Cyberspace Law Institute and Winter Working Meeting
January 25-26, 2019
Stetson University School of Law
Gulfport, FL

Putting a Finger on the Problem: An Update on U.S. Biometric Privacy Law

Niya McCray, Associate, Kabat Chapman & Ozmer LLP, Atlanta, GA
John Rothchild, Associate Professor of Law, Wayne State University, Detroit, MI

This panel will assess cutting edge biometric litigation, specifically analyzing points of contention between privacy, efficiency, and our ability to comprehend the contours of biometrics.
Presenter:
Niya T. McCray

- Associate in Labor/ Employment, General Business Litigation and Data Privacy/Cybersecurity at Kabat, Chapman, and Ozmer
- ANSI Certified Information Privacy Professional (CIPP/US)
- Member of Law360’s Cybersecurity & Data Privacy Editorial Board
Roadmap

1. Current Biometric Litigation
2. Biometrics in Practice/Somebody’s Watching Me
3. Regulatory Concerns & Controlling “Capture”
4. Questions
BIOMETRIC TECHNOLOGY

- The Legal Landscape
National Overview of Biometric Privacy Laws

Biometric Privacy in the U.S.

Group One: Biometric Privacy Laws
- Illinois is the only biometric privacy law to allow consumers to directly sue in court for alleged violations.

Source: Bloomberg BNA Research
BIPA Lawsuits

- Employees alleging that the implementation of fingerprint scanning to streamline employer timekeeping systems violated BIPA’s notice, consent, and disclosure requirements.

- Consumers against commercial entities, alleging that similar biometric data—ranging from fingerprints to facial scans—were collected during transactions in contravention of BIPA’s safeguards.
Biometric Litigation under BIPA


- Plaintiffs alleged that Google created facial templates from photos uploaded to Google Photos.
- Google countered biometric identifiers do not include photographs, and that face scans must be taken in person.
- The District Court held “Nothing in the statute says, one way or the other, how the biometric measurements must be obtained.”

Rosenbach v. Six Flags & Great America, 2017 IL App (2d) 170317

- Plaintiff alleged that Six Flags failed to obtain written consent and disclose its policies for collecting consumer fingerprints in connection with season pass purchases.
- The Appellate Court honed in on the plain meaning of “aggrieved by” language, finding that plaintiff must do more than allege a technical violation of the Act. There must be “an actual injury, adverse effect, or harm.”

In re: Facebook Biometric Information Privacy Litigation & Gullen v. Facebook Inc. (Northern District of California)

- What is the actual scope of BIPA? The strength of its protections?
- Plaintiffs, both users and non-users of the Facebook platform, allege that Facebook did not obtain “written, informed consent” for using facial recognition software to suggest “tagging” options to friend.
- Plaintiffs assert that Facebook has no formal data retention policy and the language contained therein is ambiguous.
- Court has concluded that both the users and nonusers alleged a concrete injury sufficient to establish the threshold Article III standing.
Rivera v. Google

- Case gets dismissed?
- Article III Standing Issues
  - Concrete Injury?
  - Causation?
  - Remedy?
- Does violation presuppose compensation?
- Applicable to Facebook and Snapchat litigation
BIOMETRICS in PRACTICE
Somebody’s Watching
Facebook’s 10-Year Challenge
Challenge is the Best Teacher

- Facebook’s facial recognition algorithm
- What did a widespread, voluntary “challenge” teach Facebook about time progression of biometric data?
- What, if any, ownership do you have to differential nature of your biometrics?
- Opt-out of facial recognition system?
Bird’s Eye View

- 77% of Airports and 71% of Airlines are planning programs or research/development in biometrics
- Facial recognition to check-in at self-service kiosks, to drop off checked baggage, clear TSA checkpoints, board flights
Today’s Convenience is Tomorrow’s Liability

- Delta Chief Operating Officer Gil West: "It saves nine minutes on the ground for the boarding process which is time that our customers won’t be spending in lines waiting to board the aircraft."

- A typical stop at a TSA ID check station can take 11-20 seconds. With this, you’re cleared to continue on in 3 seconds.

- Camera-based system that compares scans of travelers’ faces to a database of verified ID photos curated by US Customs and Border Protection (CBP).

- Using the system is totally optional. Oversight? Accountability? Safeguards?

- The CBP says facial images of US citizens scanned at airports are deleted from their database shortly after confirmation. Facial images of non-citizens who arrive in the US are stored for 75 years, and departure photos of non-citizens are deleted after 14 days. (Delta doesn’t have control of the database)
Amazon
Rekognition

- $0.10/$0.12 per minute in exchange for analysis and processing of user uploaded videos and images
- User verification, facial recognition, people counting, and public safety
1984

- Orlando tests out Amazon’s Rekognition service
- Omnipresent government surveillance
  - Phase 1: 6 months
  - Phase 2: 9 months
- "There are eight video streams (from existing City-owned cameras) Amazon would have access to through the pilot program and it also includes photos of the faces of seven OPD officers who volunteered to have their images used in the pilot."
Saving Face...

- Over 85 activist groups demanding that Amazon not sell its FRT to the government
- 150,000 customers have signed petitions
- Over 400 Amazon employees have iterated discomfort with the product
- Civil rights: disparate impact on minorities
- Google and Microsoft vowed to refrain until the dangers are addressed
(Eye) Bank

- Eye scanning, face-and voice-recognition technology for corporate accounts
- Instead of username, password, corporate ID number, and a code from a security token
- Smaller financial organizations are also rolling out eye-scanning technology to their customers
- Beyond eye-scans and fingerprinting, Palm authentication has also been used in the finserv industry (Verifast)
Palm Reading (Vascular Biometrics)

- Pattern of veins is predetermined prior to birth and more unique than a fingerprint
- Healthcare field implemented palm scans to ensure accurate treatment
- Standardized testing (Pearson VUE) implemented to prevent test-taker fraud
BIOMETRIC TECHNOLOGY
Unresolved Issues & Controlling Capture
Expanding the Field: Pending Biometric Privacy Legislation

Bills Targeting Collection/Use of Biometric Data Specifically

- New Hampshire: H.R. 523,
- Montana: H.R. 518
- Massachusetts: H.R. 1985
- Connecticut: H.R. 5522
- Alaska: H.R. 72
- Michigan: H.R. 5019
- California
- Idaho
- New York

Amendments to Existing Breach Laws to include Biometrics

- Delaware
- New Jersey
- North Carolina
- Wisconsin
- Wyoming
- Nebraska
- New Mexico
- Iowa
- Oregon
- Maryland
Seeing Double

- Convenience v. Privacy
- Modern American “Right to Privacy”
  - Right to Control
  - Right to be Forgotten
  - Right to Erasure
- Surveillance State
- Policy Safeguards
  - Omnibus privacy legislation
- Ramifications of a True Breach Incident
  - Ownership/Property Interest
  - Data Storage & Access
Litigation Concerns

Things to Think About

- Potential Defense positions
  - Extraterritoriality, personal jurisdiction, choice of law, and standing arguments
- What types of personal information, including biometrics, does your company collect
- Who are your service providers/vendors? Do your contracts include data security provisions?
  - Liability? Consent?

Things to Do

- Update, develop, and reinforce written policies in connection with an organizational security plan
  - Train your employees
- Regularly conduct privacy risk assessments
  - Fully formulate your data incident response plan
- Less is best; only collect the minimum amount of data necessary to accomplish the task
Questions?

- Niya T. McCray, CIPP/US
  Kabat, Chapman & Ozmer, LLP
  nmccray@kcozlaw.com
  Niya.t.mccray@gmail.com