The Emerging Legal Risks of Biometric Data Use

June 19, 2019

Greg Leighton
Sonya Rosenberg
Neal Gerber Eisenberg
gleighton@nge.com
srosenberg@nge.com

Lindsey Christen
Assistant General Counsel
Camping World and Good Sam
www.campingworld.com
lchristen@campingworld.com

Amanda Suchecki
Assistant General Counsel
Heidrick & Struggles
www.heidrick.com
asuchecki@heidrick.com

NEAL GERBER EISENBERG

ACC Association of Corporate Counsel CHICAGO

What We Will Cover Today

1. BIPA basics
2. Other states' biometric privacy laws and pending legislation
3. BIPA state of the law, litigation defenses and compliance considerations
4. Beyond employment: Other biometric use cases
5. How biometrics intersect comprehensive privacy frameworks

Background About BIPA – A Refresher

- Introduced in 2008, The Biometric Information Privacy Act ("BIPA"), 740 ILCS 14 *et seq*. was the first law of its kind
- Multiple states have enacted similar laws (or are in the process of doing so), but BIPA remains the most "expansive" law in many ways
  - Pertains to employers
    - As opposed to simply regulating consumer protection
  - Permits a private right of action for individuals harmed by BIPA violations
    - Up to $1,000 for each negligent violation
    - Up to $5,000 for each intentional/reckless violation
  - Broad definition of biometric data
    - Can apply to fingerprints/other information collected for timekeeping purposes
    - May be amended soon to include "wearable devices"

What About Other States - Texas

- Texas was the second state (after IL) to pass such a law
  - Tex. Bus. & Com. Code Ann. § 503.001
  - Only applies to "biometric identifiers" – similar to BIPA
    - *Exemption*: If a company uses time clock technology that only collects information based on an analysis of the data (i.e. the distance between points in a fingerprint) rather than the data itself
  - Only applies to data that is "captured" for a "commercial purpose"
    - Term not defined
  - Does not require a written retention/destruction policy
  - **No private right of action**
    - Only the Attorney General may bring a lawsuit
    - Can seek up to $25,000 in damages per violation

What About Other States – Washington

- Washington Biometric Privacy Act (HB 1493) became effective July 23, 2017
  - Regulates biometric data collected for “commercial purposes”
  - Explicitly exempts employers using data for security purposes
    - Fingerprints for time clocks (to prevent time fraud) fits into this exemption
  - Also exempts photographs, voiceprints, face or geometry hand scans
  - Does not require written consent
  - **No private right of action**
    - Attorney General may bring suit

What About Other States – New York

- New York does not have a separate biometric information law, but instead it amended an existing section of the New York Labor Law (Section 201-a)
  - Prohibits employers from requiring the fingerprinting of employees as a condition of continued employment
    - Requires an opt-out procedure
  - A 2010 opinion letter from the NY Department of Labor allowed:
    - **Voluntary** fingerprinting of employees
    - Instruments that measure data, but do not actually scan and keep a copy

What About Other States – Pending Legislation

- Arizona
  - HB 2478 introduced on January 28, 2019
    - Regulates “commercial purposes”
    - Will not encompass employers using this data for employment purposes unless the data is sold or disclosed to a third party
    - No private right of action
      - Results in a violation of the Arizona Consumer Fraud Statute
      - Up to $10,000 per violation

What About Other States – Pending Legislation

- Florida
  - Florida Biometric Information Privacy Act introduced in February 2019
  - Closely tracks BIPA
    - Provides for a private right of action (same penalties as BIPA)

- Massachusetts
  - Senate bill introduced in January 2019
  - Broad definition of biometric data
    - Similar to CCPA
  - Largely focused on commercial purposes
  - Provides for a private right of action
    - But exempts employers collecting data within the scope of employment

Illinois BIPA Requirements

- BIPA has a comprehensive set of rules for companies that collect biometric data
- 5 key features
  1. Informed consent prior to collection
  2. Limited right to disclose data
  3. Prohibits profiting from such data
  4. Obligations concerning appropriate safeguarding and destruction of data
  5. Private right of action with statutory damages and attorney's fees

BIPA – State of the Law in Illinois

- Courts are still grappling with how to interpret and apply BIPA
- Most significant "unresolved" issue is **standing** to bring a private right of action
  - *Rosenbach* case – IL Supreme Court ruling
    - A technical violation (i.e. a failure to receive informed consent or a failure to provide the requisite notices concerning purpose and scope of collection), without more, **is a sufficient injury** to bring a claim
    - The **threat** of improper disclosure is enough
      - None of the pending cases, including *Rosenbach* allege an actual breach
    - "When a private entity fails to adhere to the statutory procedures, as defendants are alleged to have done here, "the right of the individual to maintain [his or] her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized." This is no mere "technicality." The injury is real and significant."
  - Many federal courts have disagreed

BIPA – State of the Law in Illinois

- Multiple federal courts have dismissed BIPA lawsuits on the grounds that they do not meet Article III standing requirements
  - *Spokeo* – Federal court jurisdiction is limited to actual "cases and controversies"
    1. Plaintiff suffered an "injury-in-fact"
    2. Injury is "fairly traceable" to the defendant's alleged misconduct
    3. Injury is "likely to be redressed" by a judicial ruling in the plaintiff's favor
  - What is an "injury-in-fact"
    - Concrete
    - Particularized
    - Actual or imminent, not conjectural or hypothetical
  - Note: providing jurisdiction is the moving party's burden (could be the defendant's burden in a case of removal to federal court)

BIPA – State of the Law in Illinois

- Is a technical violation of BIPA an injury-in-fact?
  - *McGinnis v. United States Cold Storage, Inc.* (N.D. Ill. Jan. 3, 2019)
    - No standing for a plaintiff who suffered a technical violation of BIPA when his employer retained his fingerprints without first acquiring the requisite informed consent, nor providing a written retention/destruction plan
      - Employee "knew" that this fingerprints were being collected when he punched in every day
        - » Notice/consent were implied
      - No actual improper disclosure of this data
  - *Santana v. Take-Two Interactive Software, Inc.*, (2d Cir. 2017)
    - No standing for a plaintiff who suffered a technical violation of BIPA
      - Again, no actual improper disclosure
      - Implied consent in that the plaintiff *knew* his data was being collected for the software
        - » Note: this is a consumer-driven case, not an employee-driven case

BIPA – State of the Law in Illinois

- However, at least one federal court in Illinois *has* found that a technical violation of BIPA is enough to confer standing
  - *Dixon v. Wash. & Jane Smith Cmty.*, (N.D. Ill. May 31, 2018)
    - The Court found it instructive that in addition to "bare procedural violations" of BIPA, the plaintiff alleged that her employer disclosed her data to Kronos without her knowledge and thereby violated "her right to privacy in her biometric information"
    - "Invasion of privacy lawsuits are nothing new; at common law, violations of the right to privacy have been recognized as a valid basis for a suit.".

- **Bottom line: The law in this area is mixed, and continuing to evolve. Do pay attention to the "substantive" v. "procedural" paradigm.**

BIPA – Common Litigation Defenses

- **Common litigation defenses** center around these unresolved issues:
  - Standing concerns
  - "Violation" is undefined
    - Courts have largely interpreted this term to refer to each "aggrieved" individual employee (or consumer)
  - Definition of "collected/stored"
    - Different rulings based on whether the information, in its original form, is stored, rather than a tokenization of that data
      - For example: If your phone was stolen, the thief doesn't now have your fingerprint because your phone reads and recognizes your fingerprint via a numerical formula, NOT by actually keeping a "copy" of your actual fingerprint and comparing it to that copy every time
  - Scope of informed consent
    - Can it be implied?
    - What about a generic waiver?
    - What about an electronic-only waiver?

Common Approaches to BIPA

- The two extremes:
  - "No thanks. We're staying as far away as we can from biometric technology."
  - "Yeah, we use the technology, but we're not worrying about BIPA. We should be fine."
- What about employers who've been using the technology and just recently found out about BIPA?
  - Implement policy and acknowledgments, but does that tip off a potential class action?
  - Remove the technology?
  - Do nothing?

Biometric Technology Is Here To Stay

- Companies that do not use biometric technology currently are best positioned to prevent any BIPA related issues
  - If you know what technology is likely to be used and why – there are only so many uses in the employment context – consider implementing policy and obtaining acknowledgements in advance
  - If you don't know or are not ready, at a minimum, business should be alerted so you know before the technology is implemented
- Companies who do use the technology, but do not have the policy or acknowledgments in place
  - Implement policy and acknowledgments

Maintaining Compliance

- ✓ Obtain written consent from all employees
  - How is the information captured
  - How is the information used
  - How is the information stored
  - When and how will the information be destroyed
  - Detail full scope of any disclosures, actual or possible, to third parties
    - (i.e. timekeeping companies, building security vendors)

- ✓ Maintain a written policy
  - Thoroughly detail how the company retains and destroys this data
  - Consider detailing who has access to such data and security measures in place

Maintaining Compliance

- ✓ Prepare a plan for improper disclosures/breach
  - How will you give proper notification to employees and other third parties
  - What steps will you take to prevent future breaches
- ✓ Ensure that all vendors who may have access to this data (or collect it on the company's behalf) have similar written guidelines and emergency plans
- ✓ Ensure that the destruction plan includes all data, including any copies
- ✓ Review/update your policies and written consent forms

Maintaining Compliance – Other Considerations

- Business necessity for collecting this data?
  - BIPA is explicit that if there are other ways to accomplish the same business objective, companies should not collect biometric data
  - Convenience/efficiency may not be worth it
- Do not keep this data for any longer than necessary
  - The sooner you can destroy the data, the better!
- Review policies and guidelines
  - The law in this area is changing
  - Help demonstrate an appropriate level of care

Maintaining Compliance – Other Considerations

- Check any applicable insurance contracts (i.e. EPLI)
  - May include carve-outs for “statutory violations”

- Review arbitration agreements
  - To compel arbitration of BIPA claims, you must be explicit in the language
  - *Liu v. Four Seasons Hotel, Ltd., 2019 IL App (1st) 182645* (April 9, 2019)
    - An arbitration agreement that included “wage/hour violations” did not encompass BIPA claims
    - This is about privacy, not wage and hour issues
      - Even though a time clock was involved!

Legislative Initiatives to Limit BIPA

- BIPA remains the most expansive law of its kind
- Previous efforts to amend BIPA have failed
- Efforts currently underway
  - HB3024: Amend the definition of “biometric identifier” to include wearable devises
  - SB2134: Amend BIPA to strip the private right of action
    - Enforcement would be regulated under the DOL or the Attorney General
      - Akin to TX and WA law
    - Followed directly on the heels of *Rosenbach*

Illinois Is The Pioneer In the Employer Privacy Area

- Longstanding Right to Privacy in the Workplace Act
  - No requesting info about previously filed workers comp claims
  - No discrimination based on off-duty lawful conduct
  - No requesting employees' or applicants' social media or e-mail passwords
  - Retaliation Protections

Illinois Is The Pioneer In the Employer Privacy Area

- On **May 29th**, Illinois passed the Artificial Intelligence Video Interview Act
  - Anticipated to be signed by the Governor soon
  - No using "artificial intelligence" to evaluate applicants unless:
    - Notify applicants
      - Explain how the technology works
      - Explain the purpose for the technology
    - Obtain consent prior to the interview
  - Restricts employers from "sharing" video interviews
  - Also requires that **all copies** of a video interview are destroyed within 30 days of an applicant's request

Other Biometric Use Cases

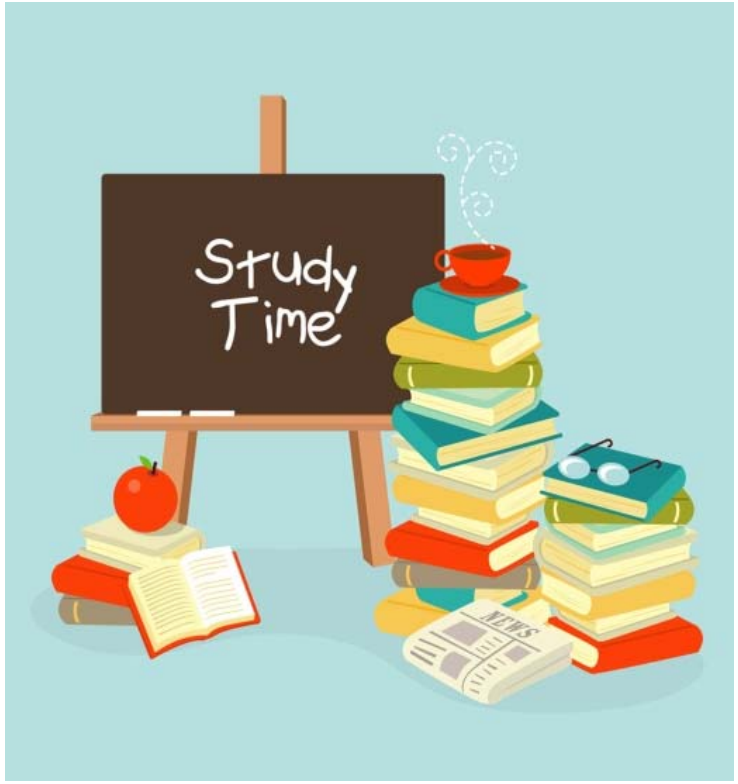
- Job Applicant – use of video in HR Tech on the rise
- Social Media – Facebook/Shutterfly, etc.
- Consumer Profiling
- Health/Fitness
- Imagination is the limit!

How Biometrics Intersect Comprehensive Privacy Frameworks

- Biometrics are special category data under GDPR
  - Explicit consent required
  - Other heightened processing requirements
  - Data Subject Rights
- Biometrics are personal data under CCPA
  - Granular notice requirement
  - Restriction on sale/disclosure
  - Data Subject Rights
- Integrate Biometrics into your global compliance program

Some parting tips

- Do an internal audit
- Review/update current policies and practices
- Engage with vendors to ensure compliance
- Keep abreast of rapidly changing law



Questions?