Overcoming the Compliance Challenges of Biometrics

David Todd

Overcoming the Compliance Challenges of Biometrics

GIAC (GLEG) Gold Certification

Author: David L Todd, dtodd@mastersprogram.sans.edu
Advisor: *Benjamin Wright*

Accepted: 5/11/19

Abstract

Due to increased regulations designed to protect sensitive data such as personally identifiable information (PII) and protected health information (PHI), hospitals and other industries requiring improved data protections are starting to adopt biometrics. However, adoption has been slow within many of the industries that have suffered most of the breaches over the last several years. One reason adoption has been slow is that companies hesitate to implement biometrics across their organization without first understanding the vast complexities of the various state-by-state privacy regulations. By adopting a common biometrics compliance framework, this research will show how organizations can implement biometric solutions that comply with the overall spirit of the different state privacy and biometric regulations, enabling those companies to improve global data protections.

1. Introduction

Research on password limitations has been thoroughly documented over the last 20 years. Password length, password complexity, password timeouts, etc. have all been analyzed with various recommendations to strengthen a company's security posture. Biometrics can be described as authentication enhancers because they enhance the traditionally stored password controls, thereby mitigating the risk of many end-user workarounds. Most legacy applications still require the conventionally stored password. However, enabling biometrics as an alternative to the end-user having to recall and correctly type in a complex password can improve overall data protections. So why did one hotel management company's biometrics project end so abruptly following the initial kick-off?

The project's goal was to install fingerprint scanners on the front desk computers at five select Illinois and Indiana hotels. The purpose of the biometrics pilot was to improve overall security by eliminating the harmful practice of sharing passwords and to improve the guest's front desk experience by reducing computer lockouts by hotel personnel. Lockouts were a common occurrence since the organization established a complex twelve-character password for all employees. Key metrics from the pilot would be collected and analyzed to complete a compelling business case and eventual rollout of biometrics across the entire organization.

A biometrics vendor volunteered to donate several optical USB fingerprint readers for the pilot. These fingerprint readers and associated software would be installed at all front desk workstations at five hotels. Success would be measured in a documented Return on Investment (ROI) business case, evaluating key metrics to determine if authentication enhancers, such as biometrics devices can be more secure and more cost-effective than the traditional username and password approach. The ROI would compare historic IT Service Desk tickets at each participating property with ticket data from the pilot period. In addition, working with the hotel operations team, the business case would document improvements in the average wait time at the front desk. The Biometrics Implementation Team randomly selected hotels in Illinois and Indiana for the biometric pilot. On installing the new biometric fingerprint scanners at one of the Chicago locations, the third-party installer casually asked the IT team if the front desk

personnel had signed waivers authorizing the company to collect fingerprint data. General Counsel was immediately contacted for guidance because the IT Team was unaware of the need for a biometrics privacy waiver.

General Counsel informed the Biometrics Implementation Team that the state of Illinois has a regulation called the Biometrics Information Privacy Act of 2008, more commonly referred to as BIPA. The General Counsel ended up having more questions about biometrics than the Implementation Team had answers. The team had focused almost entirely on the technical aspects of installing and supporting a biometrics solution and little time understanding and documenting the legal requirements. After much debate, the team opted to put the entire project on hold until the biometric legal requirements could be recorded.

At present, there is "no comprehensive federal law specifically addressing an employer's obligations" (Gross Sholinsky & Steinmeyer, 2018) for managing biometric data. Therefore, this research will evaluate the legal and compliance regulations related to biometric implementations across three states in the U.S. The analysis includes a review of Illinois's Biometric Information Privacy Act (BIPA), Washington state's Biometric Privacy Law, and the Texas Biometric Privacy Act. In comparing the regulations, compliance requirements, reporting requirements, and penalties of the three laws, a common biometrics compliance framework is introduced. When the best-practices framework is implemented correctly, a company's biometric implementation across any of the 50 states should be legally defensible on completion.

2. Biometrics Maturity

The use of biometrics and biometric authentication methods has matured over the last century from primarily a law enforcement tool, which continues to this day, to a full array of solutions. Biometric technologies have expanded into such areas as smartphone/computer authentication, time and attendance clocks, customer loyalty programs, workforce management, patient tracking, financial services, driver identification, and registering blood donor records, to name a few examples (Waterson & Hoffman, 2019).

The World of Forensic Science encylopedia.com source on Fingerprint Analysis (Famous Cases) (2005) describes the early history of biometrics as follows:

> Notes about the ridges, loops, and spirals of fingerprints were first made in 1686 by Marcello Malpighi. However, it was not until 1880 that fingerprints were recognized as a means of personal identification by Henry Faulds, who also identified a first-ever fingerprint. The first book about fingerprints was published in 1888 by Sir Francis Galton, and was titled simply Fingerprints. Galton established the first classification system for fingerprints and was the first to assert that no two prints are the same, or that the odds of two prints being identical were about 1 in 64 billion.

Juan (Josip) Vucetich was also considered to be one of the earliest pioneers in fingerprint analysis. Vucetich was a Croatian-born Argentinean anthropologist and police investigator who was one of the front-runners of scientific dactyloscopy, or identification by fingerprints. In June 1882, a colleague of Vucetich was able to capture digital imprints left behind on a door post at a murder scene of two children. The mother denied any involvement and blamed the murder on her neighbor. Using the fingerprint data, the investigators confronted the mother with the fingerprint evidence, and the mother eventually confessed (Vucetich, Juan. World of Forensic Science 2005).

It wasn't until the late 1980s, and early 1990s before the science of biometrics finally became established in technology with the entry of the personal computer. As a result, "Computers were able to scan fingerprints and palm prints, and store images of those prints in automated identification databases" (*Fingerprint Analysis (Famous Cases)* 2005).

The history of corporate breaches demonstrates that password controls alone continue to fail despite guidance on improved password management techniques and password complexity enhancements. Security professionals and standards organizations (e.g., ISO, NIST, ISC2, etc.) continue to modify password complexity guidelines, password lengths, and password expiration timeframes only to continue to find that end-users discover workarounds. Enhancements to strengthen the traditional recall of stored passwords have been significantly explored using such improvements as biometrics, proximity devices, RFID (Radio Frequency Identification), facial recognition, and voice

recognition. Adding biometric solutions to existing password controls has become a cost-effective solution so that the process of end-user recall of passwords could finally be eliminated in the workplace.

3. Comparing Biometrics Regulations by State

Unlike personally identifiable information (PII) such as social security numbers and credit card numbers, which can be changed if compromised, biometric data is uniquely tied to an individual's "measurable human biological and behavioral characteristics" (Gross Sholinsky, 2018) and therefore cannot be realistically changed (Gross Sholinsky, 2018). However, biometric-specific legislation is limited throughout the U.S. If the law does exist, it is generally categorized as privacy-related legislation and not biometric-specific.

There are only a few states that have adopted biometric-specific legislation, including the states of Illinois, Texas, and Washington. However, many states have biometric privacy legislation pending, including Massachusetts, New York, Delaware, Alaska and Michigan (Shinabarger & Swanson, 2019). By comparing and contrasting the regulations, compliance requirements, reporting requirements, and penalties of the biometric laws in the three states where laws are already in place, we will build a foundation and understanding of the conditions that, when implemented, should be legally defensible regardless of state.

3.1. Illinois's Biometric Information Privacy Act (BIPA)

Signed into law in October 2008, the Illinois Biometric Information Privacy Act (BIPA) applies to a private entity's use of biometric data for any purpose. State or local government agencies are excluded from BIPA regulations. Even though the Illinois BIPA legislation is fewer than four pages long, it is the most comprehensive of the biometric privacy laws in the U.S. Illinois' BIPA is divided into four primary sections:

1. Legislative intent
2. Definitions
3. Retention, collection, disclosure, and destruction

4. Right of action

3.1.1. Legislative Intent

The Illinois General Assembly recognized that "biometrics is growing in the business and security screening sectors" ((740 ILCS 14/) Biometric Information Privacy Act 2008) and, therefore, felt it was time to provide some guidelines around its use. Unlike credit card data, the Illinois legislators understood that the owner of the biometric data, if compromised, has no recourse because of the nature of the biological uniqueness of the information collected. One can reissue a credit card if the data is compromised, but one cannot realistically change their fingerprint, retina, voice or facial features. With that being said, the BIPA legislation is both timely and essential to protect the "public welfare, security, and safety" ((740 ILCS 14/) Biometric Information Privacy Act 2008) of its residents.

3.1.2. Definitions

A common term used throughout the legislation is "biometric identifier," which means a fingerprint, retina or iris scan, voiceprint, or scan of the hand or the geometry of the face ((740 ILCS 14/) Biometric Information Privacy Act 2008). To be more explicit in the BIPA legislation, the Illinois General Assembly identified a long list of what is excluded as a biometric identifier:

- Writing samples
- Written signatures
- Photographs
- Human biological samples used for scientific testing
- Demographic data
- Tattoo descriptions
- Physical descriptions such as height, weight, hair color, or eye color
- Others ((740 ILCS 14/) Biometric Information Privacy Act 2008)

When implementing a biometrics solution in the U.S., one must understand what is included and not included as a biometric identifier, because each state has adopted

variations of the Illinois BIPA definition in their definitions. Per Illinois ((740 ILCS 14/) Biometric Information Privacy Act 2008, biometric information is:

> [A]ny 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.

The Illinois BIPA goes on to define confidential and sensitive information as "personal information that can be used to uniquely identify an individual or an individual's account or property" ((740 ILCS 14/) Biometric Information Privacy Act 2008). Examples of confidential and sensitive information include genetic testing, PINs, driver's license numbers, and social security numbers.

As previously mentioned, a private entity excludes all state and local government agencies, but does include "any individual, partnership, corporation, limited liability company, association, or other group, however organized" ((740 ILCS 14/) Biometric Information Privacy Act 2008). This is an important definition because it is broader than the entity definitions in both Texas and Washington.

One of the essential components of BIPA is related to the requirement of written consent. "With all of the new BIPA lawsuits working their way through the court system, one common question arose in virtually every case: can an employee pursue a claim under BIPA based merely on the failure to receive the requisite notice and consent document, even if the employee suffered no actual damages as a result of this violation?" (Clark & Walden, 2019). BIPA defines written release as "informed written consent or, in the context of employment, a release executed by an employee as a condition of employment" ((740 ILCS 14/) Biometric Information Privacy Act 2008).

3.1.3. Retention, Collection, Disclosure, and Destruction

A private entity that collects biometric identifiers or biometric information needs to develop a written policy that can be made available to the public on request. In the policy, the private entity needs to document its retention schedule and guidelines for permanently destroying any biometric identifiers and biometric information collected. If an individual's biometric data is not used within three years, the biometric information

must be permanently destroyed ((740 ILCS 14/) Biometric Information Privacy Act 2008).

As stipulated in the ((740 ILCS 14/) Biometric Information Privacy Act 2008 itself:

> *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.*

Also, ((740 ILCS 14/) Biometric Information Privacy Act 2008) stipulates that 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 how the private entity stores, transmits, and protects other confidential and sensitive information.*

3.1.4. Right of Action

BIPA provides for a private "right of action" that allows plaintiffs to recover from $1000 for negligent violations to $5,000 for the intentional or reckless violation, or actual damages for each violation. The right of action provides any person who feels aggrieved

by a violation of the Biometric Information Privacy Act to file a claim against the offending party in the Illinois circuit court or as a supplemental claim in federal district court ((740 ILCS 14/) Biometric Information Privacy Act 2008). Additional fees such as attorney fees, court costs, expert witness fees, and related fees may also be levied if deemed appropriate by the courts ((740 ILCS 14/) Biometric Information Privacy Act 2008).

3.2. Texas Biometric Privacy Act

In 2009 Texas passed the Biometric Privacy Act, which in comparison, is similar to the Illinois BIPA. The law firm of Garlo Ward, P.C. published an article titled *Texas Biometric Privacy Law restricts specific "biometric identifiers"* specifically addressing the topic of biometric identifiers in the Texas Biometric Privacy Act:

> Texas law applies only to biometric identifiers and defines those as specifically a retina or iris scan, fingerprint, voiceprint, the record of a hand or face geometry. It is important to note that it specifically includes the records of the specific biometric data and does not include the analysis of biometric indicators. As for penalties, reports indicate that the law allows for civil penalties of up to $25,000x, but only the attorney general can bring suit against companies for biometric privacy violations.

Like Illinois, the "biometric identifier" in Texas means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry. However, in Texas, the legislation does not stipulate exclusions from the list of “biometric identifiers.” The lack of clarity in defining exclusions will force attorneys to debate the finer points of the legislation in court.

The Texas act requires prior notice to the individual whose biometrics will be captured and requires the individual’s consent. The legislation does not stipulate what form constitutes “consent," but based on initial case law, the legislators intended for the permission to be in writing and not verbal.

Texas used the language “commercial purpose” to define what entities are obligated to abide by the Biometric Privacy Act legislation. Unfortunately, this act does not clearly define what it means by commercial purpose. “There are several restrictions on the use of biometric identifiers for commercial purposes. The law is silent as to

whether or not non-profit organizations or government agencies fall within the scope of commercial purposes" (Duran, 2017). Again, Texas continues to be vague in many areas, expecting the details to be resolved in court.

In the Texas Biometric Privacy Act, a person who possesses a biometric identifier of an individual that is captured for a commercial purpose:

> *(1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless: (A) the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death; (B) the disclosure completes a financial transaction that the individual requested or authorized; (C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code; or (D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant;*
>
> *(2) shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than how the person stores, transmits, and protects any other confidential information the person possesses; and*
>
> *(3) shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires, except as provided by Subsection (c-1)* (Texas, Capture or use of Biometric Identifier 2009).

3.3. Washington Biometric Privacy Law

After Illinois and Texas, Washington has become the third state to pass legislation regulating how businesses may use biometric information. Jay Inslee, the governor of Washington state, signed into law H.B. 1493 in May of 2017, making this legislation "Washington's first statute governing how individuals and non-government entities collect, use, and retain biometric identifiers" (Washington Becomes the Third State with a Biometric Law 2018). The same article goes on to state that "[t]he law prohibits any "person" from "enroll[ing] a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent

the subsequent use of a biometric identifier for a commercial purpose" (Washington Becomes the Third State with a Biometric Law 2018).

The law in Washington also places restrictions on the sale, lease, and other disclosures of biometric identifiers. Although Illinois, Texas, and Washington have similar protections, "the Washington law defines the content and activity it regulates in different terms… the Washington law does not provide a private right of action" (Washington Becomes the Third State with a Biometric Law 2018).

3.3.1. Overview of Washington House Bill 1493

The Washington state law oversees the collection, usage, and retention of "biometric identifiers." Biometric identifiers are defined as "data generated by automatic measurements of an individual's biological characteristics" (RCW 19.375 2017). The Washington law includes "fingerprints, voiceprints, eye retinas, irises, or other unique biological patterns or characteristics used to identify a specific individual" (RCW 19.375 2017). HB 1493 excludes both physical and digital photographs explicitly. Washington's definition of a biometric identifier is broader than the previous two states.

Another distinguishing factor to Washington's biometric act is the law states explicitly that it does not limit or govern using biometric technology for security reasons and defines "security purposes" as purposes to prevent the fraud or theft of anything of value, including "intangible goods." One form of fraud or theft is called "buddy punching." A buddy punch is when one employee clocks in for another employee who may be running late to work. According to a recent survey by the American Payroll Association, this wage theft practice affects nearly 75% of employers. The survey goes on to explain that employees on average steal 4.5 hours per week from their employers (Duran, Learn How Washington's New Biometric Privacy Law Affects Businesses 2019).

Beyond using time clocks or security measures, employers and other businesses who use biometrics for non-commercial purposes will still be able to use biometric identifiers (Duran, Learn How Washington's New Biometric Privacy Law Affects Businesses 2019).

3.4. Case Law / Precedent

When embarking on a biometrics implementation, it is important to consider both current law and legal precedent. The concept of legal precedent comes from the Latin stare decisis which means "to stand by that which is decided" (LII Staff, Stare Decisis 2017). It states, "Once a case is decided, it establishes a precedent, or a judicial decision that should be followed when a similar case comes to court" (Precedent and the Doctrine of Stare Decisis 2019). Legal precedent is particularly important in the ever-changing field of cybersecurity where laws are still in their infancy. "Stare decisis allows common law to develop gradually and incrementally" based on judges' rulings in other cases (Fernandez & Ponzetto, 2010). This makes it vital to consider legal precedent in addition to current laws. So, *stare decisis* is essentially "the rule of precedent" (Sholinsky & Steinmeyer, 2018).

As of February 2019, it is reported that the state of Illinois has "more than 200 (and climbing) class actions filed under the [Biometric Information Privacy Act] law in the past two years" (Shinabarger & Swanson, 2019). The Illinois Supreme Court recently issued a ruling in the case of *Rosenbach* v. *Six Flags* interpreting a key component of Illinois' Biometric Information Privacy Act (BIPA). The Supreme Court overturned the state appellate court's ruling, holding that Six Flags failed to "obtain proper consent or provide an appropriate disclosure" (Kim, 2019) when they collected a minor's fingerprint as a standard process in granting a season pass to the amusement park. The fact that the season ticket holder was a minor had little bearing on the case. Six Flags argued that the lawsuit was meritless since the plaintiff suffered no harm or actual damages. The court concluded that "a person need not have sustained actual damage, beyond violation of his or her rights under the Act, in order to bring action under it" (Kim, 2019). The courts ruling has consequences for all companies since the precedent has now been established that actual damages are not a required prerequisite to filing a lawsuit (Kim, 2019).

Both Facebook and Google, who have similar photo-tagging features, are facing lawsuits that they are violating the Illinois BIPA law since they are tagging faces on photographs and making recommendations to link those faces to particular people. BIPA explicitly exempts photographs in paragraph 740 ILCS 14/10 of the act where it lists the following biometric identifiers as not included: "writing samples, written signatures,

photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions…" ((740 ILCS 14/) Biometric Information Privacy Act 2008). As expected, Facebook is fighting the case and arguing the lawsuit is without merit and claiming the BIPA exclusions (Brandom, 2015).

Based on a review of the cases pending, most pending cases are in Illinois since BIPA is the most restrictive and comprehensive biometric legislation enacted. Washington state's biometric privacy law "has significant compliance obligations but lacks a right for consumers to sue" (Shukovsky, 2017). The Texas statute is similar to its Illinois BIPA counterpart, but it doesn't have a broader "biometric information" provision. However, the most significant difference is that Texas does not allow for a private right of action. In Texas, it's not a private individual, but the attorney general who must file suit to enforce the Texas Biometric Privacy Law. The attorney general can sue companies seeking up to $25,000 per violation (Duran, 2017).

4. Biometrics Compliance Framework Introduced

The Biometrics Compliance Framework (BCF) is derived directly from the relevant case law and regulations from the following three states analyzed: (1) the Illinois Biometric Information Privacy Act (BIPA); (2) the Texas Biometric Privacy Act; and (3) Washington state's Biometric Privacy Law. The BCF matrix highlights the specific biometric/privacy requirements and compares those requirements across the three states analyzed. When comparing the regulations, compliance requirements, reporting requirements, and penalties of the three laws, implementing the biometrics compliance framework, companies can implement their biometrics solutions and minimize legal risk.

Due diligence, an effective requirement gathering process, and specifically an inclusive process when identifying project stakeholders are strongly recommended before embarking upon a biometrics implementation. According to the Project Management Professional (PMP) Study Guide, "Stakeholders are those folks (or organizations) with a vested interest in your project" (Heldman, 2018). It may not be obvious to include Legal as a key stakeholder in a biometrics project, but doing so is critical to the success of a biometric-related project. In-house our outside legal counsel can provide specific guidance related to the various forms of biometrics being considered for your

implementation. In addition, each state has variations of requirements, and it may be necessary to modify your implementation plan.

The Biometrics Compliance Framework (BCF) is designed to pull into a single view the primary definitions and requirements for each state where specific biometrics laws are in place. In most cases, but not all, the Illinois BIPA is the most restrictive of the laws. BIPA is also the only state as of this writing that allows for a private "right of action", which means that "any person who feels they have been aggrieved by a violation of this act to file a claim against the offending party" ((740 ILCS 14/) Biometric Information Privacy Act 2008).

4.1. How to Use the Biometrics Compliance Framework

The Biometrics Compliance Framework (BCF) is divided into several categories to expedite the requirements gathering process:

- Definitions
- Legislative Intent
- Retention, Collection, Disclosure & Destruction
- Penalties & Fines

Each BCF definition and requirement are designated with a BCF ID or identification number. The definitions are primarily documented for reference purposes and can be pulled into a requirements document and listed as nonfunctional or potentially functional requirements. As defined in the PMP Study Guide, "Nonfunctional requirements are those that describe characteristics needed for the requirement to function, such as security needs, performance, and reliability" (Heldman, 2018). In this case, many legal requirements would be considered as nonfunctional requirements.

The BCF requirements in the two sections titled "Legislative Intent" and "Retention, Collection, Disclosure & Destruction," would both transfer over to the requirements document as "functional requirements." Using the PMP Study Guide again as a reference, "Functional requirements are those that describe how the product will perform" (Heldman, 2018).

The last section in the BCF titled "Penalties & Fines" can be used in the project risk register when identifying potential risk or in determining risk mitigation priorities.

Either way, having a clear understanding of the potential penalties and fines associated with a biometric project should help maintain focus on the details to ensure a smooth lawsuit-free implementation.

When evaluating each biometric requirement, refer to the BCF and review what the requirement is for all three states – Illinois (IL), Texas (TX), and Washington (WA). If all three states have the same requirement, then clearly that requirement should be included as a functional (or nonfunctional) requirement in your project requirements document. For those requirements where all three states are not in agreement, the requirement was not specified (N/S), or the state either implicitly or explicitly excluded a requirement, then those are areas where it is recommended that the legal stakeholder(s) get engaged to provide direction and clarification. In general, the conservative approach to best ensure that your organization implements a solution that complies with the overall spirit of the privacy legislation, it is recommended that the state with the most stringent/defined requirement be the requirement to adhere to during implementation.

To highlight a few examples of how to use the BCF:

EXAMPLE 1:

BCF 13: Written Release – *Informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.*

Project Team Recommendation: Written consent is clearly a specification in all three states and therefore should be documented as a requirement. Exactly how the consent should be worded is left up to interpretation, and legal counsel should be consulted.

EXAMPLE 2:

BCF 15: Consent Upon Death – *The individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death.*

Project Team Recommendation: In this example, both TX and WA provide for an individual to allow for disclosure of his/her identity in the event of one's disappearance or death. However, the state of IL provides no disclosure option – in fact, IL is entirely silent on the topic. Following the most conservative approach, the Written Consent Waiver should not allow for disclosure of one's identity in the case of death or disappearance. However, legal counsel should be consulted.

EXAMPLE 3:

BCF 17: Notification of Retention – *Requires notification to 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.*

Project Team Recommendation: IL specifies a notification requirement in writing regarding the retention term, but the requirement is not specified in TX or WA. Following the conservative approach and upon consulting with legal, the recommendation would be to implement this process regardless of state.

4.2. Biometrics Compliance Framework (BCF)

BCF ID	Requirement	Description	IL	TX	WA
		Definitions	Effective Oct 2008	Effective Sept 2009	Effective July 2017
BCF01	Biometric Identifiers	Data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns of characteristics that are used to identify a specific individual.	YES	YES	YES
BCF02	Biometric Information	Any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.	YES	N/S	N/S
BCF03	Biometric System	An automated identification system capable of capturing, processing, and storing a biometric identifier, comparing the biometric identifier to the one or more references, and matching the biometric identifier to a specific individual.	N/S	N/S	YES
BCF04	Commercial Purpose	A purpose in furthering the sale or disclosure to a third party of a biometric identifier for the marketing of goods or services when such goods or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier.	YES	YES	YES
BCF04.01	Commercial Purpose Exclusion	Commercial purpose does not include a security or law enforcement purpose. The purpose of preventing shoplifting, fraud, or any other misappropriation or theft of an item of value, including tangible and intangible goods, services, and other purposes in furtherance of protecting the security or integrity of software, accounts, applications, online services, or any person.	NO	NO	YES
BCF05	Confidential and Sensitive	Confidential and sensitive information means personal information that can be used to uniquely identify an individual or an individual's account or property.	YES	N/S	N/S
BCF06	Capture	The process of collecting a biometric identifier from an individual.	N/S	N/S	YES
BCF07	Enroll	To capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual.	N/S	N/S	YES
BCF08	Private Entity	Applies to a private entity's use of biometric data for any purpose and is an individual, partnership, corporation, limited liability company, association, or another group; however it is organized. A private entity does not include a state or local government agency.	YES	YES	YES
BCF09	Reasonable Care	Store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry.	YES	YES	YES
BCF10	Right of Action - Plaintiff	Allows recovery by plaintiffs - The right of action provides any person who feels they have been aggrieved by a violation of this act to file a claim against the offending party.	YES	NO	NO
BCF11	Right of Action - State Attorney General	Allows recovery by plaintiffs. The right of action provides any person who feels they have been aggrieved by a violation of this Act to file a claim against the offending party.	NO	YES	YES
BCF12	State & Local Agencies	Applies to state or local government agencies' use of biometric data for any purpose.	NO	YES	YES
BCF13	Written Release	Informed written consent or, in the context of employment, a release executed by an employee as a condition of employment. If the biometric identifier is that of a minor, it is strongly recommended that written consent also be obtained by a parent or legal guardian (refer to case Rosenbach v. Six Flags).	YES	YES	YES

BCF ID	Requirement	Description	IL	TX	WA
		Legislative Intent			
BCF14	Biometric Identifiers	Data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns of characteristics used to identify a specific person.			
BCF14.01		Retina	YES	YES	YES
BCF14.02		Iris Scan	YES	YES	YES
BCF14.03		Fingerprint	YES	YES	YES
BCF14.04		Voiceprint	YES	YES	YES
BCF14.05		Record/Scan of hand	YES	YES	N/S
BCF14.06		Record/Scan of face geometry	YES	YES	N/S
BCF14.07		Or other unique biological patterns or characteristics that is used to identify a specific individual	N/S	N/S	YES
BCF14.07		Writing samples	NO	N/S	N/S
BCF14.08		Written signatures	NO	N/S	N/S
BCF14.09		Photographs (physical or digital)	NO	N/S	NO
BCF14.10		Human biological samples used for scientific testing	NO	N/S	N/S
BCF14.11		Demographic data	NO	N/S	N/S
BCF14.12		Physical descriptions (such as height, weight, hair color, eye color)	NO	N/S	N/S
BCF14.13		Tattoo descriptions	NO	N/S	N/S
BCF14.14		Video or audio recording	N/S	N/S	NO
BCF14.15		Information collected, used, or stored for health care treatment, payment or operations. (E.g. X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy.)	NO	N/S	NO
		Retention, Collection, Disclosure & Destruction			
BCF15	Consent Upon Death	The individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death.	N/S	YES	YES
BCF16	Disclosure	May sell, lease, or otherwise disclose the biometric identifier to another person if consent has been obtained from the individual.	YES	YES	YES
BCF16.01	State/Federal Statute	Disclosure permitted if required or permitted by a federal statute or by a state statute.	N/S	YES	YES
BCF16.02	Law Enforcement Request	Disclosure permitted if the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant.	N/S	YES	YES
BCF16.03	Financial Transaction	Disclosure permitted to complete a financial transaction that the individual requested, initiated or authorized.	N/S	YES	YES

BCF ID	Requirement	Description	IL	TX	WA
BCF16.04	Provide Product or Service	Disclosure permitted to provide a product or service subscribed to, requested, or expressly authorized by the individual.	N/S	N/S	YES
BCF16.05	Third Party Disclosure	Disclosure permitted to third party who contractually promises that the biometric identifier will not be further disclosed and will not be enrolled in a database for a commercial purpose inconsistent with the notice and consent described.	N/S	N/S	YES
BCF16.06	Litigation Disclosure	Disclosure permitted to prepare for litigation or to respond to or participate in judicial process.	N/S	N/S	YES
BCF17	Notification of Collection	Requires notification to the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored.	YES	YES	YES
BCF18	Notification of Retention	Requires notification to 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.	YES	N/S	N/S
BCF19	Protection Requirement	Store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than how the private entity stores, transmits, and protects other confidential and sensitive information.	YES	YES	YES
BCF19.1	Retention - Illinois	Must develop a written policy, made available to the public, that establishes 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.	YES	N/A	N/A
BCF19.2	Retention - Texas	Shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires, except if captured for security purposes by an employer, the purpose for collecting the identifier is presumed to expire on termination of the employment relationship.	N/A	YES	N/A
BCF19.3	Retention - Washington	May retain the biometric identifier no longer than is reasonably necessary to provide the services for which the biometric identifier was enrolled.	N/A	N/A	YES
BCF20	Written Release	Receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.	YES	YES	YES
		Penalties & Fines			
BCF21	Civil Penalties	Law allows for civil penalties	YES	YES	YES
BCF21.01	Illinois Penalties	Civil penalty of $1,000 or actual damages, whichever is greater, for negligent violations. Damages of $5,000, or actual damages, whichever is greater, for intentional or reckless violations. Illinois also provides for attorney's fees.	YES	N/A	N/A
BCF21.02	Texas Penalties	Civil penalty up to $25,000 per violation.	N/A	YES	N/A
BCF21.03	Washington Penalties	Civil penalty of no more than $5,000.	N/A	N/A	YES
YES = Specifically Specified in Regulation(s)					
NO = Specifically Excluded in Regulation(s)					
N/S = Not Specified in Regulation(s)					
N/A = Not Applicable					

((740 ILCS 14/) Biometric Information Privacy Act 2008)
(Texas, Capture or use of Biometric Identifier 2009)
(RCW 19.375 2017)

David Todd

5. Conclusion

When embarking upon a biometrics implementation at your U.S. based organization or entity, one can feel confident that the implementation and management of the collected biometrics data can be legally defensible by following the Biometrics Compliance Framework (BCF) best-practices matrix. The BCF was derived directly from the relevant case law and biometric-specific privacy regulations from the states of Illinois, Texas, and Washington. The BCF matrix highlights the specific biometric/privacy requirements and compares those requirements across the three states analyzed. When comparing the regulations, compliance requirements, reporting requirements, and penalties of the three laws, implementing the biometrics compliance framework, companies can implement their biometrics solutions with minimal legal risk.

The number of states in the U.S. that have adopted biometric-specific privacy regulations is limited. However, many states have biometric-specific privacy legislation pending, including Massachusetts, New York, Delaware, Alaska and Michigan (Shinabarger & Swanson, 2019). By implementing biometric-related controls in place that are in alignment with Illinois, Texas, and Washington's law, companies can have a relative level of confidence in implementing biometric-related technologies that meet the spirit of the laws already in place.

The use of biometrics and biometric authentication methods have matured since used primarily for law enforcement purposes by the early biometric pioneers such as Malpighi, Faulds, and Galton in the late 1800's. Today, biometric technologies have expanded into such areas as smartphone/computer authentication, time and attendance clocks, customer loyalty programs, workforce management, patient tracking, financial services, driver identification, and registering blood donor records, to name a few examples (Waterson & Hoffman, 2019). Take advantage of the multiple biometric solutions available to protect personally identifiable information throughout your organization. Biometrics can be implemented safely and legally as authentication enhancers to the standard stored password controls.

David Todd

References

Brandom, R. (2015, December 21). Is Facebook's photo-tagging system violating privacy law? Retrieved May 10, 2019, from https://www.theverge.com/2015/12/21/10634100/facebook-photo-tagging-lawsuit-biometric-privacy-law

Clark, G. R., & Walden, W. A. (2019, February 08). Illinois Supreme Court Confirms BIPA Floodgates Are Open. Retrieved May 11, 2019, from https://www.quarles.com/publications/illinois-supreme-court-confirms-bipa-floodgates-are-open/

Duran, A. (2017, December 29). Understanding the Texas Biometric Privacy Law as an Employer. Retrieved April 05, 2019, from https://www3.swipeclock.com/blog/understanding-texas-biometric-privacy-law-employer/

Duran, A. (2019, March 19). Learn How Washington's New Biometric Privacy Law Affects Businesses. Retrieved April 09, 2019, from https://www3.swipeclock.com/blog/learn-washingtons-new-biometric-privacy-law-affects-businesses/

(740 ILCS 14/1 to 14/99) Biometric Information Privacy Act. (2008). Retrieved April 25, 2019, from http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

Fingerprint Analysis (Famous Cases). World of Forensic Science. (2005). Retrieved April 28, 2019, from https://www.encyclopedia.com/social-sciences-and-law/law/crime-and-law-enforcement/fingerprint

Gross Sholinsky, S., & Steinmeyer, P. A. (2018). Expert Q&A on Biometrics in the Workplace: Recent Developments and Trends. Retrieved April 25, 2019, from https://www.ebglaw.com/content/uploads/2018/02/Sholinsky-Steinmeyer-Reuters-Expert-QA-Biometrics-February-2018.pdf

Heldman, K. (2018). PMP: Project management professional exam study guide. Indianapolis, IN: Sybex, a Wiley brand.

Kim, T. (2019, February 18). Rosenbach v. Six Flags: Illinois Supreme Court Interprets Illinois Biometric Privacy Law. Retrieved May 10, 2019, from https://jolt.law.harvard.edu/digest/rosenbach-v-six-flags-illinois-supreme-court-interprets-illinois-biometric-privacy-law

Learn How Washington's New Biometric Privacy Law Affects Businesses. (2019, March 19). Retrieved April 28, 2019, from https://www3.swipeclock.com/blog/learn-washingtons-new-biometric-privacy-law-affects-businesses/

LII Staff. (2017, June 05). Stare Decisis. Retrieved April 29, 2019, from https://www.law.cornell.edu/wex/stare_decisis

RCW 19.375. (2017). Retrieved April 05, 2019, from https://app.leg.wa.gov/RCW/default.aspx?cite=19.375

Shinabarger, E. J., & Swanson, A. V. (2019, February 6). Several States Considering Laws Regulating the Collection of Biometric Data. Retrieved May 10, 2019, from https://www.winston.com/en/privacy-law-corner/several-states-considering-laws-regulating-the-collection-of-biometric-data.html

Sholinsky, S. G., & Steinmeyer, P. A. (2018). Expert Q&A on Biometrics in the Workplace: Recent Developments and Trends. Retrieved April 29, 2019, from https://www.ebglaw.com/content/uploads/2018/02/Sholinsky-Steinmeyer-Reuters-Expert-QA-Biometrics-February-2018.pdf

Shukovsky, P. (2017, July 18). Washington Biometric Privacy Law Lacks Teeth of Illinois Cousin. Retrieved May 10, 2019, from https://www.bna.com/washington-biometric-privacy-n73014461920/

Texas. (2009). Capture or use of Biometric Identifier. Retrieved April 05, 2019, from https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm

Vucetich, Juan. World of Forensic Science. (2005). Retrieved April 22, 2019 from Encyclopedia.com: https://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/vucetich-juan

Ward, J. (2018, March 25). Texas Biometric Privacy Law restricts certain "biometric identifiers." Only three states have laws regulating the collection and storage of Biometric data. Retrieved April 05, 2019, from https://www.garloward.com/2018/03/26/texas-biometric-privacy-law-restricts-certain-biometric-identifiers-three-states-laws-regulating-collection-storage-biometric-data/

David Todd

Washington. (2017). An ACT Relating to biometric identifiers. Retrieved April 10, 2019, from http://lawfilesext.leg.wa.gov/biennium/2017-18/Pdf/Bills/House%20Passed%20Legislature/1493-S.PL.pdf#page=1

Washington Becomes the Third State with a Biometric Law. (2018, August 03). Retrieved April 28, 2019, from https://www.insideprivacy.com/united-states/state-legislatures/washington-becomes-the-third-state-with-a-biometric-law/

Waterson, L., & Hoffman, F. (2019, January 16). 10 Ways Biometric Technology is Implemented in Today's Business World. Retrieved May 09, 2019, from http://www.m2sys.com/blog/biometric-technology/10-ways-biometric-technology-implemented-business/

Last Updated: June 18th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Cyber Defence Canberra 2019	Canberra, AU	Jun 24, 2019 - Jul 13, 2019	Live Event
SANS ICS Europe 2019	Munich, DE	Jun 24, 2019 - Jun 29, 2019	Live Event
SANS Cyber Defence Japan 2019	Tokyo, JP	Jul 01, 2019 - Jul 13, 2019	Live Event
SANS Paris July 2019	Paris, FR	Jul 01, 2019 - Jul 06, 2019	Live Event
SANS Munich July 2019	Munich, DE	Jul 01, 2019 - Jul 06, 2019	Live Event
SEC450 Security Ops-Analysis Beta 1	Crystal City, VAUS	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Pittsburgh 2019	Pittsburgh, PAUS	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Charlotte 2019	Charlotte, NCUS	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS London July 2019	London, GB	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Cyber Defence Singapore 2019	Singapore, SG	Jul 08, 2019 - Jul 20, 2019	Live Event
SANS Rocky Mountain 2019	Denver, COUS	Jul 15, 2019 - Jul 20, 2019	Live Event
SANS Columbia 2019	Columbia, MDUS	Jul 15, 2019 - Jul 20, 2019	Live Event
SANS Pen Test Hackfest Europe 2019	Berlin, DE	Jul 22, 2019 - Jul 28, 2019	Live Event
SANS San Francisco Summer 2019	San Francisco, CAUS	Jul 22, 2019 - Jul 27, 2019	Live Event
DFIR Summit & Training 2019	Austin, TXUS	Jul 25, 2019 - Aug 01, 2019	Live Event
SANS Riyadh July 2019	Riyadh, SA	Jul 28, 2019 - Aug 01, 2019	Live Event
SANS July Malaysia 2019	Kuala Lumpur, MY	Jul 29, 2019 - Aug 03, 2019	Live Event
SANS Boston Summer 2019	Boston, MAUS	Jul 29, 2019 - Aug 03, 2019	Live Event
SANS London August 2019	London, GB	Aug 05, 2019 - Aug 10, 2019	Live Event
Security Awareness Summit & Training 2019	San Diego, CAUS	Aug 05, 2019 - Aug 14, 2019	Live Event
SANS Crystal City 2019	Arlington, VAUS	Aug 05, 2019 - Aug 10, 2019	Live Event
SANS Melbourne 2019	Melbourne, AU	Aug 05, 2019 - Aug 10, 2019	Live Event
SANS Prague August 2019	Prague, CZ	Aug 12, 2019 - Aug 17, 2019	Live Event
Supply Chain Cybersecurity Summit & Training 2019	Arlington, VAUS	Aug 12, 2019 - Aug 19, 2019	Live Event
SANS Minneapolis 2019	Minneapolis, MNUS	Aug 12, 2019 - Aug 17, 2019	Live Event
SANS San Jose 2019	San Jose, CAUS	Aug 12, 2019 - Aug 17, 2019	Live Event
SANS Virginia Beach 2019	Virginia Beach, VAUS	Aug 19, 2019 - Aug 30, 2019	Live Event
SANS Chicago 2019	Chicago, ILUS	Aug 19, 2019 - Aug 24, 2019	Live Event
SANS Amsterdam August 2019	Amsterdam, NL	Aug 19, 2019 - Aug 24, 2019	Live Event
SANS August Malaysia 2019	Kuala Lumpur, MY	Aug 19, 2019 - Aug 24, 2019	Live Event
SANS MGT516 Beta Three 2019	Arlington, VAUS	Aug 19, 2019 - Aug 23, 2019	Live Event
SANS Tampa-Clearwater 2019	Clearwater, FLUS	Aug 25, 2019 - Aug 30, 2019	Live Event
Security Operations Summit & Training 2019	OnlineLAUS	Jun 24, 2019 - Jul 01, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced