New York Law Journal

WWW.NYLJ.COM

An ALM Publication

Legal Risks and Rules of the Move to Biometrics

MARCH 2, 2015

By Mark Melodia, Paul Bond and Angela Angelovska-Wilson

In Sweden, 95 percent of transactions are digital.[1] Its payment engineers even hope to see a move to a DNA-based payment model. Said one, perhaps tongue-in-cheek: "My favorite payment actually is DNA payment. You spit in a cup next to the cashier … it's the absolutely safest way, right? … Someone would have to copy your DNA."[2]

As hackers beat form after form of authentication, more and more companies are turning to biometrics to know who's who. The epidemic of identity theft continues, making novel biometric forms of identification all the more reasonable. As regulators push to limit uses of SSNs, device-identified data, and other traditional forms of identification, biometrics provides an attractive alternative to those whose businesses run on personal information. A new report from Juniper Research[3] has found that more than 770 million biometric authentication applications will be downloaded per year by 2019, up from just six million this year and dramatically reducing dependence on alphanumeric passwords in the mobile phone and other markets.

But U.S. law around fingerprints, retinal scans, voice prints, and other forms of biological-based identification is patchy at best. This article will explore the developing legal framework behind the race to biometric adoption.

What Are Biometrics?

It is hard to regulate what you cannot define, and there is no set legal or industry definition for "biometrics." Even Illinois and Texas, the two states to attempt more comprehensive regulation of the issue, vary slightly in definition. The Illinois Biometric Information Privacy Act defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[4] While Texas uses similar language, Illinois specifies exclusions to its definition that Texas does not. Namely, in Illinois "Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color."[5]

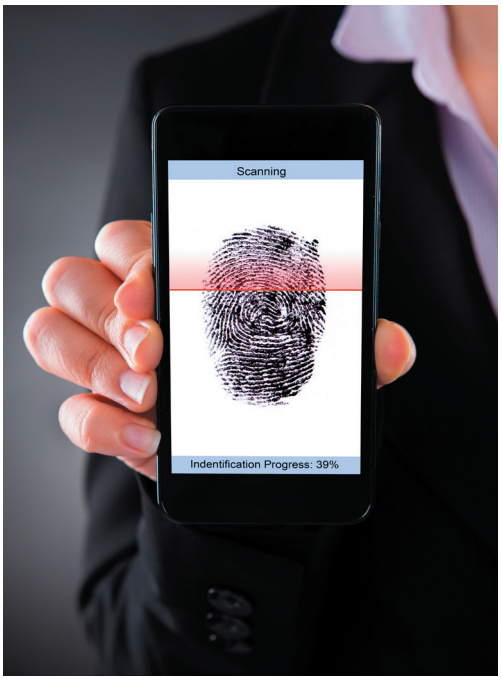
The Federal Bureau of Investigations defines biometrics more broadly. "Biometrics are the measurable biological (anatomical and physiological) or behavioral characteristics used for identification of an individual."[6] And, indeed, many more recent biometric authentication technologies capture not anatomical records but records of behavior, from keyboard strokes to screen touches on a mobile device. Thus, biometric collection is made possible in large part by the so-called Internet of Things, itself the subject of concern and extensive review by the Federal Trade Commission.[7] Attempts to regulate biometric information extend to derivative forms of such information—for example, Illinois applies protections to biometric information "regardless of how it is captured, converted, stored, or shared."[8]

Importantly, the range of personal/biological information that could be called "biometric" is much broader than what is protected by any existing, specific federal law. For example, the federal Genetic Information Nondiscrimination Act of 2008 (GINA) regulates the use of "genetic information," described by that Act as "with respect to any individual, information about—(1) such individual's genetic tests, (2) the genetic tests of family members of such individual, and (3) the manifestation of a disease or disorder in family members of such individual."[9] GINA prohibits, for example, the use of genetic information to discriminate in employment practices. Most biometric information would not meet this definition, and would fall outside of GINA's protections.

How Are Companies Using Biometrics?

While government and military operations have been using biometric identification for a number of years now, the commercial application and use by companies is still maturing. Examples of current uses include:

- Mobile payment applications such as Apple Pay are used to authenticate and initiate payments;
- Employers are switching to biometric measures (like iris scan) to reduce lost time due to punch card fraud;
- Technology like the iPad can be unlocked by the user's fingerprint;
- Financial institutions are capturing voiceprint details on calls to substantially reduce the incidence of identity theft and fraud;
- Nightclubs and restaurants are using facial recognition technologies to create customer profiles of high-end customers;
- Retailers are using the same technology to keep track of known criminals and check-bouncers for loss prevention purposes; and,
- Advertisers, both online and in physical stores, are using biometric information (from facial patterns to breath rate) to personalize advertising in real time.



In 2014, the President's Counsel of Advisors on Science and Technology provided a detailed report on the future of Big Data.10 According to this body:

> [T]he ability exists to sense remotely the pulse of an individual, giving information on health status and emotional state … It is foreseeable, perhaps inevitable, that these capabilities will be present in every cell phone and security surveillance camera, or every wearable computer device. (Imagine the process of negotiating the price for a car, or negotiating an international trade agreement, when every participant's Google Glass (or security camera or TV camera) is able to monitor and interpret the autonomic physiological state of every other participant, in real time.)[11]

Researchers have been successful in using facial recognition data to determine likely life span.[12] A comedy club in Barcelona is offering a

pay-per-laugh model in conjunction with a tablet app.[13] The potential applications of biometric data are limited only by the availability of relevant data and the legal limits now in place or soon to come.

What Are Potential Risks?

In passing its Biometric Information Privacy Act, Illinois set forth its motivations. The statement of the Legislature summarized the main concerns:

> (c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.[14]

Part of the value proposition of biometrics is that they are identifiers that inhere in who we are and what we habitually do. They are not artificial or external, and cannot be reassigned by our bank or a government agency. For this reason, some states (albeit, a small minority) have included biometric information among the types of information that can trigger a data security breach notification requirement.[15] Even in those states that do not require notification to individuals when biometric information is lost or stolen, the risk associated with maintaining databases of such information is clear. The Illinois statement continues:

> (d) An overwhelming majority of members of the public are wary of the use of biometrics when such information is tied to finances and other personal information.[16]
>
> (e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.[17]

It is open to doubt whether the legislature's view of public opinion on biometric identifier-facilitated transactions was true when passed in 2008, is true now, or will be true in the future. For example, there is some evidence to suggest that the use of mobile payments is mainly constrained by initial retailer reluctance, and not by that of consumers.[18]

> (f) The full ramifications of biometric technology are not fully known.

This last point by the Illinois legislature is the least controversial. It is very difficult to predict the uses to which biological-based information could be put in the future. Indeed, in some of the contexts where biometric information is being collected, such as in a store or on a public street, parties collecting the information would be hard-pressed to contact the data subjects later when new, socially-beneficial uses develop. Even contemporaneous notice of data collection may often be impractical, given how pervasive and generic the collection has become.[19]

What Laws Are in Place?

While the technology rabbits race ahead, the legal tortoises plod behind. Every new technology from steamboats to player pianos to software to drones have challenged the ability of judges to apply existing law, and legislatures and regulators to make new law.

There is no directly applicable federal law regarding biometrics per se. Depending on context, HIPAA may apply; GINA may apply; or, they may not. The generally applicable federal standard will remain the prohibition against unfair or deceptive practices under §5 of the FTC Act. The FTC has brought enforcement actions against certain companies concerning privacy and security of, for example, camera feeds.[20] The FTC also has authority to enforce the provisions of the Fair Credit Reporting Act (FCRA) when any information, including biometric information, is used to determine eligibility for credit, insurance, or employment. This FCRA authority may become more and more important as biometric information is used to blacklist certain consumers or segment the advertising shown to them. The federal government will also continue to try to coordinate development of voluntary standards around biometrics, such as the Department of Commerce's NTIA Privacy Multistakeholder Process on Facial Recognition Technology.[21]

The states—as usual—are the legal laboratories testing new approaches on this issue. The most express laws with respect to biometrics remain the Illinois and Texas acts. The Illinois law provides, for example, that "No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information," without proper notification and consent.[22] The statute also provides that "No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information," and does not provide an exclusion for consent.[23] Especially given that the Illinois statute provides for a private right of action for any violation and $1,000 per person in damages for a negligent violation and $5,000 per person in damages for an intentional or reckless violation, it is easy to see that the national biometric service providers face significant potential liability.

Like Illinois, Texas imposes policy and destruction period requirements, and limits collection and use of biometric data. Texas also allows the Attorney General to recover $25,000 in civil penalties per violation.[24]

Conclusion

Biometric technologies are already a booming business, with many existing applications. Those applications will continue to grow. While few U.S. laws expressly and directly apply to biometric technologies, those few laws can have a powerful impact and should be carefully weighed in any potential application. In addition, the whole existing framework of U.S. law with respect to consumer and employee protections continues to apply. New technologies must be reviewed in light of long-existing standards as much as developing guidance.

Endnotes:

1. Ari Shapiro, "Cash Is Definitely Not King For Card-Carrying Swedes," National Public Radio (Feb. 2, 2015), available at http://www.npr.org/blogs/parallels/2015/02/02/383321605/cash-is-definitely-not-king-for-card-carrying-swedes.
2. Id.
3. Juniper Research, "Human Interface & Biometric Devices Emerging Ecosystems, Opportunities & Forecasts 2014-2019," available at http://www.juniperresearch.com/research/human-interface-biometric-devices.
4. (Illinois) Biometric Information Privacy Act, 740 ILCS 14/10.
5. Id.
6. Federal Bureau of Information, "Fingerprints and Other Biometrics," available at http://www.fbi.gov/about-us/cjis/fingerprints_biometrics.
7. Federal Trade Commission, Internet of Things: Privacy & Security in a Connected World (Jan. 2015)(IOT Report).
8. (Illinois) Biometric Information Privacy Act, 740 ILCS 14/10;
9. Pub.L. 110–233, 122 Stat. 881, enacted May 21, 2008.
10. "Big Data and Privacy: A Technological Perspective," Executive Office of the President, President's Counsel of Advisors on Science and Technology (May 2014), available at http://www.whitehouse.gov/blog/2014/05/01/pcast-releases-report-big-data-and-privacy, p. 23.
11. Id.
12. Samanta Dean, "This facial recognition software doesn't just analyze the age a person's face appears—it also predicts how long that person will live," Virginian-Pilot & Ledger Star (Norfolk Va.), Oct. 14, 2014.
13. Dominic Basulto, "An innovative new payment model that's no laughing matter: This could be the template for new payment models based on your body's responses to stimuli," Washington Post, Oct. 14, 2014.
14. (Illinois) Biometric Information Privacy Act, 740 ILCS 14/5(c)-(f).
15. See, e.g., Neb. Rev. Stat. §87–801 et seq. (includes Nebraska resident's name in combination with any biometric data, including a fingerprint, voiceprint, retina or iris image, or any other unique physical representation).
16. (Illinois) Biometric Information Privacy Act, 740 ILCS 14/5(c)-(f).
17. Id.
18. Andrea Chang, Shan Li, "Businesses remain on Apple Pay sidelines: Consumers embrace mobile payments, but retailers' reluctance poses a challenge," Los Angeles Times, Oct. 30, 2014.
19. See, however, the FTC's deprecation of that concern in FTC IOT Report.
20. Federal Trade Commission, "Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy: Hundreds of Camera Feeds for Home Security, Baby Monitoring Were Hacked, Posted Online," available at http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.
21. http://www.ntia.doc.gov/other-publication/2014/privacy-multistakeholder-process-facial-recognition-technology.
22. 740 ILCS 14/15(b).
23. 740 ILCS 14/15(c).
24. V.T.C.A., Bus. & C. §503.001(d).

Mark Melodia, Paul Bond, and Angela Angelovska-Wilson are partners at Reed Smith.