How Biometrics Are – and Soon May Not Be – Used by Private Investigators

BY **GEORGIANA EISENHARDT**

While the recent popularity of artificial intelligence (AI), automation and machine learning are giving biometrics a boost, law enforcement and private investigators (PI's) have used biometric data for years. Think of your favorite episode of Law & Order: Special Victims Unit. Every time an SVU detective dusts for fingerprints, asks for a blood sample or finds a circumspect hair at a scene, they are collecting – and storing – biometric data.

Moreover, modern biometric practices are starting to catch up with the more advanced theatrical aspirations of SVU and its ilk. Some PI's are now working with biometric data that includes retina and iris scans, voice matching, as well as scans of hand or face geometry.

Understanding how these newer biometric datapoints work within the realm of private investigation is important. If you are an investigator working with advanced biometric data, or might soon become one of them, you must carefully consider every aspect of your work in this realm to avoid exposing yourself to costly legal disputes. This includes any acquisition, collection, transmission, scanning or providing of this data to or for others. There are plenty of cautionary tales available regarding biometric data and sizable legal settlements.

A Quick Recap

In my last article I shared that biometric data is any information about an individual's physical attributes that can be stored. Biometric data provides physical proof that connects an individual to an action or location. Unfortunately, there are technologies now available that make biometric data easier to fake or replicate. This presents serious challenges to authenticate that same data. Similarly, there are privacy issues to consider. There are rules and regulations governing biometric data privacy, and those rules vary by state. Understanding them is important to safely navigating the challenges and leveraging the benefits of biometric data for more successful investigations.

Biometrics as PI Tools

As mentioned, there are many types of biometric data. PI's should fully understand what they are looking to accomplish when collecting data, and which type of data will best help them accomplish their goals. They include:

- **Fingerprinting and Physical Samples:** Fingerprints, along with blood and hair samples, are the surest indicators that a specific individual can be tied to a particular location. Additionally, with the use of fingerprints to create and open locks on phones, computers, doors and more, it is now easier to tie an individual to a device that may be instrumental in an investigation. PI's should ensure they know the local rules and regulations around fingerprint and DNA collection, as only certain certified individuals can collect such data under federal law.
- **Patterns and Structures:** As with fingerprints, the use of retinal and facial recognition technologies is becoming widely popular, both for devices as well as in the world of security. Such patterns and structures, while possible to replicate, are more difficult to replicate or steal than a simple numeric or alphabetical password. The challenge for PI's is getting into a device in an investigation to find applicable evidence. Doing so without the individual's permission is morally and ethically wrong. It also crosses several legal boundaries. A final note on facial recognition: There is growing use of cameras among personal residences and commercial and public spaces. Access to this data – either provided by the homeowner, building owner or government entity – is a significant aid to PI's investigating certain matters. PI's should be sure to better understand local laws and regulations involving access and use of this digital footage, as well as their use with facial recognition programs.
- **Voice Matching:** Many PI's rely on recording devices for observation, surveillance and questioning. Such recording devices can catch an individual's voice, but not their image or other physical attributes. Using voice matching technology, an individual's voice can be matched and may be admissible in court as evidence.
- **Behavioral Characteristics:** While less perfect and/or unique than other biometric data, such as fingerprinting or DNA sequencing, behavioral characteristics, such as

the way one walks, how much pressure one uses when writing their signature, even, in some instances, which hand is their dominant hand can be used as biometric data.

Biometrics and the Law

As important as understanding how biometrics can be used by PI's, it is just as important to understand the local rules, regulations and existing and pending legislation around the use of this data. There is a growing body of legislation and litigation that suggests there are as many risks as advantages for those not familiar with these laws. Here are a few recent examples:

The Illinois Biometric Information Privacy Act (BIPA) has driven several costly claims, most notably a $92 million settlement of a class-action lawsuit by TikTok's parent company, ByteDance. Under BIPA, private entities are restricted from obtaining through any means a person's biometric data without receiving consent first. There are also several restrictions regarding use and storage of such data under BIPA.[1]

A 2021 New York law requires businesses to advise clients if biometric data is being tracked or captured. This law led to a class-action lawsuit against Amazon and its Go stores in the state which was tracking customer biometric data.[2]

In late 2022, the Texas attorney general filed a privacy lawsuit against Google. The Texas AG claimed Google illegally collected the face and voice data of the Lone Star state's citizens without first securing their consent.[3]

According to a February 2023 client alert from law firm Wilmer Hale, at least 15 biometric privacy laws have been proposed in Arizona, Hawaii, Maryland, Massachusetts, Minnesota, Mississippi, Missouri, New York, Tennessee, Vermont and Washington state. The firm also noted California, Colorado, Virginia, Connecticut and Utah closely regulate biometric data.[4]

One result of the emerging legislation, litigation and related jury verdicts connected to the collection, use, access and dissemination of biometric date is that insurers are taking a more cautious approach to underwriting to minimize any potential exposure to biometric-related claims.

Biometric Basics

While the variety of biometrics is expanding the ability of PI's to conduct better and more accurate investigations that bring greater accountability to bear, these tools and their application come at a price. PI's must not only understand how to employ biometrics in their work, they will also find it crucial to understand how they can legally gather, store, disseminate, and apply biometric data; and that understanding will need frequent refreshing as both technology and the legislative environment evolve.

For PI's who have a clear idea of where their investigation is headed, what they are looking for and how to manage the evidence available, they can apply biometrics to complete a thorough and successful investigation. **PI**

Reference

1. https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2021/03/The-Coming-Wave-of-Biometric-Class-Action-Suits.pdf
2. https://www.nbcnews.com/tech/security/amazon-sued-not-telling-new-york-store-customers-facial-recognition-rcna75290
3. https://www.nytimes.com/2022/10/20/technology/texas-google-privacy-lawsuit.html
4. https://www.wilmerhale.com/en/insights/client-alerts/20230224-biometric-privacy-law-update

Georgiana Eisenhardt is program manager for PI Protect from the Brownyard Group, where she works closely with private investigators, security consultants and professionals in related fields. PI Protect is a leading provider of specialized insurance coverage for investigators. Learn more at https://brownyard.com/.