Cybersecurity, Privacy, & Communications Webinar: Regulation of Biometric Data

Jonathan G. Cedarbaum & Arianna Evers

January 11, 2018

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Attorney Advertising

Speakers

Jonathan Cedarbaum, Partner

Arianna Evers, Senior Associate

Webinar Guidelines

- Participants are in listen-only mode
- Submit questions via the Q&A box on the bottom right panel
- Questions will be answered as time permits
- Offering 1.0 CLE credit in California and New York*
- WebEx customer support: +1 888 447 1119, press 2

**WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program may be able to claim England & Wales CPD for this program. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Attendees requesting CLE credit must attend the entire program.*

Roadmap

I. Types and Uses of Biometric Technologies
II. State Biometric Privacy Laws and Litigation Under the Illinois Biometric Privacy Act
III. Proposed State and Federal Biometrics Legislation
IV. Federal Privacy Laws
V. Facial Recognition Technology: Federal Guidance and Concerns About Government Uses
VI. Some Approaches Outside the United States

TECHNOLOGY OVERVIEW

Types and Uses of Biometric Technologies

- Basic definition: measurements of physiological characteristics

- Common and developing types:
  - Fingerprints
  - Facial geography
  - Iris or retinal scans
  - Palm prints
  - Thermal imaging of blood flows
  - Behavioral biometric

Types and Uses of Biometric Technologies

- Identity verification and management
- Some common contexts for use:
  - Governmental:
    - criminal investigation
    - border screening
    - intelligence surveillance
    - combat identification
    - physical access control
    - device access control
  - Commercial:
    - device access control
    - identity verification for transactions
    - Identify verification for human resources
    - physical access control
    - targeted advertising

Growth of the Biometrics Industry

- Dozens of startups
- Perhaps $3-10B in sales worldwide

- Many expect at least 10% and perhaps 20% growth/year in size of the industry over the next decade

STATE BIOMETRIC PRIVACY LAWS AND LITIGATION UNDER THE BIPA

State Biometric Privacy Laws

- Comprehensive biometric privacy laws
  - Illinois – Biometric Information Privacy Act (BIPA) (2008)
  - Texas – Capture or Use of Biometric Identifier Act (2009)
  - Washington – H.B. 1493 (Passed July 23, 2017)
- Data breach notification statutes
  - Delaware, Iowa, Illinois, Maryland, Nebraska, New Mexico, North Carolina, Oregon, Wisconsin, Wyoming
- Laws regulating the use of student biometric information
- Laws prohibiting state agencies from using biometric data in connection with ID cards or driver's licenses

Illinois Biometric Information Privacy Act (BIPA)

- 740 ILCS 14/1 *et seq*.
- "'Biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry"
- Does not include
  - Writing samples or signatures
  - Physical descriptions such as height, weight, hair color, or eye color
  - Photographs
  - Information captured from a patient in a health care setting
  - Demographic data
- "'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"

Illinois Biometric Information Privacy Act (BIPA)

- No collection without written release
- No sale of biometric data
- No disclosure without consent
- Must protect data using “reasonable standard of care” within industry
- Retention and destruction policies must be public
- Information must be destroyed when no longer needed or 3 years after last interaction
- **Creates a private right of action for “any person aggrieved”**
- Per violation penalties for the greater of actual damages or (1) $1,000 (negligence), or (2) $5,000 (recklessness)
- Carve-out for companies subject to GLBA

Litigation Under BIPA: Facial Recognition

In re Facebook Biometric Information Privacy Litigation, No. 3:15-cv-03747-JD (N.D. Cal. filed 8/17/2015)

- Originally filed in N.D. Ill., but transferred after Facebook filed motion based on a forum selection clause in its user agreement.
- Facebook's initial effort to dismiss the case was denied (5/5/2016). Issues presented:

  (1) **Choice of law**: whether plaintiffs were precluded from suing under BIPA by choice-of-law provision in Facebook's user agreement;

  (2) **Photos**: whether Facebook's facial recognition technology is excluded from BIPA because it analyzes photographs.
- Pending motions:
  - ***Spokeo***: Facebook's renewed motion to dismiss based on the Ninth Circuit's opinion on remand in *Robins v. Spokeo.*
  - **Extraterritoriality/dormant Commerce Clause**: Facebook's motion for summary judgement, in which it argues that (1) any alleged violation took place outside Illinois and the statute lacks extraterritorial reach, and (2) BIPA's application to the conduct in question violates the dormant Commerce Clause.

Litigation Under BIPA: Facial Recognition

Rivera v. Google, No. 1:16-cv-02714 (N.D. Ill. filed 3/1/2016)

- Google moved to dismiss:

  (1) **Photos**: BIPA does not regulate photos or information derived from photos;

  (2) **Extraterritoriality**: application of BIPA to alleged conduct occurring outside Illinois would result in an extraterritorial application of the statute;

  (3) **Dormant Commerce Clause**: would also violate the dormant Commerce Clause.

- Court denied Google's motion (2/27/2017):
  - "For each face template, Google is creating a set of biology-based measurements ('biometric') that is used to identify a person ('identifier'). More importantly, as alleged, a face template is one of the specified biometric identifiers in the [BIPA], namely 'a scan of . . . face geometry.'"
  - "The bottom line is that a 'biometric identifier' is not the underlying medium itself, or a way of taking measurements, but instead is a set of measurements of a specified physical component (eye, finger, voice, hand, face) used to identify a person."
  - Discovery needed to determine whether alleged violations occurred in Illinois and Google's burden of compliance with BIPA.
- 3/5/2018 deadline for fact discovery on all issues, merits and non-merits

Litigation Under BIPA: Standing and Aggrievement

Vigil v. Take-Two Interactive Software, 235 F.Supp.3d 499 (S.D.N.Y. 2017)

- Collection of facial data for creation of avatars for video games
- Court granted Defendant's motion to dismiss for lack of Article III standing and for failure to state a cause of action:
  - Procedural violations alleged by Plaintiffs insufficient under *Spokeo* because there were no allegations that Take-Two would use the collected biometric data in a manner inconsistent with creating a personalized avatar for in-game play.
  - Plaintiffs failed to establish that their use of the MyPlayer feature resulted in any imminent risk that the data protection goal of BIPA would be frustrated.
  - Plaintiffs failed to allege they were injured by a statutory violation, and were therefore not "aggrieved."
- Second Circuit affirmed district court's finding that Plaintiffs lacked Article III standing.
- ***Mcullough v. Smarte Carte*** (N.D. Ill. Aug. 1, 2016): fingerprint scan; relied upon by *Vigil*
- ***Rosenbach v. Six Flags Entertainment*** (Ill. Ct. App. Dec. 21, 2017) (unpublished): "aggrieved" requires actual injury, not just "technical violation," but injury need not be pecuniary
- ***Monroy v. Shutterfly, Inc.*** (N.D. Ill. Sept. 15, 2017): allegation of actual injury not required

Litigation Under BIPA: Fingerprints

- Many class actions filed under BIPA concern fingerprint recognition technology and use of that technology either (i) to monitor employee work hours or (ii) to enroll members in organizations
- Approximately 30 such employee class actions filed in the past six months
- Exemplary cases:
  - ***Sekura v. L.A. Tan Enterprises, Inc.***, No. 2015-CH-16694 (Ill. Cir. Ct. filed 2015) (settled for $1.5M)
  - ***Rottner v. Palm Beach Tan, Inc.***, No. 2015-CH-16695 (Ill. Cir. Ct. filed 2015) (ongoing)
  - ***Doporcyk v. Roundy's Supermarkets. Inc***., No. 1:17-cv-05250 (N.D. Ill. Filed 2017) (motion for summary judgement on BIPA claim pending)
  - ***Johnson v. United Airlines, Inc.***, No. 2017-CH-14832 (Ill. Cir. Ct. filed 2017) (ongoing)

Litigation Under BIPA: Other Considerations

- Arbitration Clauses
  - ***Norberg v. Shutterfly***, No. 1:15-cv-05351 (N.D. Ill.). After Plaintiffs overcame Shutterfly's motion to dismiss, Shutterfly moved to compel arbitration. Parties settled soon thereafter.
  - ***Martinez v. Snapchat***, No. 2:16-cv-05182 (C.D. Cal.). Plaintiffs consented to Snapchat's motion to compel arbitration based on its terms of use.
- Insurance coverage
- Statute of limitations
- Indemnification

Texas Capture or Use of Biometric Identifier Act

- Texas Business & Commercial Code § 503.001
- Applies to “biometric identifiers” **captured for commercial purposes**:
  - Retina or iris scan
  - Fingerprint
  - Voiceprint
  - Record of hand or face geometry
- No collection without informed consent
- No sale or disclosure except in narrow exceptions
- Must protect “using reasonable care”
- Must destroy within 1 year of when no longer needed
- **No individual cause of action; enforcement by state AG**
- Statutory penalty of $25,000 per violation
- No known enforcement actions

Washington H.B. 1493

- Applies to “biometric identifiers”: data used to identify a specific individual that is generated by automatic measurements of an individual’s biological characteristics, such as:
  - Fingerprint
  - Eye retinas
  - Voiceprint
  - Irises
  - Other unique biological patterns or characteristics

- Exceptions for:
  - Physical or digital photographs
  - Information collected for health care treatment
  - Video or audio recording (or data generated therefrom

Washington H.B. 1493

- May not **enroll** biometric identifier in database without notice **OR** consent **OR** mechanism for preventing subsequent use for commercial purpose
- No sale or disclosure except in certain circumstances
- Must protect with “reasonable care”
- May only retain as long as “reasonably necessary” to fulfill purpose
- **No private right of action; enforcement by state AG**

LEGISLATIVE PROPOSALS

Proposed Biometric Legislation

- S. 2124, Consumer Privacy Protection Act of 2017
- Alaska H.B. 72 (2017)
  - Similar to BIPA
  - Private right of action
- Michigan H.B. 5019 (2017)
  - Similar to BIPA
  - Private right of action
- New Hampshire H.B. 523 (2017)
  - Similar to BIPA
  - Private right of action

FEDERAL PRIVACY LAWS

Federal Privacy Laws Potentially Encompassing Biometrics

- **COPPA**: regulations include photo or video image of face of child under 13 in definition of "personal information"
- **Driver's Privacy Protection Act**: prohibits use and disclosure of certain personal information in state motor vehicle records for commercial purposes, including photos
- **FCRA**: for identity theft, elements of "identifying information" include "[u]nique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation
- **FERPA**: regulations include biometrics in definition of PII
- **GLBA**: not expressly included in regulations, but may be encompassed by definition of "nonpublic personal information," which includes "personally identifiable financial information," which includes "any information a consumer provides . . . to obtain a financial product or service"
- **HIPAA**: full-face images and biometric identifiers included among personal identifiers that must be removed before PHI no longer consider personally identifiable

FACIAL RECOGNITION TECHNOLOGY

Facial Recognition: Federal Guidance

- FTC, *Facing Facts* (2012)
  - maintain reasonable data security protections for consumers' images and the biometric information collected from those images
  - establish and maintain appropriate retention and disposal practices for the consumer images and biometric data that they collect
  - consider the sensitivity of information when developing facial recognition products and services
  - provide users with a clear notice – outside of a privacy policy – about how the feature works, what data it collects, and how it will use the data
  - affirmative express consent before (i) using a consumer's image or any biometric data derived from that image in a materially different manner than they represented when they collected the data, or (ii) identifying anonymous images of a consumer to someone who could not otherwise identify him or her

Facial Recognition: Federal Guidance

- NTIA, Privacy Multistakeholder Process, “Privacy Best Practice Recommendations for Commercial Facial Recognition Use” (2016)
  - Transparency
  - Good data management
  - Use limitation
  - Security safeguards
  - Data quality
  - Problem resolution and redress

Facial Recognition: FBI and Non-Federal Law Enforcement

- Integrated Automated Fingerprint Identification System (IAFIS) from 1999: “world’s largest person-centric database”
- Next Generation ID (NGI) from 2011:
  - adds facial recognition; FACE Services unit
  - starts iris scan pilot
  - improves automated fingerprint matching
- GAO, congressional, and private scrutiny


GAO

United States Government Accountability Office

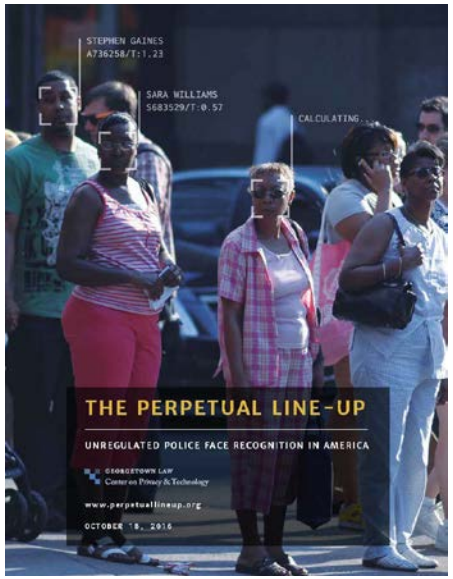
Report to the Ranking Member, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate

May 2016

FACE RECOGNITION TECHNOLOGY

FBI Should Better Ensure Privacy and Accuracy

GAO-16-267



Facial Recognition: Biometric Entry-Exit Program

- Administered by Customs and Border Protection (CBP) within Department of Homeland Security (DHS)
- Automated entry-exit system authorized in 1996
- Biometric system authorized in 2002, 2004, and 2007
- $1 billion in funds allocated in 2016
- Expedited by 2017 travel ban executive order
- Fingerprints used since 2004
- Facial scanning in testing since 2016
- Full deployment of facial scanning program planned by 2018
- Controversy: application of program to U.S. citizens

APPROACHES OUTSIDE THE U.S.

European Union

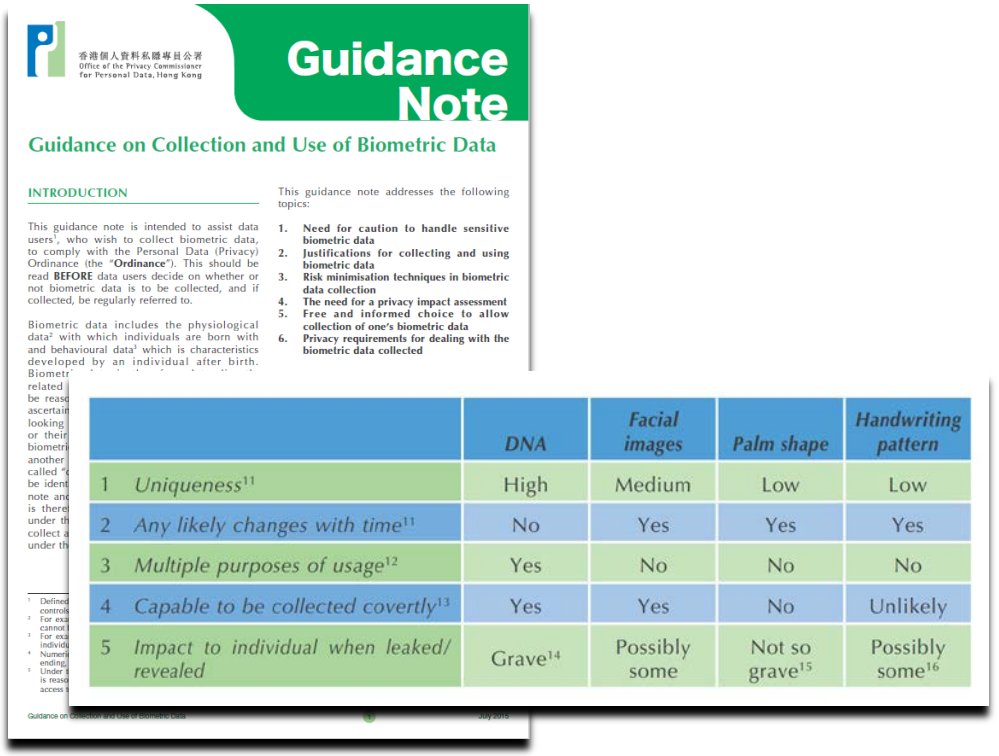
- **WP29 Opinion 4/2007**
  - "[B]iological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability"
- **WP29 Opinion 3/2012**
- **General Data Protection Regulation**
  - "[P]ersonal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data"
  - Recognized as a "special category" of personal data
  - Processing is limited to where there is a basis for processing, such as consent of the data subject or processing for narrow enumerated purposes
  - Data controllers will need to conduct privacy impact assessments in most instances
  - Member states can impose additional conditions (and limitations) on processing

China

- No national law regulating biometrics, but China's National Information Security Standardization Technical Committee has finalized the Personal Information Security Specification, which will take effect May 2018
- Draft standard explicitly includes a natural person's biological identification data (*e.g.*, gene, fingerprint, voiceprint, palm print, pinna, iris, and facial features) and behavior in its scope
- Biometric information would be regulated as sensitive personal information, with Article 5.4 requiring heightened security measures for sensitive personal information

Hong Kong

- Guidance issued by the Office of the Privacy Commissioner for Personal Data in 2015
- Collection must be for a lawful purpose related directly to its function and activity
- Practice principles of risk minimization
- Conduct a PIA
- Notice and consent
- Data security



香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Guidance Note

Guidance on Collection and Use of Biometric Data

INTRODUCTION

This guidance note is intended to assist data users[1], who wish to collect biometric data, to comply with the Personal Data (Privacy) Ordinance (the "**Ordinance**"). This should be read **BEFORE** data users decide on whether or not biometric data is to be collected, and if collected, be regularly referred to.

Biometric data includes the physiological data[2] with which individuals are born with and behavioural data[3] which is characteristics developed by an individual after birth.

This guidance note addresses the following topics:

1. **Need for caution to handle sensitive biometric data**
2. **Justifications for collecting and using biometric data**
3. **Risk minimisation techniques in biometric data collection**
4. **The need for a privacy impact assessment**
5. **Free and informed choice to allow collection of one's biometric data**
6. **Privacy requirements for dealing with the biometric data collected**

		DNA	Facial images	Palm shape	Handwriting pattern
1	*Uniqueness*[11]	High	Medium	Low	Low
2	*Any likely changes with time*[11]	No	Yes	Yes	Yes
3	*Multiple purposes of usage*[12]	Yes	No	No	No
4	*Capable to be collected covertly*[13]	Yes	Yes	No	Unlikely
5	*Impact to individual when leaked/ revealed*	Grave[14]	Possibly some	Not so grave[15]	Possibly some[16]

India

- Aadhaar, a 12 digit unique identification number, in combination with biometric data
- Launched in 2009; more than 1.2 billion individuals enrolled
- Significant concerns about data security
- In August 2017, the Supreme Court unanimously found a fundamental right to privacy in the Indian Constitution. Next year constitutional questions relating to the program will be before the court
- White paper on a data protection framework for India

Questions?

Jonathan Cedarbaum
jonathan.cedarbaum@wilmerhale.com
+1 202 663 6315

Arianna Evers
arianna.evers@wilmerhale.com
+1 202 663 6122

**WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program may be able to claim England & Wales CPD for this program. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Attendees requesting CLE credit must attend the entire program.*