

# LEGAL SERVICES

## DIVISION OF LEGAL AND RESEARCH SERVICES LEGISLATIVE AFFAIRS AGENCY STATE OF ALASKA

(907) 465-3867 or 465-2450  
FAX (907) 465-2029  
Mail Stop 3101


State Capitol  
Juneau, Alaska 99801-1182  
Deliveries to: 129 6th St., Rm. 329

### MEMORANDUM

March 16, 2012

**SUBJECT:** Information regarding the handling of biometric information  
(CSSB 98(JUD); Work Order No. 27-LS0661 R )

**TO:** Representative Wes Keller  
Attn: Ernest Prax

**FROM:**  Terry Bannister  
Legislative Counsel

You have asked three questions about the regulation of biometric information. You have provided some documents about this subject. You have indicated that the context of this bill is SB 98. For the purposes of this memo, I am using "biometric information" in the sense of the measurement and analysis of human body characteristics. Under CSSB 98(JUD), "biometric data" means fingerprints, handprints, voices, facial mapping, iris images, retinal images, vein scans, hand geometry, or finger geometry.

Because of the scope of this request, this memo is limited to providing you with a general overview of the existing legal areas that appear to relate to your questions. Each of the items in this memo could be discussed in more detail, but I did not want to delay getting this to you. This memo does not address proposals for the handling of biometric data. If you need more information on a particular item, or if this memo does not discuss an item that you believe is significant, please contact me so that we can discuss the item.

1. What legal provisions are in place that may affect how biometric information is collected, stored, shared, and used by private sector entities?

#### A. Alaska statutes.

(1) Alaska Personal Information Protection Act (AS 45.48). The sections on breach of security involving personal information (AS 45.48.010 - 45.48.090) do not appear to cover biometric information because the definition of "personal information" in AS 45.48.090 does not contain a term that would cover biometric information. The sections on credit reports and credit score security freezes (AS 45.48.100 - 45.48.290) do not appear to cover biometric information, just credit reports. The sections on the protection of social security numbers (AS 45.48.400 - 45.48.480) apply only to social security numbers, not other personal information. The sections that regulate the disposal of records (AS 45.48.500 - 45.48.590) may arguably cover biometric information because the definition of "records" covers "material on which information that is written, drawn, spoken, visual, or electromagnetic is recorded or preserved," except publicly available

information. The sections allowing a factual declaration of innocence after identify theft (AS 45.48.600 - 45.48.670) arguably cover identify theft by using another person's biometric information, but the section is limited to correcting a criminal conviction. The section allowing the right to file a police report regarding identify theft (AS 45.48.680) arguably covers identity theft by using another person's biometric information, and allows an individual to report identity theft. The section on the truncation of card information (AS 45.48.750) only addresses card number digits and expiration dates.

(2) AS 06.01.028 (Depositor and customer records confidential). To the extent any biometric information is contained in depositor and customer records, this section would apply to prevent financial institutions that are subject to AS 06 from releasing them, but there are some exceptions. Under AS 06.01.050, this includes a commercial bank, savings bank, credit union, premium finance company, small loan company, bank holding company, financial holding company, trust company, savings and loan association, deferred deposit advance licensee under AS 06.50, and a licensee under AS 06.60. A financial institution that violates this section is liable to a depositor or customer for damages caused by the disclosure.

(3) Revised Alaska Trust Company Act. AS 06.26.610 makes trust company records relating to customers confidential, with exceptions. To the extent any biometric information is contained in those records, this section would apply to prevent their disclosure.

(4) State criminal offenses. It may be possible to use one or more of the following sections when a factual situation involves biometric information.

AS 11.46.180, theft (of property) by deception, and AS 11.46.190, theft by receiving (stolen property). The application to biometric information depends on how "property," as defined under AS 11.81.900, is interpreted and what factual situation is involved.

AS 11.46.200, theft of services. Covers computer access, so arguably covers access to biometric material on a computer or the use of biometric material to access a computer.

AS 11.46.600, scheme to defraud--by using false or fraudulent pretense, representation to obtain property or services. Arguably could cover using another person's biometric information to obtain property or services.

AS 11.46.740, criminal use of a computer. Broad provision relating to use of a computer to obtain a person's information, introducing false information to damage the information record of a person, and other situations. Arguably applies to obtaining or interfering, etc., with a person's biometric information contained in a computer under certain factual conditions.

(5) AS 45.50.471 - 45.50.561 (Alaska Unfair Trade Practices and Consumer Protection Act). Covers unfair trade practices, so arguably could cover, for example, misrepresentation caused by using false biometric information, or other misuse of

biometric information, by a seller or other entity in a commercial transaction. It may be possible to use this Act to remedy violations of the US-EU Safe Harbor Program by private businesses who participate in that program if the violations amount to misrepresentation of the adoption or use of the program principles. Both the state and private persons have remedies under the Act. There are exceptions to the coverage of the Act.

B. Federal statutes and executive orders.

(1) The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 - 3422). Protects the confidentiality of personal financial records contained in bank records. A financial record means any record held by a financial institution relating to a customer's relationship with the financial institution. So any biometric information contained in a customer's record at a financial institution would arguably be subject to the Act.

(2) Financial Modernization Act of 1999 (Gramm-Leach-Bliley Act) (15 U.S.C. 6801 - 6827). This Act regulates the disclosure of the financial information of the customers of financial institutions. The Act at 15 U.S.C. 6803 requires a financial institution to disclose its privacy policy for nonpublic personal information of the bank's customer, and the Act at 15 U.S.C. 6802 requires the financial institution to give the customer the opportunity to opt out of certain disclosures. The definition of "nonpublic personal information" provided at 15 U.S.C. 6809 is very broad and could arguably cover biometric information in a customer's file with the financial institution. Under 15 U.S.C. 6824, the Act allows for enforcement under state laws, if consistent with the Act, including state laws that provide greater protection.

(3) Federal Trade Commission Act (15 U.S.C. 41 - 58). As mentioned under the US-EU Safe Harbor Program later in this memo, this Act is being used to remedy violations of that program by private businesses who participate in that program.

(4) Fair Credit Protection Act (15 U.S.C. 1681 - 1681x). Governs consumer-reporting agencies, which are agencies that regularly engage in the practice of assembling or evaluating consumer information for the purpose of furnishing consumer reports to third parties. The Act sets restrictions on the disclosure of "medical information." The term could theoretically include biometric information, but is directed to the health or medical condition of an individual for credit purposes.

(5) Health Insurance Portability and Accountability Act of 1996: HIPAA Privacy Rule (45 C.F.R. Parts 160 and 164). Contains restrictions and requirements that "covered entities" (e.g., under 45 C.F.R. 160.103, a health care provider and a health plan) must follow to protect the security of an individual's health information. The Privacy Rule refers to the removal of "biometric identifiers," among other items, in one approach that it approves for making health information not individually identifiable. 45 C.F.R. 164.514(b)(2)(i)(P).

(6) Federal Trade Commission Fair Information Practice Principles. These principles are directed at the privacy of personal information involved in online transactions and they are voluntary. This personal information could theoretically include biometric information.

C. State constitutional provisions.

Article I, sec. 22. Explicit right to privacy. The primary purpose of this right to privacy is to protect the personal privacy of individuals from unwarranted intrusions by the government.<sup>1</sup> Therefore, unless there is some state action involved, this constitutional provision does not apply to the private sector's operations.

D. Federal constitutional provisions.

The federal constitutional provisions that might apply (e.g., the Fourth Amendment's search and seizure provisions and the the Fourteenth Amendment's due process provision) apply to governmental action and, unless some governmental connection can be proven, not to private sector operations. The case that you cited, Whalen v. Roe, 429 U.S. 589 (1977), involved a state statute, so any right to privacy arguably recognized by that case requires that there be some state or federal action involved. State action frequently is based on a statute. I am not aware that the state or federal supreme courts have at this time recognized a specific privacy right in biometric information.

E. International provisions.

US-EU Safe Harbor Program.<sup>2</sup> In light of the EU's privacy protections, this program was established to enable U.S. entities to satisfy the EU's privacy directive<sup>3</sup> ("Directive") and prevent U.S. entities from being shut out of the EU market because they had inadequate information protection. The program appears to cover biometric information because the Directive's definition appears to cover biometric information.<sup>4</sup>

---

<sup>1</sup> State v. Planned Parenthood of Alaska, 35 P.3d 30, 38 (Alaska 2001), cited by Miller v. Safeway, Inc., 102 P.3d 282, 288 (Alaska 2004).

<sup>2</sup> For an overview, see "[http://export.gov/safeharbor/eu/eg\\_main\\_018476.asp](http://export.gov/safeharbor/eu/eg_main_018476.asp)".

<sup>3</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as amended. (For text of the Directive, see "<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT>".)

<sup>4</sup> Directive, Chapter 1, Article 2(a): "(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;"

As part of their US-EU Safe Harbor program obligations, organizations are required to have in place a dispute resolution system that will investigate and resolve individual complaints and disputes and procedures for verifying compliance. They are also required to remedy problems arising out of a failure to comply with the principles. Sanctions that dispute resolution bodies can apply must be severe enough to ensure compliance by the organization; they must include publicity for findings.

The Federal Trade Commission and the U.S. Department of Transportation have both stated in letters to the European Commission that they will take enforcement action against organizations that state that they are in compliance with the US-EU Safe Harbor framework, but then fail to live up to their statements.

F. Privacy tort provisions.

At this time, there appear to be four general privacy torts recognized by courts. These are discussed in Section 652 of the Restatement (Second) of Torts. Section 652H discusses the damages that can be awarded for these torts. The use of each tort for biometric information depends on the factual situation involved in the particular case and whether that factual situation satisfies the specific requirements for the tort. The following descriptions of these torts give a general overview of the tort and do not provide all of the specific requirements for each.

(1) Unreasonable intrusion upon the seclusion of another. According to sec. 652B, this privacy tort can occur by intentionally intruding on another person's private affairs or concerns if the intrusion would be highly offensive. Only occurs when the intrusion is into a private place of the person. Theoretically, this could apply to biometric information obtained in this manner.

(2) Appropriation of another person's name or likeness. According to sec. 652C, this privacy tort involves the use of someone else's name or likeness for personal gain or benefit without the person's consent or other authorization. The theory behind this tort is the recognition that a person has the right to exclusively benefit from the person's own name and being. Theoretically, this privacy tort could apply to biometric information if a person uses the biometric information of another person in the person's business or to steal from the person, as in identity theft.

(3) Unreasonable publicity given to another person's private life. According to sec. 652D, this privacy tort involves publicly disclosing someone's private (non-public) personal information without consent or authorization. The dissemination of information contained in a public record, however, is not an actionable offense because the information is already rightfully in the public domain (e.g. a criminal or court record). Theoretically, this privacy tort may apply to biometric information that is not public information.

(4) Publicity that unreasonably places another person in a false light before the public. According to sec. 652E, this privacy tort involves intentionally or recklessly disseminating to the public information about a person that is both false and would be considered highly offensive to a reasonable person. Theoretically, this privacy tort could apply to biometric information if the biometric information of one person were used in some way to place the person in a false position in the public eye.

#### G. Misrepresentation tort provisions.

At this time there appear to be two misrepresentation torts recognized by the courts and discussed by the Restatement (Second) of Torts that may apply to biometric information. The first is intentional misrepresentation and the second is negligent misrepresentation.

(1) Fraudulent misrepresentation. According to sec. 525, this tort applies when a person fraudulently makes a misrepresentation to induce another person to act or refrain from acting in reliance on the misrepresentation. In your context, this tort might apply, for example, if a business misrepresents that the person has adopted the US-EU Safe Harbor program information privacy principles in order to obtain customers that provide biometric information to the business. This is just one possible application.

(2) Negligent misrepresentation. This tort covers information negligently supplied for the guidance of others. According to sec. 552, this tort applies when a person in the course of business, employment, or another transaction in which the person has a financial interest negligently supplies false information for the guidance of persons in their business transactions. The person is subject to liability for financial loss caused by the recipient's justifiable reliance on the information -- under certain conditions. In your context, this tort might apply, for example, if a business negligently provided incorrect biometric information to a person who relied on the information in the person's business, and that incorrect biometric information caused the person to suffer financial damages as a result.

#### H. Contractual approach.

If there is a contract that involves the taking, keeping, storing, etc., of biometric information, then a breach of that contract will make the person who breaches the contract liable for the damages resulting from the breach.

2. Are private entities that collect biometric information required to have a privacy policy or a terms of use agreement outlining how biometric information will be used, stored, shared, and disposed of? Are they required to notify a person submitting their biometric information? Could the private entity expose itself to legal action if it does not have a privacy policy or a terms of use agreement?

There does not appear to be any general governmental requirement in the U.S. that a company have a privacy policy specifically addressing the collection, use, storage, sharing, or disposition of biometric information. Of course, as indicated under

question 1, if biometric information occurs in a situation that is covered by a governmental confidentiality or regulatory requirement, then the private company will have to comply with that requirements. One example would be found in bank records that contain any biometric information (e.g., for account access or identification); in that case, both state and federal law regulate the sharing of those records.

As discussed earlier in this memo, a private business can enter into a voluntary agreement under the US-EU Safe Harbor Program if it wants to participate in the E.U. market and avoid violating the E.U.'s privacy laws. The US-EU Safe Harbor program is not directly enforceable by U.S. law. However, the Federal Trade Commission and the U.S. Department of Transportation have both stated in letters to the European Commission that they will take enforcement action against organizations that state that they are in compliance. In addition, as discussed under question 1, an intentional or negligent failure to comply with a policy so adopted by a company could expose the company to private or state or federal action for misrepresentation under unfair trade practices laws.

3. Are there existing guidelines that the State of Alaska must abide by regarding the collection and use of biometric information?

There are no express existing general guidelines for the state when it collects biometric information.

However, AS 12.62.160 and AS 12.64.010 provide fairly comprehensive confidentiality provisions for information that lands in the criminal justice system, including fingerprints. AS 12.62.160 exempts criminal justice information from disclosure under the state's public record disclosure requirements under AS 40.25. AS 12.64.010 enacts the National Crime Prevention and Privacy Compact. In general, this Compact organizes an electronic information sharing system among the federal government and the states to exchange criminal history records for noncriminal justice purposes authorized by federal or state law, such as background checks for governmental licensing and employment. One of the purposes of the Compact is to require the FBI and each state that is a party to the Compact to adhere to certain standards concerning record dissemination, use, response times, system security, and information quality, including the accuracy and privacy of such records. In the Compact, the definition of "positive identification" includes a reference to fingerprints and other biometric identification techniques.

Aside from criminal justice information, if a factual situation covers biometric information and falls within any of the confidentiality provisions salted throughout the statutes (or federal provisions that apply to the particular state action) those provisions may apply to the particular situation. In addition to other statutory provisions mentioned elsewhere in this memo, the following statutes provide examples of these confidentiality statutes.

AS 06.01.025 (Records of department). Under this section, the information in the records of the department obtained through the administration of AS 06 (Banks and Financial Institutions) is confidential, is not subject to subpoena, and may be revealed only with the

consent of the department. In the future, the information collected from financial institutions through state banking inspections could contain biometric information (e.g., a fingerprint for security or access purposes).

AS 06.55.407 (Confidentiality) (Alaska Uniform Money Services Act). This section is similar to AS 06.01.025, but applies only to persons engaging in providing money services.

AS 08.02.040 addresses the confidentiality of patient mental health records received under certain licensing chapters by the Department of Health and Social Services.

AS 12.65.015 and 12.65.140 provide the confidentiality requirements for state child fatality review teams.

Motor vehicle-related records. Under AS 28.15.151(f), the Department of Administration must maintain, with certain exceptions, the confidentiality of the records kept by the department relating to, e.g., driver's licenses and accident reports. This would, for example, cover facial images taken for drivers' licenses. Under AS 28.35.030(d), the department must maintain the confidentiality of records related to the treatment program ordered for operating a motor vehicle, aircraft, or watercraft while under the influence of, for example, alcohol. This would cover biometric information taken during those programs.

DNA Identification System. Under AS 44.41.035(f), the Department of Public Safety must keep the information in its DNA Identification System confidential. And AS 44.41.035(h) requires the adoption of reasonable procedures for the collection, use, storage, and expungement of the information in the system.

The provisions in AS 45.48.500 - 45.48.590 that regulate the disposal of records appear to cover biometric information because the definition of "records" covers "material on which information that is written, drawn, spoken, visual, or electromagnetic is recorded or preserved," except publicly available information. The sections apply to state governmental agencies, except the judicial branch.

If I may be of further assistance, please advise.

TLB:ljw  
12-208.ljw