Strafford

Presenting a live 90-minute webinar with interactive Q&A

Data Privacy Class Actions and Biometric Legislation: Standing and Certification Issues in Facebook and Google

THURSDAY, AUGUST 16, 2018

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Rachel Mossman, Attorney, **Shearman & Sterling**, Washington, D.C.

Alfred J. Saikali, Chair, Privacy and Data Security Practice, **Shook Hardy & Bacon**, Miami

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-866-869-6667** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the ^ symbol next to “Conference Materials” in the middle of the left-hand column on your screen.
- Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides for today's program.
- Double click on the PDF and a separate page will open.
- Print the slides by clicking on the printer icon.

SHOOK
HARDY & BACON

Shearman
SHEARMAN & STERLING

Data Privacy Class Actions and Biometric Legislation

Standing and Certification Issues in *Facebook* and *Google*

Presenters

Alfred J. Saikali
Shook, Hardy and Bacon

Chair, Data Security and Privacy Practice

asaikali@shb.com

Rachel Mossman
Shearman & Sterling

Associate, Litigation

rachel.mossman@shearman.com

Agenda

I. Defining biometric data and privacy concerns

II. Overview of existing biometric data privacy legislation

III. Recent biometric class actions

IV. Implications for plaintiffs and companies in the changing landscape of biometric-capture litigation

Defining Biometric Data

Biometric Data Defined

- Biometrics are physical characteristics that can be measured and used to identify an individual.
- Biometrics are unique because, unlike other kinds of identifiers, they cannot be changed.
- The collection and capture of certain biometrics are regulated by separate statute in three states. Each statute specifies the types of biometrics it covers.
- Other states define biometric information in their broader consumer protection statutes.

Biometric Data Defined (continued)

- Illinois Biometric Information Privacy Act, 740 ILCS 14/1 ("BIPA")
  - "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.
  - "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.
- Texas Biometric Privacy Law, Tex. Bus. & Com. Code Ann. § 503.001
  - "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.
- Washington Biometric Privacy Law, WASH. REV. CODE 19.375.101
  - "Biometric identifier" means 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.

Capture of Biometric Data

Capture of Biometric Data – Enrollment and Storage

- There has been a fundamental misunderstanding of the way the technology works.
- Scan measures ridge patterns or “minutiae points.”
- An algorithm is applied to create a mathematical representation of the person.
- The numerical representation is encrypted/stored, and sometimes associated with another piece of information, like an employee number or badge number.
- The numerical representation cannot be reverse engineered to re-create the finger/face.
- No image of the finger/face is ever stored.

Biometric Privacy Legislation

Biometric Privacy Legislation

Illinois Biometric Information Privacy Act, 740 ILCS 14 ("BIPA")

Texas Biometric Privacy Law, Tex. Bus. & Com. Code Ann. § 503.001

Washington Biometric Privacy Law, WASH. REV. CODE 19.375.101

To whom does the statue apply?

- Illinois
  - "private entities"
  - "means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof." 740 ILCS 14/10.
- Texas
  - "a person"
- Washington
  - "a person"
  - "means an individual, partnership, corporation, limited liability company, organization, association, or any other legal or commercial entity, but does not include a government agency." RCW 19.975.010 (7)

Do the statues only apply for certain uses?

- Illinois
  - No, the statute applies to all uses.
- Texas
  - Yes, the act only applies to biometric identifiers collected for “commercial purposes.”
- Washington
  - Yes, Washington also limits applicability to identifiers collected for “commercial purposes.”
  - Commercial purposes “means a purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of 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. ‘Commercial purpose’ does not include a security or law enforcement purpose.” RCW 19.375.010(4)

What has to happen *before* capture?

- Illinois
  - Inform the subject that the identifier is being collected
  - Inform the subject of the purpose and length of time for which the identifier will be used
  - Obtain **written** consent
- Texas
  - Inform individual
  - Receive individual's consent
- Washington
  - Provide notice and obtain consent, or
  - Provide a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose

Now that you have biometric data, what do you have to do?

- Keep it safe!
  - All three statutes set forth guidelines for the standard of care to be used in protecting the biometric data:
    - Illinois: must protect using the "reasonable standard of care" within the industry and in a manner the same as, or more protective than, the entity protects other confidential information.
    - Texas: must protect using "reasonable care" and in a manner that is the same as, or more protective, than the manner in which the person stores, transmits, and protects any other confidential information the person possesses.
    - Washington: must take "reasonable care" to guard against unauthorized access to and acquisition of biometric identifiers that are in the possession or under the control of the person.

Anything else?

- Destroy it when it is time
  - All three statutes also have guidelines for retaining and destroying biometric data:
    - Illinois: must develop and **publish** a written retention/destruction policy and permanently destroy biometric data when the initial purpose for collecting or obtaining the identifiers has been satisfied or within three years of the individual's last interaction with the private entity, whichever is first.
    - Texas: must destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date when the purpose for collecting the identifier expires (subject to a few exceptions).
    - Washington: may retain the biometric data no longer than is reasonably necessary to: (i) comply with a court order, statute, or public records retention schedule specified under federal, state, or local law; (ii) protect against or prevent actual or potential fraud, criminal activity, claims, security threats, or liability; and (iii) provide the services for which the biometric identifier was enrolled.

What can't you do with it?

- Illinois
  - You can't sell it. Ever.
  - "No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15 (c)
- Washington
  - You can't use it in a manner that is materially inconsistent with the terms under which it was originally provided. RCW 19.375.020 (5).

What *may* you do?

- All three statutes permit disclosure under certain conditions, including where consent is received, disclosure is necessary to close the financial transaction for which the information was given, or the disclosure is required by law.
- Texas and Washington permit the sale of biometric data where consent is given.
- Notably, Washington allows sale of biometric data without consent to a "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 in this subsection (3) and subsections (1) and (2) of this section." RCW 19.375.020 (3)(e).

What can happen if you violate the statutes?

In Illinois, you can be sued by private plaintiffs.

In all three states, you may be subject to prosecution and fines brought by the attorney general.

	Illinois	Texas	Washington
Private Right of Action?	Yes	No	No
Available Relief?	$1,000 / negligent violation $5,000 / reckless violation Injunction, costs, fees	$25,000 / violation (max)	$500,000 (max)

Recent Biometric Class Actions

Right of Action

Illinois Biometric Information Privacy Act
740 ILCS 14/1 et seq.

"Any **person aggrieved** by a violation of [BIPA] shall have a right of action," and "a prevailing party may recover **for each violation**:"

1. "against a private entity that **negligently** violates a provision of [BIPA], liquidated damages of $1,000 or actual damages, whichever is greater"
2. "against a private entity that **intentionally or recklessly** violates a provision of [BIPA], liquidated damages of $5,000 or actual damages, whichever is greater"
3. "reasonable attorneys' fees and costs . . . ."
4. "other relief, including an injunction, as the [court] may deem appropriate"

Key Cases

Illinois Biometric Information Privacy Act
740 ILCS 14/1 et seq.

No Article III standing and BIPA requires injury

McCollough v. Smarte Carte, Inc., 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016)

- Finger scan system unlocked lockers, luggage carts, strollers, and massage chairs.
- Dismissed without prejudice – no injury in fact, thus no Article III standing.
- BIPA's "person aggrieved" provision requires injury.

Santana v. Take-Two Interactive, 2017 WL 5592589 (2d Cir. Nov. 21, 2017)

- Video game scanned faces and applied them to in-game avatars.
- District Court: same rulings as *McCollough*.
- Second Circuit: dismissal for lack of standing is primary and without prejudice.

Key Cases

Illinois Biometric Information Privacy Act
740 ILCS 14/1 et seq.

BIPA does not require injury

Monroy v. Shutterfly, Inc., 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017)

- Shutterfly's software scanned non-user's face in photo uploaded in Illinois.
- Court did not interpret "person aggrieved" requirement.
- BIPA does not require actual damages.

Sekura v. Krishna Schaumburg Tan, Inc., 2017 WL 1181420 (Ill. Cir. Ct. Feb. 9, 2017)

- Finger scan system identified members.
- "Person aggrieved" does not require injury.
- "Person aggrieved" includes "any person whose biometric data was mishandled in violation of BIPA has a claim."
- Court later dismissed "for the reasons outlined in *Rosenbach*" and now on appeal

Key Cases

Illinois Biometric Information Privacy Act
740 ILCS 14/1 et seq.

BIPA requires "actual harm"

Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317

- Finger scan system identified season-pass holders.
- "Person aggrieved" under BIPA "must allege some actual harm."
- "If a person alleges only a technical violation of the Act without alleging any injury or adverse effect, then he or she is not aggrieved and may not recover[.]"

Rottner v. Palm Beach Tan, No. 15 CH 16695 (Ill. Cir. Ct. Dec. 20, 2016)

- Finger scan system identified members.
- Striking liquidated damages demand; complaint failed to allege "reasonable or plausible showing of harm or actual damages."
- Illinois Appellate Court declined to hear interlocutory appeal.

Key Cases

Illinois Biometric Information Privacy Act
740 ILCS 14/1 et seq.

Scope of BIPA's "scan of . . . face geometry" provision

***In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016)**

- Facebook's "Tag Suggestions" program scans for people in uploaded photos. Uses face geometry to do this.
- Court rejected argument that BIPA does not apply because Facebook scanned photographs of faces instead of faces.
- Denied MSJ that relied on *Rosenbach*; certified class; now on interlocutory appeal to the 9th Circuit.

Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103 (N.D. Ill. 2015) (same as to Shutterfly)

Rivera v. Google, Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017) (same as to Google)

Requirements

Illinois Biometric Information Privacy Act
740 ILCS 14/1 et seq.

Are the timeclocks collecting "biometric information"?

***Doporcyk v. Roundy's Supermarkets, Inc.*, 1:17-cv-05250 (N.D. Ill)**

- Roundy's grocery store used a Kronos timeclock system to "enroll" employees for punching in and out of work.
- The timeclock measures ridge patterns by the disturbance they cause in the radiofrequency of a scanner.
- No image is collected.
- Issue raised by MSJ – whether Roundy's collects "biometric information" as that term is defined by BIPA

Requirements

Illinois Biometric Information Privacy Act
740 ILCS 14/1 et seq.

"Substantial Compliance" Sufficient?

***Santana v. Take-Two Interactive*, 2017 WL 5592589, (2d Cir. Nov. 21, 2017)**

- Video game scanned faces and applied them to in-game avatars.
- Remanding for dismissal without prejudice for lack of standing.
- In *dicta*, suggested that BIPA should not be interpreted strictly:

> "No reasonable person . . . would believe that the [video game] was conducting anything other than [] a scan [of face geometry]."

***Rosenbach v. Six Flags Entm't Corp.*, 2017 IL App (2d) 170317**

- Noting the issue of "substantial compliance," but declining to rule on it.

Issues to Watch

Following *Rosenbach* and *Rottner*

Illinois Biometric Information Privacy Act
740 ILCS 14/1 et seq.

1. Scope of *Rosenbach* going forward?
    a) Plaintiff alleged no harm whatsoever
    b) Certified questions did not raise all of BIPA's requirements.
    c) Implies at times that "any injury or adverse effect" is sufficient.
2. Will cases follow *Rottner*?
3. What is a "negligent" violation?

Changing Landscape

Looking Forward

Illinois Biometric Information Privacy Act
740 ILCS 14/1 et seq.

1. Impact of *Rosenbach* and *Rottner*.

2. Liquidated damages are available for "each violation," but what is a "violation" for purposes of that calculation?

3. What would it mean to violate BIPA "negligently"?

4. Does BIPA apply to employee time-clock technology that scans a fingertip rather than a fingerprint?

5. Will other states add a private right of action?

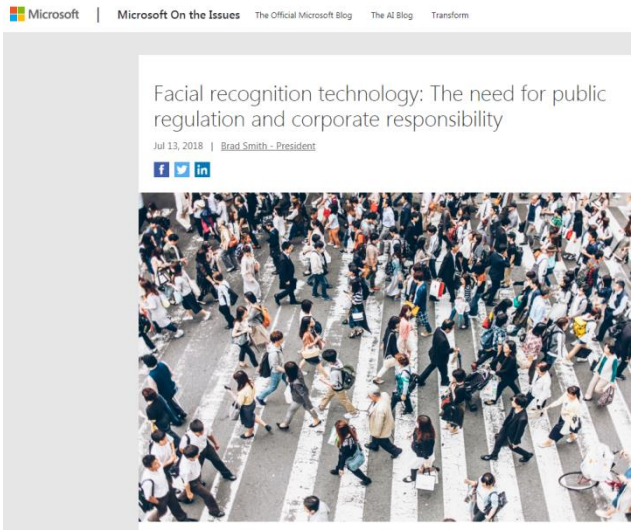
6. Considerations of *Spokeo* and Article III.

State Legislative Developments

- On June 28, 2018, California passed the California Consumer Privacy Act of 2018. AB-375.
  - The Act generally grants California citizens more rights to know how their personal information is being collected and used.
  - It goes into effect in 2020 and includes a broad definition of biometric identifiers:
    - "Biometric information" means an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.
- Other States have introduced or considered separate biometric legislation similar to the Illinois, Texas, and Washington statutes. They include:
  - New York
  - Alaska
  - Connecticut
  - Montana
  - New Hampshire
  - Michigan

Potential Federal Legislation and Guidance

In 2012, the Federal Trade Commission (FTC) addressed the growing use of facial recognition technology in a report recommending best practices for companies collecting facial scans.
https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf



On July 13, 2018, Microsoft President Brad Smith released a blog post where he urged Congress to step in an regulate facial recognition technology.
https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/

Potential Federal Legislation and Guidance

- Several bills are under review that would regulate the use of biometric identifiers:
  - The Secure and Protect Americans' Data Act (SPADA), 115 H.R. 3896
  - The Data Accountability and Trust Act (DATA), 115 H.R. 5388
  - The Biometric Information Privacy Act, 113 H.R. 4381
- These bills have been referred to subcommittees and no action has been taken on them to date.

Minimizing Risk

Practical Takeaways

Illinois Biometric Information Privacy Act
740 ILCS 14/1 et seq.

1. **Perform a Privacy Audit:** Do you collect/possess biometric information?

2. **Understand the Technology:** Work with information security personnel and vendors.

3. **Update your Privacy Policy:** Determine if a separate policy or consent form is required.

4. **Monitor the Law:** Identify applicable jurisdictions and monitor the status of pending biometric privacy laws.

SHOOK
HARDY & BACON

Shearman
SHEARMAN & STERLING

Thank You!

Alfred J. Saikali

Chair, Data Security and Privacy Practice

asaikali@shb.com

Rachel Mossman

Associate, Litigation

rachel.mossman@shb.com