Types of ID?

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

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

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

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

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

Functions of Biometric Systems

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

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

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

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

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

Common Aspects of All Biometric Systems:

All biometric technology systems have certain aspects in common. All are dependent upon an accurate reference or "registration" sample. If a biometric system is to identify a person, it first must have this sample,

positively linked to the subject, to compare against. Modern biometric identification systems, based on digital technology, analyze personal physical attributes at the time of registration and distill them into a series of numbers. Once this reference sample is in the system, future attempts to identify a person are based on a comparison of a "live" sample and the reference sample or samples.

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

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

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

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

Types of Biometrics

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

Signature

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

same speed, and with the same pen weight, as his victim.

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

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

Keystroke Dynamics

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

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

Hand Geometry

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

In deployment, traditional hand geometry systems have found acceptance in applications requiring verification of an identity, rather than a full proof or establishment of an identity. Airports, prisons, and factories have successfully employed hand-geometry-based systems to restrict access to runways, to prevent walk-out escapes during visits, and to ensure that time cards are being punched only by the worker, and not by that

worker's pal on his or her behalf. In all these instances, the subject is attempting to prove or disprove his or her membership in a relatively small group of people (authorized runway personnel, prisoners/visiting family, factory workers). When stakes are high, these systems are not relied on exclusively to confirm identity; rather, they are used to provide an additional layer of security above and beyond that provided by existing security systems.

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

Fingerprint

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

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

Facial Recognition

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

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

Eye biometrics: Iris/Retina

The human eye offers two features with excellent properties for identification. Both the iris (the colored part visible at the front of the eye) and the veins of the retina (the thin film of nerve endings inside the eyeball that capture light and send it back to your brain) provide patterns that can uniquely identify an individual. Retinal scanning is the older technology, and requires the subject to look into a reticle and focus on a visible target

while the scan is completed. It's definitely one of the more intrusive biometric technologies, with some subjects reporting discomfort at the scanning method. Iris recognition has an advantage in ease of use, in that it merely requires the subject to look at a camera from a distance of three to ten inches. The iris scanner illuminates the iris with invisible infra-red light, which shows details on darker-colored eyes that are not visible to the naked eye. The pattern of lines and colors on the eye are, as with other biometrics, analyzed, digitized, and compared against a reference sample for verification.

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

Voice Verification

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

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

Characterizing Different Biometrics

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

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

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

> *"Fingerprints are extremely distinctive, but not very robust, sitting at the very end of the major appendages you use to explore the world. Damaging your fingerprints requires less than a minute of exposure to household cleaning chemicals. Many people have chronically dry skin and cannot present clear prints. Hands are very robust, but not very distinctive. To change your hand geometry, you'd have to hit your hand very hard with a hammer. However, many people (somewhat less than 1 in 100) have hands much like yours, so hand geometry is not very distinctive. Hands are easily presented without much training required, but most people initially misjudge the location of their fingerprints,*

assuming them to be on the tips of the fingers. Both methods require some "real-time" feedback to the user regarding proper presentation. Both fingerprints and the hand are accessible, being easily presented. In the 1990 Orkand study, only 8% of customers at Department of Motor Vehicle offices who had just used a biometric device agreed that electronic fingerprinting "invades your privacy." Summarizing the results of a lengthy survey, the study rated the public acceptance of electronic fingerprinting at 96%. To our knowledge, there is no comparable polling of users regarding hand geometry, but we hypothesize that the figures would not be too different. With regard to availability, our studies have shown that a person can present at least 6 nearly-independent fingerprints, but only one hand geometry (your left hand may be a near mirror image of your right)."*

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

Characterizing Biometric Applications

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

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

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

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

Characterizing Biometric ID Systems

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

- **Data collection** Biometric systems involve at least two discrete data collection steps. First, any biometric system must contain a biometric characteristic deemed "true" or canonical from the system's viewpoint. The term "enrollment" or "registration" refers to the first entry of biometric data into the database. Second, the system must compare a later-submitted "sample" (often called a "live sample") to the sample in the database. (Scale is crucial to the enrollment step, sometimes for quite mundane reasons. In the context of biometric visa issuance by the State Department, for instance, the government has been looking at whether or not U.S. consulates around the world have room to handle the additional equipment and physical traffic needed for data collection.)
- **Transmission** Many biometric systems collect data at one location but store and/or process it at another. Such systems require data transmission.
- **Signal processing** Once a biometric is acquired, it must be prepared for comparison. There are three basic tasks here: feature extraction, quality control, and pattern matching. A fourth task in large-scale systems is pattern classification.
    - *Feature extraction* involves finding the true biometric pattern amid noise and signal degradation, preserving the critical information, and discarding redundant or unnecessary data. Dr. Wayman gives the example of a text-independent speaker-recognition system. A properly implemented system isolates "features that depend only on the speaker and not on the words being spoken." At the same time, the system focuses on features that do not change "even if the speaker has a cold or is not speaking directly into the microphone."
    - *Quality control* involves checking to see if the signal is of good quality. Ideally, it should be possible to make a quick determination so that another measure can be taken if the signal is inadequate.
    - *Pattern matching* involves comparing the live sample to the reference sample in the database. If the user claims to be Jane Doe, the pattern-matching process may only need to compare the sample to Jane Doe's stored template. In other situations, the sample must be compared to multiple templates. The pattern-matching process generates a quantitative "distance" measure of the comparison -- how close are they? Even for the same person, the distance is rarely if ever zero.
    - *Pattern classification* is a technique aimed at reducing the computational overhead of pattern matching. In large-scale systems, it can be computationally taxing to match each sample against all stored templates in the database. If biometric patterns can be categorized, then it may be possible to perform the match against only the stored templates in that category. This is sometimes referred to as "binning." A different technique with the same goal is "filtering," which involves partitioning the database based on information not contained in the biometric itself. If you know the person is a man, you don't need to check against women's biometrics. Both of these techniques introduce additional error possibilities; if binning or filtering is erroneous, then the true template is not used and a false non-match results.
- **Decision** This subsystem implements the biometric ID system's actual policy with regard to matching. In general, lowering the number of false non-matches raises the number of false matches, and vice versa. The signal processing subsystem yields a quantitative "distance" measure, but "how close or far is enough?" is a matter of policy. In a high-security application where the cost of a false acceptance could be high, system policy might prefer very few false acceptances and many more false rejections. In a commercial setting where the cost of a false acceptance could be small and treated as a cost of doing business, system policy might favor false acceptances in order not to falsely reject and thereby inconvenience large numbers of legitimate customers. The inevitable existence of these errors means that any biometric ID system must also have well-designed policies for exception handling.
- **Storage** Biometric reference samples must be stored somewhere for matching purposes. For systems only performing "one-to-one" matching, the database may be distributed on cards carried by each enrolled user. The user simply presents his or her biometric and the system checks to see if it matches

the template stored on the card. Depending upon system policy, no central database need exist, although in this application a centralized database can be used to detect counterfeit cards or to reissue lost cards without re-collecting the biometric pattern.

In other cases, centralized storage is necessary because the system must match the live sample to multiple templates. As the number of templates grows, speed becomes an increasingly significant issue. One technique is to partition the database (i.e., binning or filtering) so that any sample need only be matched to the templates in one partition. This increases system speed and decreases false matches at the expense of increasing the false non-match rate owing to partitioning errors. System error rates thus change with increasing database size and ID systems do not linearly scale.

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

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

The State of Scientific Testing of Biometric ID Systems

According to Dr. Wayman,

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

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

Media Coverage/Resources

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

Acknowledgements:

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

ALASKA STATE LEGISLATURE

Session
State Capitol, Rm. 115
Juneau, AK 99801
(907) 465-2435
Fax: (907) 465-6615

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

Senator_Bill_Wielechowski@legis.state.ak.us

Co-chair
Joint Armed Services Committee
Resources Committee

Member
Energy Committee
Judiciary Committee
World Trade Committee

SENATOR BILL WIELECHOWSKI

TO: Senator Hollis French, Chair
Senate Judicary Committee

FROM: Senator Bill Wielechowski

RE: Hearing Request for SB 190

Dear Senator French:

I respectfully ask that you schedule a hearing for **SB 190 – "An Act relating to biometric information"** in the Senate Judiciary Committee.

I intend to request that representatives from the appropriate state agencies and from legislative legal services be present to respond to any questions that may arise. Further, I would like to allow public testimony to be taken statewide by electronic means.

Please feel free to contact my aide George Ascott at 465-2435 with any questions or concerns.

Thank you for your consideration of this request.

1711

Illinois Compiled Statutes

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

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

CIVIL LIABILITIES
(740 ILCS 14/) Biometric Information Privacy Act.

(740 ILCS 14/1)
Sec. 1. Short title. This Act may be cited as the Biometric Information Privacy Act.
(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/5)
Sec. 5. Legislative findings; intent. The General Assembly finds all of the following:
(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.
(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.
(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.
(d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.
(e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.
(f) The full ramifications of biometric technology are not fully known.
(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.
(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/10)

Sec. 10. Definitions. In this Act:

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

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

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

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

"Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.

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

(740 ILCS 14/15)

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

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information

has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(740 ILCS 14/20)

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

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

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

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

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

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

(740 ILCS 14/25)

Sec. 25. Construction.

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

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

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

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

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

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

(740 ILCS 14/30)

Sec. 30. (Repealed).

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

(740 ILCS 14/99)

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

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

Top