Walter Hamilton Response to Questions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Biometrics should be used to:

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

Certain uses of biometric technology can raise worrisome privacy concerns. For example, it is now technically possible to "mine" the Internet using web crawler software to collect and build a repository of tagged facial images without a person's knowledge or consent. These images can then be processed into biometric "faceprints" and searched at high speed to look for matches. Association of these matched faceprints with their tagged biographical information can assist in building a complete profile of a person that could be used for cyber voyeurism or to steal one's identity. IBIA has made recommendations to the Federal Trade Commission to address such concerns which have been appropriately raised by members of Congress.

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

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

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

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

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

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

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

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

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

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

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

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

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

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