Cybersecurity Law Report
An Acuris company

cslawreport.com

April 3, 2019

BIOMETRICS

Navigating Today's Biometric Landscape

By *Elizabeth McGinn*, *Scott T. Sakiyama*, *Magda Gathani* and *Garylene D. Javier*, *Buckley LLP*

Biometrics-based authentication of payments and other transactions has been on the rise for the past several years, promising unparalleled convenience and security for consumers. However, the distinctive nature of biometric features that confers its advantages is also the source of the technology's critical risk. Companies using biometric data need to understand the shifting regulatory landscape both here and internationally and the pressing security and privacy considerations. Protecting consumers' biometric data is essential and companies deploying biometrics-based authentication should take deliberate steps to ensure appropriate safeguards.

See also "Biometric Data Protection Laws and Litigation Strategies (Part One of Two)" (Jan. 31, 2018); Part Two (Feb. 14, 2018).

Biometrics-Based Authentication: A Growing Trend

The expansion of biometrics-based authentication has been fueled by a growing range of uses across both the private and public sectors. Using fingerprints or voice or facial recognition can meaningfully improve the customer experience, rendering passwords and one-time authentication codes obsolete. And unlike passwords that can be stolen or codes that unauthorized users can intercept, biometric identifiers are unique and intrinsically secure. Given the benefits, consumers increasingly perceive biometric authentication as state-of-the-art technology that is at once safer and easier to use.

Products and Payments

A recent study showed that 93 percent of consumers preferred biometrics to passwords. Governments worldwide have used them for many years in high-security facilities such as military bases, nuclear reactors and correctional facilities, among others. The U.S. Customs and Border Protection uses fingerprint scans of international travelers to the U.S., and has launched pilot programs at several airports that compare facial scans of travelers to passport photos. The use of biometrics has also grown exponentially in the private sector, from cell phones to fitness centers to cars. Companies use them to grant employees physical and network access, and to punch in and out.

Use of biometrics in payment systems is growing. Apple Pay uses touch and face ID technology. Clear Payment Solutions implemented a system allowing consumers to purchase food and drinks at concession stands with nothing but their fingerprints. In January 2019 alone, Zwipe and IDEX raised $14 million and $25 million, respectively, to develop biometric payment cards.

Regulator Support

Regulators are also signaling support for biometrics. Cybersecurity regulations that the New York Department of Financial Services issued in 2017 (NYDFS Regulations) list biometric characteristics as one of the three acceptable types of authentication factors. The NYDFS Regulations require covered entities to use a multifactor authentication for individuals accessing the entity's internal network from an external network. The multifactor authentication must be accomplished through verification of at least two types of factors, with a biometric characteristic being one of the three.

See "What Covered Financial Entities Need to Know About New York's New Cybersecurity Regulations" (Mar. 8, 2017).

Protecting Biometric Information Is Critical

The distinctive nature of biometric features that confers its advantages is also the source of the technology's critical risk. New passwords and codes can be generated on demand and infinitely; a retina only once. Protecting consumers' biometric data is essential, and companies deploying biometrics-based authentication should take deliberate steps to ensure appropriate safeguards for the biometric data they collect – revisiting and updating those safeguards frequently.

The burden of protecting biometric data rests with any company that collects, stores and transfers it, and is a crucial responsibility given the inability to recover the data once breached. As the Illinois Supreme Court put it in a recent decision, an individual whose biometric data has been compromised "has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." [1]

A hack in 2018 of India's Aadhaar Enabled Payment Systems, which compromised the biometrics and personal information of over 1 billion users, underscores the significance of strong security features. Aadhaar, the world's first national biometrics-based payments system, as introduced by the government of India, allowed individuals to conduct financial transactions across any participating bank using only three inputs: (1) a number identifying the bank; (2) the customer's own national identification number assigned using fingerprints or retina scan for identification; and (3) the customer's fingerprint or retina scan to authenticate the customer at the time of transaction. The hack into the Aadhaar program included a software patch that disabled critical security features of the software used to enroll new users, and allowed users to bypass the biometric authentication of enrollment operators to generate unauthorized Aadhaar numbers.

Current Laws and Regulations

Laws and regulations relevant to biometrics are changing quickly, but not in lockstep. Indeed, a company operating in the U.S. likely faces an entirely different standard than a company operating in Europe. In the U.S., the individual states are taking the lead, leaving companies to navigate an uneven patchwork of requirements. In Europe, sweeping regulations dictate use, collection and handling of data. In either regime, companies should implement policies and procedures to ensure that the biometric data they use is secure.

Europe

The European Union's General Data Protection Regulation (GDPR) provides a unified approach to the protection and use of consumer data. Under GDPR Article 9, biometric data falls under the "special categories of personal data" processed to uniquely identify a person. Controllers (entities that control how and why the data is processed) and processors (entities that perform the processing actions as directed by controllers) in the E.U. are prohibited from processing special categories of personal data unless the individual to whom the biometric data belongs gives consent, as set out in Article 9. The Regulation protects the personal data of E.U. citizens both in and outside the E.U., as well as non-E.U. citizens who are physically in the E.U. The GDPR's definition of processing includes virtually everything, actively or passively, that touches on the use of personal data, including storing, erasing, organizing, retrieving, or transmitting it.

Broadly speaking, a company providing any type of biometric product in the E.U. must:

- create processes that allow a person to control their enrollment in a biometric payment method;
- implement appropriate organizational and technical measures and privacy policies that are GDPR compliant, such as conducting impact assessments of risks in processing biometric data, appointing a data protection officer and implementing a code of conduct governing the processing of biometric information;
- develop safeguards while planning the implementation of new biometric payment systems and work with vendors
- on adequate processes for biometric devices or naked payments ;
- implement safeguards in the transmission of biometric data; and
- require third-party processors of biometric data (such as retailers) to, among other things:
  - process biometric data only as instructed;
  - provide all necessary information to demonstrate compliance with the GDPR; and
  - destroy biometric data as directed or at the conclusion of the controller-processor relationship.

These requirements are particularly important in cloud-based payment systems that transmit data between a point-of-sale terminal that gathers biometric identifiers and a centralized database that has the information to confirm the consumer's identity. The potential damage from unauthorized database access is immense, and companies must have systems in place at both ends of the transmission process to prevent data capture by third parties. Fines for noncompliance are staggering; severe cases could be the greater of €20 million ($22.7 million) or 4 percent of global annual revenue.

See our three-part series analyzing early GDPR enforcement: "Portugal and Germany" (Jan. 23, 2019); "U.K. and Austria" (Jan. 30, 2019), "France" (Feb. 6, 2019).

United States

The U.S. Congress is weighing a federal law governing privacy, but several states, including Illinois, California, Washington, Texas and California have adopted their own privacy laws covering biometrics.

The Illinois Biometric Information Privacy Act is designed to prevent the unlawful collection

and storing of biometric information. Under BIPA, a company that wants to collect or store biometric identifiers must receive written consent from the holder of the biometric identifier, spelling out what data the company wants and how long it proposes to hold it. Companies must establish a retention schedule and guidelines for destroying the data after the initial purpose of the collection has been achieved, or if it has been three years since the last transaction between the company and the individual. Disclosure of a person's biometric information is prohibited unless exempted; completion of financial transactions as requested by the subject of the biometric information is one of only four exemptions. BIPA grants any person aggrieved by a violation of the law a right of action, with damages of $1,000 for negligent violations and $5,000 for intentional or reckless violations.

The Illinois Supreme Court's January 2019 ruling in *Rosenbach v. Six Flags Entertainment Corporation* highlighted the importance of BIPA compliance. A woman filed suit against Six Flags for collecting her son's fingerprints, without notice or consent, as a means of entry into the theme park. The court held that BIPA created a fundamental right to an individual's own biometric information and that a violation of the law itself, even if there was no actual harm, was sufficient to support a cause of action. Companies aiming to support biometric financial transactions in Illinois should educate their customers during the enrollment process of its practices for collecting, storing and transmitting biometric data, and secure the customer's written consent to the practices. Failure to do so invites legal action, including potential class actions in instances in which procedural omissions lead to serial transgressions of the law.

Due to BIPA's broad application, companies that offer biometric-related products in Illinois should proceed carefully. The facial-recognition feature of Nest Hello, a Wi-Fi-enabled doorbell with security cameras, is a significant differentiator over rival devices because owners can tag and recognize visitors when they come to the door. Nest Labs, acquired by Google in 2014, limited the feature on devices sold in Illinois, even as residents in all other states use it.

The *Rosenbach* decision could impact the development of biometric privacy doctrine outside of Illinois. New York has a bill pending that allows for a private right of action for violations related to biometric identifier information. A proposed Massachusetts bill would require companies collecting consumer personal information, which includes all information "relating to an identified or identifiable consumer" including biometric identifiers, to provide notice to the consumer before collecting such data. The Massachusetts bill also provides for a private right of action. Plaintiffs in these jurisdictions could cite the *Rosenbach* decision in support of their cases.

Similar to the Illinois BIPA, the California Consumer Privacy Act, which becomes effective January 1, 2020, also provides a private right of action. The CCPA includes biometric information in its definition of "personal information" and requires that a company inform consumers about the types of categories of information that will be collected and the purpose for which the information will be used. The CCPA provides for statutory damages of between $100 and $750 per incident.

See "Preparing for the CCPA: Best Practices and Understanding Enforcement" (Mar. 6, 2019).

Privacy laws in Washington and Texas are enforceable only by the government. Texas establishes notice and consent requirements, but narrows the collection of biometric identifiers for a commercial purpose. Washington prohibits collection of biometric identifiers in a database for a commercial purpose without notice and consent. In the Illinois, Washington and Texas laws, a company may not disclose identifiers to third parties unless the disclosure completes a financial transaction the individual requested or authorized.

Even absent statutes that allow for a private right of action, plaintiffs have other options to pursue biometric-related claims. They can allege common-law claims, such as an invasion of privacy or negligence. Many states, including California, recognize the right to privacy under state constitutional or common law, though these claims require showing an actual harm. The U.S. Office of Personnel Management is currently the target of a class-action lawsuit alleging biometric-based violations under common law following a data breach that affected 22 million federal applicants, employees and family members, and compromised, among other types of data, fingerprint records. The common-law claims included negligence, invasion of privacy and breach of contract. This case has been appealed and the viability of the common law claims in the context of biometric-related violations remains to be seen.

See also "Illinois Federal Court Denies Standing in BIPA Claim Against Google" (Jan. 23, 2019); "Illinois Appellate Decision Creates Split on Standing to Sue Under BIPA" (Dec. 12, 2018); "Actions Under Biometric Privacy Laws Highlight Related Risks" (Dec. 6, 2017).

Recommended Safeguards

Although laws are still evolving to catch up to the rapid technological advancements in biometrics, companies should develop operational and technical safeguards when designing products using them. These safeguards include mechanisms to address risks associated with each step of the biometric payment process – recruitment, enrollment, transaction and relationship termination. To the extent possible, companies should deploy multifactor biometrics-based authentication protocols. For example, authentication based on the customer's voice paired with facial recognition, or fingerprint paired with voice recognition.

See also "Overcoming the Challenges and Reaping the Benefits of Multi-Factor Authentication in the Financial Sector (Part One of Two)" (Jul. 26, 2017); Part Two (Aug. 9, 2017).

Because of the unique nature of biometric identifiers, consumers are particularly sensitive about how they are collected, stored, used and shared. Providing notice of handling procedures and obtaining consent before collecting, processing and destroying the data are major steps in avoiding privacy-law noncompliance.

Companies should also require partners and vendors to adhere to the same high standards in the handling of biometric data. Companies can limit the risks of collecting and processing biometric data by screening all third-party vendors that handle that data, conducting data and privacy risk assessments, and verifying that vendors encrypt data in transit.

Biometrics offer tremendous benefits to customers and companies alike, but present risks. With adequate diligence, companies should be able to successfully deliver on the promise of this developing technology to their and their customers' benefit.

See also "How to Maintain Effective and Secure Long-Term Vendor Relationships: Understanding the Risks (Part One of Two)" (Jun. 20, 2018); Part Two (Jun. 27, 2018); and "Checklist Approach to Effective Third-Party Vendor Oversight" (Aug. 15, 2018).

Elizabeth E. McGinn is a partner in the Washington and New York offices of Buckley LLP. Scott T. Sakiyama is counsel in the firm's Chicago office. Magda Gathani is an associate and Garylene D. Javier is a regulatory attorney in the firm's Washington office. They advise clients on consumer financial services, privacy and cybersecurity-related matters and electronic discovery.

[1] *Rosenbach v. Six Flags Entertainment Corp.*, 2017 IL App (2d).