Mendes Insights March 2018

Biometric Data: Watching the Watchers

As Illinois and other jurisdictions seek limitations, those limits get tested.

Cyber/Data Privacy and Security

Biometric Basics

Biometric technology refers to technology that captures physical, physiological or behavioral characteristics from an individual, which upon collection becomes biometric data, and that data then may be used to verify the identity of an individual. Law enforcement recognized the benefits of this type of technology, such as it was, with fingerprint analysis more than 100 years ago.[1] The FBI now has a biometric recognition database that houses over 50 million images with another 170 million fingerprints from foreign visitors to be added to that database by the Department of Homeland Security.[2] Biometric data includes voiceprints, facial recognition, retina or iris scans, DNA, palm prints and, even electrocardiographic rhythms or behavioral characteristics like gait, a typist's keystroke dynamics, mouse usage, or, perhaps even more broadly, geolocation patterns.[3] The use of biometric data to verify an individual's identity is based on the premise that these traits are unique and difficult to falsify or replicate.[4] The technology has seen significant growth in its commercial applications; including the use of fingerprint or iris scans for employees to "clock in,"

fingerprint scans to unlock devices, and potentially heartbeat data to verify financial transactions.[5] Governmental and private entities are using automated facial recognition technology as part of closed-circuit television (CCTV) surveillance systems.[6]

The seemingly indiscriminate nature of the acquisition of images and the data that supports these applications has raised privacy and security concerns among commentators and even some legislators. The developers and their law enforcement and private security customers argue that automatically identifying and tracking individuals in a large crowd, with 99% accuracy, is a useful tool for catching criminals at-large, detecting suspects, or even locating missing persons. However, because an individual cannot easily replace or alter a biometric feature, securing the databases that store the images and information presents significant challenges. Also, how the images and tracking data are collected and utilized likewise presents cause for concern. Are consumers prepared for retailers who can identify and target return customers? What is their comfort level with sales people at car dealerships who converge solely on patrons with purported high credit scores courtesy of Facebook? Recent legislation and the civil suits that followed provide useful context for these concerns.

Posting Some Guardrails

Somewhat surprisingly, the public has benefitted from a degree of self-regulation in this space.[7] However, there are three U.S. states, Illinois, Texas and Washington, with regulations on the books and proposals have been made in five others. The EU General Data Protection Regulation (GDPR), effective May 2018, specifies biometric data as a "sensitive category of personal data," which means that use or collection of such data may trigger mandatory privacy impact assessments and potentially other limitations from Member States.[8] Only Illinois seems to have had the reach of its guidelines scrutinized, effectively because the Illinois law allows for a right of private action.

In 2008, the Illinois legislature passed the Illinois Biometric Information Privacy Act (BIPA).[9] The Act regulates private entities' collection, retention, disclosure and destruction of biometric identifiers.[10] Under BIPA, a "biometric identifier" is a retina or iris scan, fingerprint, voiceprint, or hand- or face-geometry scan.[11] The Act requires entities to develop written policies, made available to the public, which establish a retention schedule and guidelines for permanently destroying identifiers.[12] Private entities that collect, capture, purchase, receive or otherwise obtain a biometric identifier or information must inform the subject in writing, inform the subject of the purpose and length of time the data will be stored, and receive a written release.[13] The private entity in possession of the identifier or information cannot sell or profit from the data without the subject's consent.[14] The entity must store, transmit and protect the information from disclosure using "the reasonable standard of care within the private entity's industry" as well as the manner in which the entity stores, transmits and protects other confidential and sensitive information.[15] Finally, the Illinois law is the only legislation that allows for a private right of action for any "aggrieved party," and allows for the recovery of $1,000 for negligent violations, $5,000 for intentional violations, or actual damages for any violation, as well as attorneys' fees/costs and other relief (injunctive).

The Texas law passed in 2009 has similar protections to BIPA but crucially, there is no private right of action.[16] The law defines "biometric identifier" as a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.[17] The law specifies that a person may not capture a biometric identifier of an individual for commercial purposes without consent, and may not sell, lease or disclose a biometric identifier without consent to disclosure; there are exceptions in the event of the individual's disappearance, where disclosure completes an authorized financial transaction, or where disclosure is required by law or made to law enforcement for lawful purposes.[18] The biometric information is to be stored/transmitted/protected with reasonable care and like that of other confidential information.[19] Destruction protocol is mandated (within a year, unless addressed by other sections of the law).[20] Civil penalties are allowed but any enforcement action is left to the attorney general.[21]

On April 11, 2017, HB 1493 was passed into law in Washington, effective as of July 2017. The "biometric identifiers" per HB 1493 are defined as "data generated by automatic measurements of an individual's biological characteristics." The law states that a person may not enroll a biometric identifier in a database for commercial purpose without providing notice, obtaining consent and providing a mechanism to prevent subsequent use.[22] The law has various exceptions (authorized by statute, identifier will not be used for commercial purposes, required for litigation) and requires reasonable care to protect unauthorized access and acquisition, as well as retention protocol.[23]

The other proposed legislation again looks at notice, consent and how to define what is biometric data.[24] In the meantime, class lawsuits citing BIPA have been filed against employers like United Airlines, and the usual tech and social media suspects, Google, Facebook, Snapchat, to name a few. Courts are starting to weigh in on the first line of defense – standing.

It's All Part of the Experience

> *[T]he abrogation of the procedural rights mandated by BIPA necessarily amounts to a concrete injury. This injury is worlds away from the trivial harm of a mishandled zip code or credit card receipt.*[25]

The Illinois law was in place for several years before there was a noteworthy level of litigation activity regarding compliance with the Act. Reportedly, as more and more employers utilized the technology for timekeeping purposes, class action litigation followed to challenge notice and consent practices.[26] Thereafter, there were challenges to applications in other commercial settings. As of 2018, there were in excess of twenty-five actions filed in Cook County Circuit Court (Illinois) with other litigation pending in federal courts in Illinois, California and one case on remand from the Second Circuit.[27] Defendants have argued that certain allegations do not fall within the Act's definition of biometric identifier.[28] Plaintiffs, generally speaking, have withstood that challenge. However, now case law is developing on certain critical points: whether these plaintiffs have standing to sue under BIPA; who is an "aggrieved party" under the statute; and, whether plaintiffs must allege actual damages or actual injury.

Face Mapping Gamers

The Second Circuit in *Santana v. Take-Two Interactive Software, Inc.* recently remanded that case back to the district court (SDNY), although it agreed with the district court's finding that plaintiffs lack Article III standing.[29] Plaintiffs sued Take-Two alleging that the 3-D mapping process used to capture a gamer's face as part of the multiplayer feature of its NBA-branded video games was collection of biometric data without consent, and other violations of BIPA (dissemination, retention protocol, storage outside of the standard of care). The district court dismissed the action with prejudice, siding with defendant that plaintiffs did not have standing and failed to state a cause of action under the statute. The Second Circuit similarly concluded that plaintiffs failed to establish that Take-Two's procedural violations created a material risk, and thus there was no "risk of real harm' to confer an injury-in-fact."[30]

Tracking Coaster Fans

An Illinois appellate court meanwhile was asked by the trial court whether a "person aggrieved by a violation of [the] Act" must allege some actual harm.[31] In *Rosenbach v. Six Flags*, plaintiff's son purchased a season pass for the theme park and defendants collected, recorded and stored his biometric data as part of its security process for entry.[32] Plaintiff alleged violations of BIPA and unjust enrichment; she did not allege that she or her son suffered any actual injury but argued that she would not have purchased the pass if she had known of defendants' conduct. The court noted that the Act does not define "aggrieved" and then followed the reasoning of lower federal courts, stating "[a]lleging only technical violations of the notice and consent provisions…does not equate to alleging an adverse effect or harm."[33]

Friend Tagging

Interestingly, a California federal court took a different approach with Facebook. In *Patel, et al. v. Facebook, Inc.*, U.S. District Court Judge James Donato denied Facebook's motion to dismiss, in which Facebook argued that plaintiffs failed to allege a concrete injury in fact.[34] The *Patel* matter is a consolidated action from three separate cases filed in Illinois (two in federal, one in state court). The allegations arise out of Facebook's "Tag Suggestions" program, where the program recognizes and identifies a face in a photograph posted, and then suggests the individual's name to be tagged, or automatically tags the subject.[35] The court decided that the statute itself created the interest at stake. The court focused on language from the Ninth Circuit court's opinion in *Spokeo II* to find that an alleged procedural violation of a statute by itself can manifest concrete injury, where a legislature conferred the right and the violation presents a real risk of harm to that concrete injury.[36]

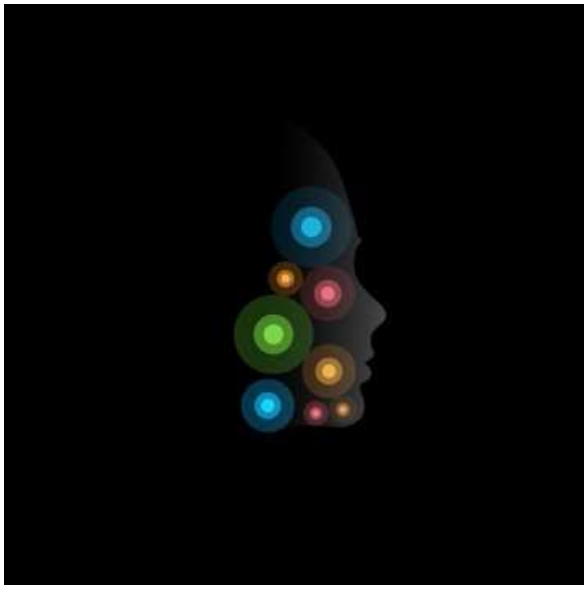
Judge Donato said that the Act "expresses the judgments of the Illinois legislature about the rights of Illinois citizens with respect to the collection of personal biometric data by corporations and businesses."[37] The court went on to say that the consent, collection and other provisions of BIPA, along with the plain text of the Act, "leave little question that the Illinois legislature codified a right of privacy in personal biometric

information."[38] The court distinguished several other similarly situated cases by noting that plaintiffs in the other cases "indisputably knew that their biometric data would be collected before they accepted the services offered" and in one case, plaintiffs "had the specific fact of prior written notice and click-through consent."[39] Likewise, distinguishing cases like *Spokeo*, the court noted that BIPA, unlike FCRA, "targets the unauthorized collection of information in the first instance."[40]

Given the *Patel* court's significant emphasis on the Act's provisions, as compared to other decisions where the courts have focused primarily on whether plaintiffs allege a mere technical violation of the Act, the next round of cases should make for compelling comparisons. The court was able to draw factual distinctions based upon the actual technology at play – facial scanning to participate in multi-player video games versus automated collection and recognition of individuals from photographs posted by a third-party.

It Did Not Play in Peoria

Illinois residents,[41] meanwhile, were recently shut-out from an online meme involving Google's Arts & Culture app feature that allowed users to compare selfies with portraits or faces depicted in works of art.[42] So it goes for Nest's "smart" doorbell camera, which product reportedly is not offered in Illinois. Illinois employers likely will figure out how best to utilize the current scanning technology, where the benefits and cost-savings outweigh the potential legal challenges. Despite Tim Cook's assurance that only your evil twin can unlock your iPhone X, lawmakers probably will continue to scrutinize the reliability of these systems.[43]



Contacts:

Kevin G. Flynn
kevin.flynn@mendes.com
1.212.261.8321

Margaret A. Reetz
margaret.reetz@mendes.com
1.212.261.8726

Lauren B. Prunty
lauren.prunty@mendes.com
1.212.261.8303

Gregory S. Mantych
gregory.mantych@mendes.com
1.212.261.8091

Editor:
David Hommel
David.Hommel@mendes.com

---

[1] U.S. Marshals Service for Students, https://www.usmarshals.gov/usmsforkids/fingerprint_history.htm. Early use of biometric data is reported circa 1891, when an Argentine police official began to compile the first-known fingerprint files based upon the work of Sir Francis Galton, a British anthropologist, who documented the characteristics by which fingerprints can be identified. The use of fingerprints began in Leavenworth Federal Penitentiary in Kansas and the St. Louis Police Department as of 1904; by 1924, the U.S. Congress established the Identification Division of the FBI.
[2] April Glaser, *Biometrics Are Coming, Along with Serious Security Concerns*, WIRED (Mar. 9, 2016, 11:00 a.m.), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/.
[3] Fingerprints and Other Biometrics, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics (last visited Mar. 1, 2018); Noelle Williams, *The Use of Biometric Data for Personal Identification Purposes*, COLUM. SCI. & TECHN. L. REV. (Nov. 13, 2017), *available at* http://stlr.org/2017/11/13/the-use-of-biometric-data-for-personal-identification-purposes/; Eduard Goodman, *Biometrics Won't Solve Our Data-Security Crisis*, HARVARD BUSINESS REVIEW (Dec. 6, 2017), *available at* https://hbr.org/2017/12/biometrics-wont-solve-our-data-security-crisis.
[4] *See* Williams, *supra* note 3.
[5] MasterCard has partnered with the biometrics company Nymi to test heartbeat authentication for credit card purchases. *See supra* note 2.
[6] Monica Chin, *Nvidia is creating AI to make cities safer... and a bit disturbing*, MASHABLE (Feb. 15, 2018), https://mashable.com/2018/02/15/nvidia-developing-facial-recognition-cameras/#TsVOAWORkiqc.
[7] Facial recognition data to unlock the iPhone X was stored on the phone's secure enclave and not in the cloud; but Apple planned to allow a third-party app developer to access some of the data, with permission from the customer and a promise not to sell that information to other parties. *See* Christina Bonnington, *Apple Plans to Share Some Data That the iPhone X Collects About Your Face. That's a Huge Worry.*, SLATE (Nov. 2, 2017, 7:25 p.m.), http://www.slate.com/blogs/future_tense/2017/11/02/apple_plans_to_share_some_iphone_x_face_id_data_uh_oh.html
[8] Danny Ross, *Processing biometric data? Be careful, under the GDPR*, THE PRIVACY ADVISOR (Oct. 31, 2017), https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/; *see also* David Meyer, *What the GDPR will mean for companies tracking location*, THE PRIVACY ADVISOR (Feb. 27, 2018), https://iapp.org/news/a/what-the-gdpr-will-mean-for-companies-tracking-location/.
[9] 740 ILL. COMP. STAT. ANN. 14/15.
[10] BIPA reportedly was in reaction to a payment company's bankruptcy, Pay By Touch, and the potential that its biometric database would be liquidated as an asset. *See* Erica Gunderson, *Biometric Data: Are We Safer in Illinois, Or Just Having Less Fun?*, CHICAGO TONIGHT (Jan. 22, 2018, 5:07 p.m.), https://chicagotonight.wttw.com/2018/01/22/biometric-data-are-we-safer-illinois-or-just-having-less-fun.
[11] Biometric identifiers do not include writing samples, photographs, biological samples used for testing/screening, demographic data, tattoo descriptions or physical descriptions, donated organs/tissues, or information captured from a patient in a health care setting, like x-rays or MRIs. 740 ILL. COMP. STAT. ANN. 14/15.

[12] *See id.* 14/15(a).
[13] *See id.* 14/15(b).
[14] *See id.* 14/15(c)(d).
[15] *See id.* 14/15(e).
[16] TEX. BUS. & COM. § 503.001.
[17] *Id.* § 503.001(a).
[18] *Id.* § 503.001(b) & (c).
[19] *Id.* § 503.001(c)(2).
[20] *Id.* § 503.001(c)(3).
[21] *Id.* § 503.001(d).
[22] WASH. REV. CODE ANN. § 19.375.
[23] *Id.* § 19.375(3) & (4).
[24] Kartikay Mehrotra, *Tech Companies Are Pushing Back Against Biometric Privacy Laws*, BLOOMBERG (July 19, 2017, 8:26p.m.), https://www.bloomberg.com/news/articles/2017-07-20/tech-companies-are-pushing-back-against-biometric-privacy-laws.
[25] *Patel v. Facebook Inc.*, Case No. 3:15-cv-03747-JD, 2018 WL 1050154, at *4 (N.D. Cal. Feb. 26, 2018).
[26] Michael J. Bologna, *Biometric Workplace Privacy Suits Erupt in Illinois State Court*, BNA (Oct. 25, 2017), https://www.bna.com/biometric-workplace-privacy-n73014471344/ ("Those 25 complaints represent more than 74 percent of the approximately 34 BIPA actions that have been filed in Cook County since the start of the year, according to Bloomberg Law Dockets data.").
[27] *Santana v. Take-Two Interactive Software*, --- F. App'x ----, 2017 WL 5592589, at *4 (2d Cir. Nov. 21, 2017) (summary order) ("Since the statutory standing arguments here are based on differing constructions of the term 'aggrieved party' as used in BIPA, the district court's resolution of the issue was a judgment on the merits that could not be properly addressed absent subject matter jurisdiction."). Relying on *Spokeo v. Robins*, 136 S. Ct. 1540 (2016), the Second Circuit affirmed the district court's dismissal of the case based upon a lack of Article III standing but vacated the district court's finding that plaintiffs were not "aggrieved by" a violation the BIPA. *See id* at *3–*5.
[28] *See, e.g.*, *Rivera v. Google*, 238 F. Supp.3d 1088, 1095 (N.D. Ill. 2017); *Norberg v. Shutterfly, Inc.*, 152 F. Supp.3d 1103, 1105 (N.D. Ill. 2015).
[29] *See id.* at *5.
[30] *Id.* at *4 (internal quotation marks and citation omitted).
[31] *Rosenbach v. Six Flags Entm't Corp.*, 2017 IL App (2d) 170317 (Dec. 21, 2017), *available at* http://www.illinoiscourts.gov/Opinions/AppellateCourt/2017/2ndDistrict/2170317.pdf.
[32] *Id.* at 3.
[33] *Id.* at 7 (citing *McCullough v. Smarte Carte, Inc.*, No. 16-C-03777, 2016 WL 4077108, *4 (N.D. Ill. Aug. 1, 2016) and *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 519–20 (S.D.N.Y. 2017)).
[34] *Patel*, 2018 WL 1050154 at *1.
[35] *Id.*
[36] *Id.* at *2 (citing *Robins v. Spokeo, Inc.* 867 F.3d 1108, 1112 (9th Cir. 2017) ("*Spokeo II*")).
[37] *Id.* at *3.
[38] *Id.* at *4.
[39] *Id.* at *5 (discussing *Take-Two* and *McCullough*).
[40] *Id.*
[41] Wikipedia, *Will it play in Peoria?*, https://en.wikipedia.org/wiki/Will_it_play_in_Peoria%3F (as of Mar 1., 2018, 12:44 GMT).
[42] Ally Marotti, *Google's art selfies aren't available in Illinois. Here's why.*, CHICAGO TRIBUNE (Jan. 17, 2018, 7:00 a.m.), http://www.chicagotribune.com/business/ct-biz-google-art-selfies-20180116-story.html.
[43] Cady Lang, *The Internet Had All of the Jokes When It Came to Apple's iPhone X Face ID*, TIME (Sept. 12, 2017), http://time.com/4938362/the-internet-had-all-of-the-jokes-when-it-came-to-apples-iphone-x-face-id/ ("[T]the chance that a random person can unlock your iPhone X with their face is 1 in a million. Unless you have an evil twin you're safe.") (internal quotation marks and citation omitted).