



PROGRAM MATERIALS

Program #2984

May 30, 2019

Biometrics and the New Wave of Class Action Lawsuits

**Copyright ©2019 by Jeffrey N. Rosenthal, Esq. and
Harrison Brown, Esq., - Blank Rome LLP. All Rights
Reserved.**

Licensed to Celesq®, Inc.

Celesq® AttorneysEd Center

www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487

Phone 561-241-1919

Fax 561-241-1969



Biometrics and the New Wave of Class Action Lawsuits

**Presented by: Jeffrey N. Rosenthal
& Harrison M. Brown**



May 30, 2019

Introduction



Jeffery N. Rosenthal
Partner, Corporate Litigation
Member, Privacy Class Action Defense Team

- **Cyberlaw columnist for *The Legal Intelligencer*:** “Biometrics and the New Wave of Class Action Lawsuits,” THE LEGAL INTELLIGENCER (Mar. 1, 2019)
- **Presenter:** DATA GOVERNANCE, STEWARDSHIP, AND PRIVACY, Rutgers Law School Fourth Annual Corporate Compliance Institute (Apr. 12, 2019); CLASS ACTION CHECK-UP: ALLEVIATING TCPA RISK FOR HEALTHCARE PROVIDERS, Pennsylvania Bar Institute’s 25th Annual Health Law Institute (Mar. 13, 2019); TCPA CLASS ACTIONS: LESSON LEARNED FROM 2017, *The Legal Intelligencer In-House Counsel CLE* (2017); DIALING UP DEFENSES TO TCPA CLASS ACTIONS, *The Legal Intelligencer In-House Counsel CLE* (2016); CLASS ACTION AVOIDANCE STRATEGIES, *The Legal Intelligencer In-House Counsel CLE* (2015)

BLANKROME

Introduction



Harrison M. Brown
Senior Associate, Corporate Litigation
Member, Privacy Class Action Defense Team

- **Author:** “Biometric Data Risk Lawsuits,” *Industry Today* (Feb. 11, 2019); “New Ruling Reiterates That Websites and Mobile Apps Need to Be ADA Compliant” (Jan. 2019); “The Telephone Consumer Protection Act: Do You Have the Correct Consent?,” *Legaltech News* (July 18, 2018)
- **Presenter:** THE WIDENING WEB OF LIABILITY: IS YOUR COMPANY WEBSITE—AND MOBILE APP(S)—COMPLIANT WITH THE ADA? (May 16, 2019)

OVERVIEW

- What are biometrics?
- What type of biometric data can be collected?
- Where is biometric technology used?
- Why should companies care about biometrics?
- Which States regulate biometric information collection?
- What are the case trends regarding biometric class actions?
- What possible defenses are available in biometric class actions?
- What can companies do to protect themselves from being targeted?

What Are Biometrics, and How Are They Used?

- **Biometrics** are measurements of a person's physical characteristics.
- **Biometric systems** analyze unique physical or behavioral characteristics to verify identity.



BLANKROME

What Types of Biometric Information Can Be Collected?

- **Biometric Identifiers:**
 - Fingerprint Scans
 - Voice Recognition
 - Facial Recognition
 - Retina/Iris Scans
 - DNA Scans
- **Biometric Information:**
 - Any information based on a biometric identifier used to identify an individual



BLANKROME

What Types of Biometric Information Can be Collected? (cont.)

- **NOT Biometric Identifiers:**

- Writing samples
- Written signatures
- Photographs
- Demographic data
- Tattoo descriptions
- Height, weight, hair color, or eye color



BLANKROME

Where Is Biometric Technology Used?



BLANKROME

Where Is Biometric Technology Used? (cont.)



BLANKROME

Where Is Biometric Technology Used? (cont.)

- *Anywhere* employees use a fingerprint based punch clock system



How Is Biometric Information Used?



- Track employee work hours using a punch clock system
- Track consumer visits to physical locations
- Track customer activity and purchases
- Identity authentication/fraud protection

Why Should Companies Care about Biometrics?

- Laws affect all companies that in any way collect/use biometric data
- Number of class action lawsuits are on the rise.
 - Current docket of over 200 biometrics lawsuits
- Exposure could include a nationwide class action seeking uncapped statutory damages with no showing of “actual harm” required!



BLANKROME

Industries Targeted for Biometric Lawsuits

- Social Media Websites



- Employers



**\$1.6 million [proposed] settlement
(May 9, 2019)**

- Retailers/Service Providers



**\$1.5 million settlement
(December 1, 2016)**

Why Do Legislators Care About Biometrics?



- Use of biometrics is growing in business/security screening sectors.
- Promise of streamlined financial transactions/security screenings.
- BUT, biometrics are unlike other unique identifiers used to access finances or other sensitive information; for example, social security numbers, when compromised, can be changed.

Why Do Legislators Care about Biometrics? (cont.)

- Once compromised, an individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric transactions.
- Majority of the public are weary of the use of biometrics.
- Legislators believe public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.



Illinois Biometric Privacy Act, 740 ILCS/14 (“BIPA”)

- Enacted in 2008, BIPA makes it unlawful for private entities to collect, store or use Biometric Information without obtaining written, informed consent and taking precautions to secure the information.
- Legislative response to Pay By Touch bankruptcy.



What's Covered by BIPA?



- “Retina or iris scan, fingerprint, voiceprint or scan of hand or face geometry” that is used to identify an individual.
- Possess, collect, capture, purchase, receive through trade, or otherwise obtain. Very broad categories of activity regulated.

What Does BIPA Require before Biometric Information Can Be Collected or Used?

- No collection unless a company first:
 - Provides written notice of biometric collection and storage
 - Gives written disclosure of the purpose of collection and length of time of information will be collected, stored, and used
 - Obtains a written release allowing for collection
- Prohibits:
 - Disclosure or dissemination to third parties, unless release obtained
 - Profit from biometric information
- Requires:
 - Written policy available to the public
 - Guidelines for permanent destruction
 - Information kept only as long as necessary to complete the purpose or destroyed within three years of last interaction with individual
 - Reasonable care to protect biometric information

How Costly Is BIPA?

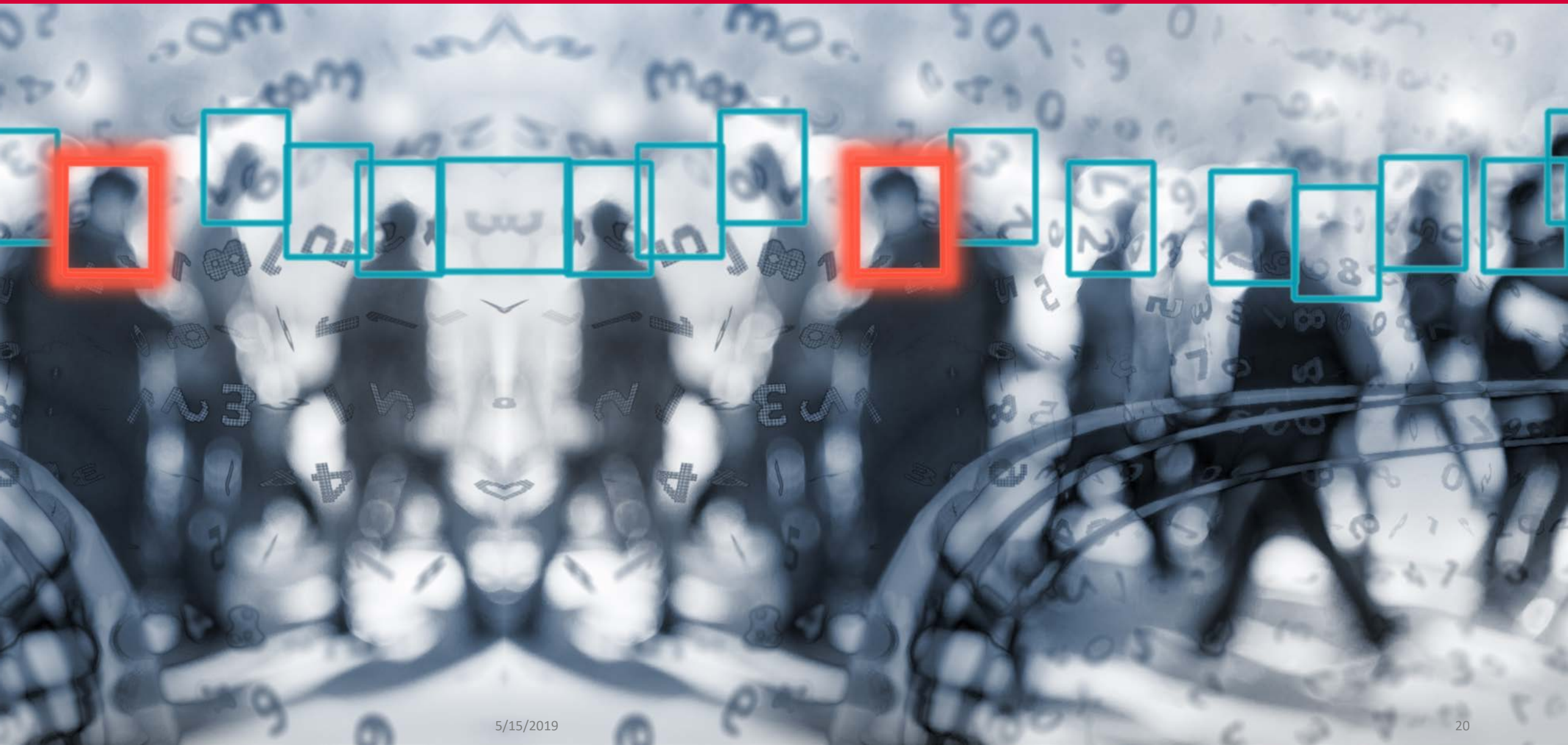
- Damages
 - Negligent violation: greater of actual damages or \$1,000 statutory penalty
 - Intentional or reckless violation: \$5,000 statutory penalty
- Attorneys' fees
- Expert witness fees
- Litigation costs

Enforceable by both the attorney general and "any person aggrieved by a violation"



BLANKROME

BIPA Class Actions



Rosenbach v. Six Flags Entertainment Corp.

No actual injury required for liability under BIPA



BLANKROME

Texas Capture or Use of Biometric Identifier Act (“CUBI”) (Tex. Bus. & Com. Code Ann. § 503.001)

- Copycat of BIPA, enacted in 2009, with a few variations.
- Only covers biometric identifiers used for a commercial purpose.
 - However, does not define a commercial purpose.
- Includes security purposes
- Notice must precede the capture of the biometric identifier
- Permits sale of biometric identifiers in certain circumstances
- Permits disclosure of biometric identifiers in certain circumstances
- Destruction required “within a reasonable time” but not later than one year
- **No private right of action**

Washington State's Law Regarding Biometric Identifiers (RCW 19.375.010 to 19.375.900)

- Third state to enact a biometric privacy law
- Biometric identifier = “data generated by automatic measurements of an individual’s biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual.”
 - Does not include “a scan of hand or face geometry”
 - Does not include photos, video and audio recordings, and information collected, used, or stored for health care
- Commercial purpose limitation
- Notice and consent requirements vary
- **No private right of action.**
- *New bill being considered by state Senate.*

Recent Trends (*Post-Rosenbach*)

- Many employee class actions against employers who use fingerprints for timekeeping
 - No written disclosure
 - No written consent
- Other jurisdictions considering biometric data legislation:
 - California
 - Arizona
 - Florida
 - Massachusetts
 - New York City

Status of Federal Legislation to Regulate Biometrics

- No single federal statute specifically addresses collection, use, or retention of biometric information.
- Several statutes, however, address privacy in other contexts.
 - HIPAA
 - GINA
 - FCRA



BLANKROME

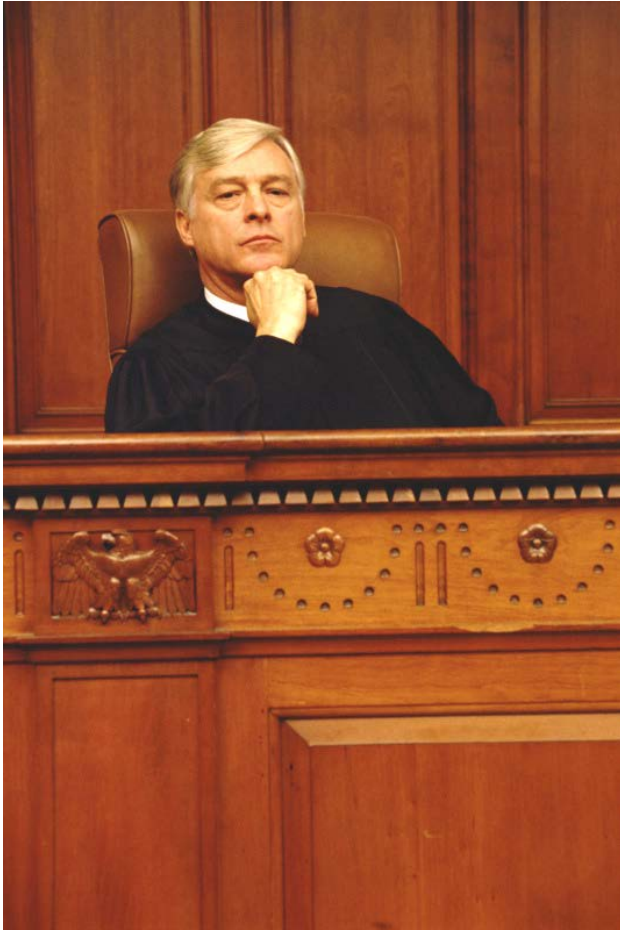
What Are the Possible Defenses to Biometric Actions?

- **Challenge applicability of BIPA and the nature of the violation:**
 - Whether the data in question constitutes Biometric Information;
 - Whether the conduct occurred primarily/substantially in Illinois; and
 - Whether the plaintiff provided any form of consent to the collection of the biometric information at issue.



BLANKROME

What Are the Possible Defenses to Biometric Actions?



- **If the case is in federal court, consider challenging the plaintiff's constitutional Article III standing.**
 - Article III injury-in-fact is a constitutional prerequisite to pursuing a claim in federal court; it is distinct from whether a plaintiff has been “aggrieved” under BIPA.
 - A “bare procedural violation, divorced from any concrete harm” is not sufficient (*Spokeo*).

What Are the Possible Defenses to Biometric Actions?

- **Challenging plaintiff's constitutional Article III standing.**
 - Pre-Rosenbach, a majority of federal courts to consider BIPA claims in the absence of actual harm held the plaintiff did not satisfy the injury-in-fact requirement.
 - Courts dismissed BIPA complaints without prejudice, or remanded to state court



BLANKROME

What Are the Possible Defenses to Biometric Actions?

- **Challenging plaintiff's constitutional Article III standing.**
 - Post-Rosenbach, if the federal court looks to the Illinois Supreme Court's interpretation, this will likely foreclose the Article III standing argument.
 - BUT, some courts have considered Article III standing separate from statutory standing; thus, state statutory interpretation is not wholly determinative of federal court standing (*i.e.*, Northern District of Illinois & Southern District of New York).
 - Issue is currently before the Ninth Circuit (*Patel v. Facebook*, Case No. 18-80053).



What Are the Possible Defenses to Biometric Actions? (cont.)

- If the case is a putative class action, consider limiting the scope of the class.
 - **Geography**
 - Because BIPA applies only to conduct within Illinois, the proposed class must be limited geographically.
 - The issue is more complicated if the defendant is based in Illinois,.
 - For nonresident defendants, scope of the class and claims will turn on whether “the bulk of the circumstances” occurred within Illinois.



What Are the Possible Defenses to Biometric Actions? (cont.)

- If the case is a putative class action, consider limiting the scope of the class.

- **Time**

- Applicable statute-of-limitations period for BIPA claims is unsettled.
- Defendants can argue for:
 - a one-year limitations period for privacy claims (*i.e.*, slander, libel and publication of matters violating right to privacy) (735 ILCS 5/13-201)

OR

- a two-year limitations period for statutes which provide a statutory penalty (735 ILCS 5/13-202).



BLANKROME

What Are the Possible Defenses to Biometric Actions? (cont.)

- **Federal Rule of Civil Procedure 23 Class Certification Arguments**

- **Typicality**

- Are there any facts that distinguish the plaintiff from the proposed class?
 - For instance, did the plaintiff—or any portion of the proposed class—provide consent for the defendant to collect biometric data?

- **Predominance**

- Do questions of law or fact common to class members predominate over any questions affecting only individual members?
 - Consider individualized issues of Article III standing and of extraterritoriality.
 - BIPA's territorial limitation may also present overwhelming individualized issues.



BLANKROME

Compliance with Biometric Privacy Laws Are Key



BLANKROME

Compliance with Biometric Privacy Laws Are Key

- ✓ Develop a written policy for retaining and destroying biometric identifiers and information.
- ✓ Make the written policy publicly available.
- ✓ Before collecting, storing or using any biometric identifiers or information, inform the person whose identifiers and information is being collected—in writing—such identifiers and information is being collected, stored or used and the specific purpose/length of time for such collection, storage and use.
- ✓ Obtain a written release from all persons providing biometric identifiers or information.
- ✓ Store all biometric identifiers and biometric information in a manner which is, at a minimum, more secure than the manner in which other confidential association information is stored.

Source: <https://www.ksnlaw.com/blog/5-tips-bipa/>

BLANKROME

RECAP

- Legislators want to encourage the use of biometrics for convenience and safety purposes, and are intent on protecting consumers from the misuse of this data based on (mostly) immutable human characteristics.
- The scope of potential damages—and the fact that, under certain state laws, there may not be a requirement to prove “actual harm”—makes biometrics suits very attractive to plaintiff’s lawyers.
- As a result, the number of biometrics suits have skyrocketed.
- There are various defenses available, but their efficacy is unknown.
- Compliance is an important step in avoiding a biometrics class action.

QUESTIONS?



Contact:

Jeffrey N. Rosenthal

Phone: 215.569.5553

rosenthal-j@blankrome.com

Harrison M. Brown

Phone: 424.239.3433

hbrown@blankrome.com

BLANKROME