OLLIS/AKERS/ARNEY
HUMAN RESOURCES CONSULTING

PROTECTING TOMORROW...TODAY.

The Risks of Collecting Biometric Data

Biometric data refers to an individual's unique physical and genetic characteristics, including facial geometry, iris scans, fingerprints and voiceprints, gait rhythms, behavioral patterns and certain types of DNA. In recent years, a growing number of organizations have begun collecting stakeholders' biometric data to help enhance account authentication measures, deploy stricter access controls, create personalized marketing materials, and monitor employees' workplace attendance and activities.

While biometric data can allow organizations to maintain greater operational visibility and provide stakeholders with more individualized experiences, it also carries risks related to data privacy and personal security. Further, the regulatory landscape for biometric data collection is constantly evolving, paving the way for potential compliance issues and subsequent legal penalties and litigation. As such, it's imperative for organizations that collect biometric data to review these exposures and take steps to combat them. This article provides more information on the risks of collecting biometric data, explains the current regulatory landscape for such collection and offers related risk management tips.

Data Collection Risks

Some of the main risks that organizations may face by collecting biometric data are:

- **Privacy concerns**—Biometric data includes a range of personal and genetic identifiers that, unlike other types of data (e.g., usernames, passwords and PINs), cannot be easily changed or replaced. This makes biometric data particularly sensitive, thus posing heightened concerns regarding the ethics of organizations collecting such private stakeholder information and potentially leaving it vulnerable to misuse or abuse.
- **Security exposures**—Because biometric data is so sensitive, cybercriminals could be more likely to target it in security incidents (e.g., data breaches and ransomware attacks). What's worse, the exploitation of this data may leave behind lasting—or even permanent—ramifications for impacted organizations' stakeholders. Specifically, the release of this information could result in stakeholders having to deal with ongoing identity theft concerns. Additionally, due to the genetic component of biometric data, the exploitation of this information could also cause considerable security issues among stakeholders' relatives.
- **Reputational issues**—As security incidents rise in frequency and severity, stakeholders are increasingly holding organizations accountable for failing to protect against or promptly respond to these events. Consequently, organizations that misuse stakeholders' biometric data or contribute to its exploitation by neglecting to implement proper security safeguards could encounter severe reputational losses, including diminished public trust, reduced customer loyalty and lower staff retention rates.

The Evolving Regulatory Landscape

In addition to the risks of biometric data collection, organizations should also be aware of the current regulatory landscape for this topic; evolving data privacy legislation could pose compliance concerns. The primary focus of this legislation centers around the wrongful collection of data. What constitutes wrongful or unlawful data collection varies by jurisdiction.

While there isn't an overarching national consumer data privacy law that applies specifically to biometric data in the United States, some aspects of federal legislation regulate certain sectors and individuals (e.g., the Health Insurance Portability and Accountability Act and the Children's Online Privacy Protection Act). More comprehensive data privacy laws concerning biometric data, such as the following, have also been adopted at the state and international levels:

- **The Biometric Information Privacy Act (BIPA)**— Illinois was the first state to regulate the collection of biometric data upon implementing the BIPA in 2008. This legislation forbids organizations operating in this state from collecting individuals' biometric data unless they have informed these individuals about the data being collected, provided information on how long it will be stored and received written consent to move forward with collection. The BIPA also permits individuals to sue organizations directly if they violate this legislation.
- **The Capture or Use of Biometric Identifiers Act (CUBI)**—Texas was the next state to introduce such legislation by establishing the CUBI in 2009. This law prohibits organizations operating in the state from collecting individuals' biometric data for commercial purposes unless they notify these individuals and receive explicit consent before obtaining this information. The CUBI also restricts organizations from selling or disclosing biometric data to other parties and requires this information to be destroyed in a "reasonable" time frame after use.

- **The Washington Biometric Privacy Protection Act (HB 1493)**—Implemented in 2017, HB 1493 restricts organizations that operate in Washington or service residents in this state from collecting individuals' biometric identifiers for commercial purposes without first providing notice of doing so, receiving clear consent and developing mechanisms to prevent these identifiers from being released, sold or otherwise disclosed to additional parties.
- **The General Data Protection Regulation (GDPR)**—Established in 2018, the GDPR restricts organizations that operate in the European Union or service residents in this area from collecting or processing individuals' biometric data without first receiving explicit consent to do so. Even then, organizations must clearly outline how this data will be used and stored. Because the GDPR classifies biometric data as a "special category of personal information," this law also requires organizations to conduct data protection assessments and take extra precautions when storing such data.

Apart from this legislation, some states have created broader data privacy laws that include some stipulations on biometric data. Examples of such laws include:

- **The California Privacy Rights Act (CPRA)**—Although the CPRA, which was introduced in 2020 and went into effect in 2023, doesn't solely focus on biometric data, the law categorizes this data as a form of "sensitive personal information," particularly when it's being used to "uniquely identify" an individual. When collecting biometric data for this purpose, the CPRA requires organizations that service California residents to inform individuals how their data will be obtained and processed, including whether it will be shared with third parties. Upon receiving this information, individuals have the right to limit the use of their data or opt out of disclosure.
- **The Virginia Consumer Data Protection Act (VCDPA)**—Introduced in 2021 and enacted in 2023, the VCDPA enforces similar standards for organizations that service Virginia residents as those outlined in the CPRA; however, this law includes a more restrictive definition of biometric data, prohibits organizations from processing individuals' data without prior consent and requires extra documentation regarding data collection protocols.
- **The Colorado Privacy Act (CPA)**—Also introduced in 2021 and enacted in 2023, the CPA enforces similar standards for organizations operating in Colorado as those outlined in the VCDPA; yet, this law does not clearly define biometric data and includes stronger guidelines regarding how individuals can consent to have their data collected.

Going forward, additional jurisdictions will likely follow suit with similar data privacy legislation. In fact, at least 10 other states have recently proposed such laws. Even though it may be complicated, organizations have a duty to comply with applicable data privacy laws. Failure to adhere to relevant legislation when collecting biometric data could be deemed wrongful, leaving noncompliant organizations subject to legal penalties ranging from thousands to millions of dollars in fines and strict sanctions. Compounding these expenses, organizations that engage in improper biometric data collection, processing, sharing or storage practices could also be susceptible to costly litigation brought on by disgruntled stakeholders, especially if their data gets compromised.

Risk Mitigation Techniques

In light of the risks and challenging regulatory landscape surrounding biometric data collection, employers should consider these risk management measures:

- **Conduct a risk assessment**. First, employers should review and document their specific risks related to biometric data collection. In doing so, they can better understand their exposures and determine necessary mitigation tactics.
- **Leverage robust data privacy practices**. When obtaining biometric data, keeping this information private is a must. Proper safeguards may include data minimization and cancelable biometrics. Data minimization refers to limiting the collection, processing and storage of biometric information to only what is absolutely critical to conduct key operations and provide essential services. Cancelable biometrics rely on advanced algorithms that modify biometric data prior to storing it, thus upholding the original data's integrity while ensuring the information appears invalid to cybercriminals if they try to access it.
- **Adopt technical controls**. Various technical controls can also help organizations protect biometric data. Namely, encryption techniques and access controls (e.g., deploying the principle of least privilege, segregating operational networks and implementing multifactor authentication measures across workplace systems) can limit the risk of such data being compromised. Employers should also ensure that the technical controls used by third-party vendors align with their security standards to minimize possible supply chain vulnerabilities.
- **Educate employees**. Employers should be sure to educate employees on their biometric data collection protocols and ensure those responsible for handling and storing such data have been trained to do so safely. This education shouldn't be a one-time occurrence; employees should receive regular training, especially as biometric data risks and regulations continue to evolve.
- **Maintain compliance**. By working with trusted legal counsel, organizations can ensure their biometric data collection processes remain compliant with all applicable international, federal, state and industry-specific data privacy laws. Compliant practices may include developing clear protocols for obtaining consent from individuals before collecting biometric data, providing transparent communication on how this data will be used, implementing strict data storage and

disposal measures, and completing necessary data collection documentation. As data privacy legislation progresses, organizations should make it a priority to stay informed and adjust their data collection processes when needed.

- **Have a plan**. Creating cyber incident response plans can help organizations ensure necessary procedures are taken when cyberattacks occur to keep related losses to a minimum. These plans should be well-documented and practiced regularly, and they should address a range of cyberattack scenarios (including data breaches or ransomware incidents that involve the exploitation of biometric information).
- **Secure ample coverage**. Finally, employers should purchase adequate insurance to maintain financial protection against losses arising from security incidents involving biometric data disclosure. Employers can consult insurance professionals to discuss their coverage needs.

Conclusion

Collecting biometric data comes with serious risks. By understanding these exposures, staying up to date on the latest data privacy legislation and implementing proper safeguards, organizations can maintain secure and successful operations with biometric data collection. Contact us today for more risk management guidance and insurance solutions.
