BIOMETRICS

WHAT IS IT?

The term "biometric" derives from Greek words, bio (meaning life) and metric (to measure. See Biometrics Definition, TechTarget.com. Biometric identification refers to any technology that relies on intrinsic physical or behavioral traits to either identify you or authenticate your identity. When used for identification, an image is run against a database of images. For authentication -- such as to access a protected account - an image has to be accessed from the device to confirm a match. See *generally* A. Glaser, *Biometrics Are Coming Along With Serious Security Concerns*, Wired (3/2016).

There are two primary types of biometric identifiers: physiological, which relate to the composition of the user, such as fingerprints, facial recognition, iris recognition, retina scanning, voice recognition and DNA matching. Behavioral identifiers encompass the unique ways that individuals act such as gait or gestures. See Biometrics Definition, *supra*.

WHY NOW?

Law enforcement has been using fingerprints to identify and track people for over a century. So why are biometrics such a hot topic now? Several reasons. Not surprisingly, technology advances have improved biometrics identification systems and reduced the cost, making them more widely accessible. The technology is advancing rapidly too: whereas back in 2013, when Apple's iPhone 5s became one of the first phones to feature a fingerprint scanner, today, virtually every consumer electronic device - smartphones, tablets and smart home controls can be accessed through fingerprint or voice recognition. Businesses are incorporating biometrics too, using the data to track worker time and attendance.

Increased concern over security is another factor contributing to the growth of the biometrics sector. Many view biometric identification (such as fingerprint scans) as a solution to lengthy airport security lines. A recent survey by Visa revealed that 46 percent of consumers polled view biometrics as more secure than passwords or PINS for verifying identity, and 50 percent view biometrics as more convenient than storing multiple passwords.

On the flip side, biometric identification raises significant privacy concerns. Alvaro Bedoya, quoted in a Wired article best

characterized why biometrics - though not inherently invasive - feel that way. Bedoya explained that "A password is inherently private. The whole point of a password is that you don't tell anyone about it. Biometrics, on the other hand, are inherently public…"I do know what your ear looks like, if I meet you, and I can take a high resolution photo of it from afar. I know what your fingerprint looks like if we have a drink and you leave your fingerprints on the pint glass." Moreover, when facial recognition is used in law enforcement context - such as use of facial recognition to bar shoplifters from a store - the resulting harm of misidentification can be significant.

In 2015, the General Accounting Office published Facial Recognition Technology: Commercial Uses, Privacy Issues and Applicable Federal Law. GAO-15-621 in response to the proliferation of information resellers--companies that collect and resell information on individuals--which dramatically increased the collection and sharing of personal data for marketing purposes, raising privacy concerns among some in Congress. The GAO recommended that Congress should consider strengthening the consumer privacy framework to reflect the effects of changes in technology and the increased market for consumer information. At the same time, GAO cautioned that any changes should seek to provide consumers with appropriate privacy protections without unduly inhibiting commerce and innovation.

KEY LEGAL ISSUES:

Standing: As with privacy and data breach cases (See Privacy Section), at least one reported biometrics case was dismissed on standing grounds. *See Santana v. Take-Two Interactive Software*, No. 17-303 (November 21, 2017). There, a user sued Take-Two, developer of a video game with a feature that allows players to scan their face into the game to create a personalized avatar. The user argued that the disclosure was inadequate under Illinois Biometrics Privacy Act. The Second Circuit affirmed the lower court's dismissal, holding that the complaint failed to raise a material risk of harm and thus, did not satisfy standing requirements under *Spokeo*. *See also Rosenbach v. Six Flags Entertainment Corporation*, Docket No. 2-17-0317, Appellate Court of Illinois, Second District (Dec. 21, 2017)(holding that a plaintiff who alleges only a technical violation of the statute without alleging some injury or adverse effect is not an aggrieved person under section 20 of the [Illinois Biometric Information Privacy Act]); *but see Monroe v. Shutterfly*, Case No. 16 C 10984 (Sep. 15, 2017)(declining to dismiss case based on plaintiff's failure to allege damages).

Criminal Law: Biometric information challenges traditional concepts of privacy under traditional Constitutional jurisprudence. Consider for example, the plain view doctrine, which holds that evidence discovered in plain view during the course of a stop doesn't violate the Fourth Amendment. But since certain biometric information -

such as facial recognition is always in plain view, does that mean that a police officer can snap a photo of a driver for speeding and run it through a database? Or does the fact that biometric evidence is non-invasive entitle law enforcement to collect a wide range of information whenever a suspect is arrested?

In *Maryland v. King*, 133 S. Ct. 1958 (2013), the Supreme Court, in a 5-4 decision ruled that "when officers make an arrest supported by probable cause to hold for a serious offense and bring the suspect to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment." The Court's ruling rested on both an arrestee's reduced expectation of privacy, but also the minimal invasiveness of a DNA swab. Under this reasoning, an arrestee could be subject to a battery of biometric gathering procedures that while non-invasive to perform nonetheless unreasonably intrude on privacy because of the information produced. By contrast, Scalia, writing for the dissent held categorically that the Fourth Amendment categorically prohibits a suspicionless search - irrespective of how non-invasive it may be.

Biometric information implicates the Fifth Amendment as well. Whereas forcing an arrestee to disclose a password to a phone violates the right against self-incrimination, but compelling production of a fingerprint is sometimes viewed differently. See *State v. Baust*, 2014 WL 10355635 (Va. Cir. Ct. Oct. 28, 2014) (ruling that "the Defendant cannot be compelled to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the same," because while the former is testimonial, "[t]he fingerprint, like a key, . . . does not require the witness to divulge anything through his mental processes"). *But see In re Application for a Search Warrant*, 236 F.Supp.3d 1066 (N.D. Ill. 2017)(granting search warrant for residence, but denying request "to compel any individual who is present at the subject premises at the time of the search to provide his fingerprints and/or thumbprints 'onto the Touch ID sensor of any Apple iPhone, iPad, or other Apple brand device in order to gain access to the contents of any such device). For additional discussion, see Erin M. Sales, Note, *The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination*, 69 U. Miami L. Rev. 193 (2014) (suggesting that "biometric authentication will not implicate the privilege to be free from self-incrimination"). *But see* Kara Goldman, Note, *Biometric Passwords and the Privilege Against Self-Incrimination*, 33 Cardozo Arts & Ent. L.J. 211 (2015) ("use of the fingerprint as a password is a direct link to communicative, as well as potentially incriminating, information, and serves as a replacement for traditional password, is protected by the Fifth Amendment).

State Laws: To date, three states - Illinois, Texas and Washington State have enacted laws to protect biometric

information. All three statutes prohibit the sale or disclosure of biometric information collected from an individual unless the individual consents to disclosure, or the disclosure is required by state or federal law or pursuant to subpoena. In addition, the Washington statute permits disclosure of biometric information without consent where doing so is necessary to provide a service subscribed to or authorized by the user. By contrast, Illinois' Biometric Information Privacy Act (BIPA), 740 ILCS 14/5(b) also requires that a business in possession of biometric identifiers have a publicly available written policy, and to establish a retention schedule and guidelines for the destruction of biometric information. The policy must require the destruction of biometric information whenever the initial purpose for its collection has been satisfied, or within three years, whichever occurs first. Texas BIS has a one-year destruction period instead of three-year period, but does not require a publicly-available written policy.

Privacy Suits: Lawsuits have been filed against Facebook and Google under Illinois' BIPA, alleging that the companies violated the law by collecting images from users without consent and using them to build "the world's largest privately held database of consumer biometric data." *See Facebook Biometric Info. Privacy Litig*, 185 F.Supp. 3d 1155 (N.D. Ca. 2016), *Rivera v. Google, Inc.*, No. 16-02714 (N.D. Ill. Feb. 27, 2017)See *Tech Companies Pushing Back on Biometrics*, Bloomberg (7/20/2017). In *Rivera*, Google attempted to argue that its collection of facial images were not "biometric information" within the meaning of BIPA - a claim that the court quickly disposed of given BIPA's broad definition of biometric information. The court also rejected Google's claim that BIPA had extraterritorial effect; the court found that the Legislature had not intended extraterritorial scope and in any event, the acts took place in the cloud with, which sufficient local contacts could be presumed to be in Illinois. Facebook sought dismissal on other grounds - arguing that the plaintiffs not suffered harm and lacked standing under Spokeo. The judge rejected that argument, explaining that "The right to say no is a valuable commodity...The case concerns the "most personal aspects of your life: your face, your fingers, who you are to the world." See *Facebook Judge Frowns on Bid to Toss Biometric Suit,* Bloomberg (11/30/2017)(discussing motion to dismiss). Both suits are considered bellweather cases and will be closely watched as they move forward,

Choice of Law: At least one court determined that Illinois substantive law would apply to a suit brought against Facebook under the BIPA and transferred to federal court in California. Although Facebook's terms of use stated that California law should apply, the court declined to enforce them, and ruled instead that BIPA would govern. The court reasoned that if it were to enforce the California choice-of-law clause over Illinois Biometric Privacy Act ("BIPA"), "the Illinois policy of protecting its citizens' privacy interests in their biometric data . . . would be written out of

existence" because California has "no law or policy equivalent to BIPA *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016), *But see Palomino v. Facebook*, Case No. 16-cv-04239 (N.D. Ca. 2017)(enforcing California choice of law clause in suit filed under New Jersey consumer protection statute, finding that California has its own robust consumer protection statutes).

Employment: With the advent of scanners, microchips, lawsuits against employers for collection of biometric data have exploded. In the latter half of the year, roughly 30 lawsuits were filed against employers, alleging violations of Illinois' BIPA. *See Illinois Employers Flooded With Class Actions Stemming From Biometric Privacy Law*, IllinoisPolicy.org (10/17/2017). Employers adopting biometric devices - such as scanners or microchips to track employees cannot force employees to submit to tracking based on religious objections. In *US EEOC v. Consol. Energy*, 4th Cir. (6/12/2017), the Fourth Circuit affirmed a jury verdict finding that an employer wrongfully refused to accomodate an employee who informed his supervisors that his religious beliefs (which he documented with a note from his pastor) prevented him from using the scanning system.

Future Trends & Opportunities: Biometrics is just in its nascency and will challenge current beliefs regarding the meaning of privacy, and the extent of an individual's right to be left alone. Applicable law governing biometrics will also change, as more states enact biometric privacy statutes or if Congress steps in to propose a federal law.