Gallagher

Facial Scanning Technology: **Managing Compliance Risk for Retailers**

CLIENT ADVISORY

In the digital age, data collection has become an integral part of operations for retailers. With the advent of advanced technologies, businesses are increasingly utilizing facial recognition systems to enhance customer experience, streamline operations and provide an added layer of security in retail stores. However, this practice raises significant compliance, liability and ethical concerns that must be addressed to protect both the business and its customers.

The basics of facial recognition

1. **Image capture:** The process begins with capturing an image or video of a person's face using a camera. This can be done in real-time or by using pre-existing images.
2. **Face detection:** The system detects the presence of a face within the captured image. This involves identifying facial features such as the eyes, nose and mouth, and distinguishing the face from other objects in the image.
3. **Feature extraction**: Once a face is detected, the system extracts key features from the face. This can include the distance between the eyes, the shape of the cheekbones, the contour of the lips and other unique facial landmarks.
4. **Face mapping:** The extracted features are converted into a mathematical representation known as a faceprint. This faceprint is a unique set of data points that represent the individual's facial features.
5. **Comparison:** The faceprint is then compared against a database of stored faceprints. This database can contain faceprints of known individuals for identification purposes or be used to verify a person's identity by matching it with a specific faceprint.
6. **Decision making:** Based on the comparison, the system determines whether there is a match. If the faceprint matches one in the database, the system can identify or verify the individual.

What can go wrong?

Organizations that use facial recognition technology should be mindful of privacy and ethical concerns, particularly regarding consent and data protection. There are several legal liability pitfalls to consider, including but not limited to:

- **Privacy liability:** Customers may feel their privacy is invaded if they are unaware of or uncomfortable with being monitored through facial recognition systems.
- **Data breaches:** Biometric data is sensitive and, if breached, can lead to identity theft and other security issues.
- **Regulatory risk:** Non-compliance with data collection laws can result in regulatory investigations, fines and settlements, damaging the retailer's reputation and financial standing.

Risk management techniques

By proactively addressing these risks and implementing robust compliance and data protection strategies, organizations can better manage risks associated with facial recognition technology. As a first step, retailers should engage legal counsel to fully understand which laws they need to comply with. There are potentially a myriad of data protection regulations that may vary by region. In the United States, the California Consumer Privacy Act (CCPA) and the Illinois Biometric Information Privacy Act (BIPA) are two prominent examples of legislation that govern how businesses collect, store and use personal data, including biometric information like facial scans. In fact, multiple states have either introduced bills or already passed privacy laws relating to data collection requirements. In the European Union, the General Data Protection Regulation (GDPR) sets stringent requirements for data collection and processing, emphasizing the need for explicit consent and transparency.

Some general considerations include:

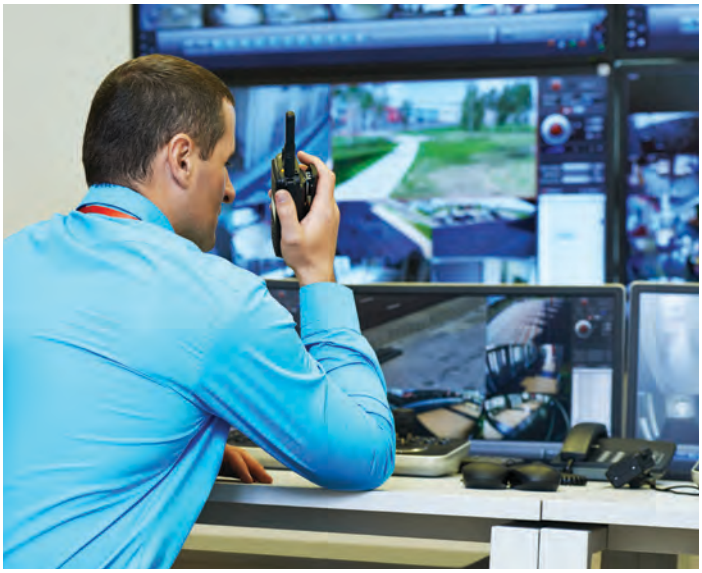
1. **Obtain explicit consent:** Before collecting biometric data, businesses must inform customers about the data collection process and obtain their explicit consent.
2. **Implement data security measures:** Retailers must ensure that collected data is stored securely and protected against unauthorized access and breaches.
3. **Provide data access and deletion rights:** Customers should have the right to access their data and request its deletion if desired.
4. **Limit data collection retention:** Only collect the minimum amount of data for the intended purpose and follow a written data retention policy.
5. **Conduct regular audits:** Regular audits and assessments should be conducted to ensure compliance with applicable laws and regulations.

Leveraging cyber insurance

Cyber insurance and other insurance policies may help organizations transfer risks associated with losses stemming from the latest emerging cyberthreats, including those posed by facial recognition technology.

However, the scope of cyber insurance coverage for wrongful data collection claims may vary greatly from policy to policy. Some cyber insurance carriers will specifically exclude these types of losses, while others may cover them, subject to specific underwriting protocols.

Cyber insurance applicants should be prepared to answer questions about their data collection practices and the steps they are taking to avoid legal liability.



Some of these may include:

1 **Data collection practices:**

- What types of biometric data are collected (e.g., facial recognition, fingerprints, iris scans)?
- How is consent obtained from individuals whose biometric data is collected?
- Are individuals informed about how their biometric data will be used and stored?

2 **Data storage and security:**

- How is biometric data stored (e.g., encrypted databases, cloud storage)?
- What security measures are in place to protect biometric data from unauthorized access or breaches?
- How long is biometric data retained, and what is the process for data deletion?

3 **Compliance and legal considerations:**

- Is the organization compliant with relevant data protection regulations (e.g., GDPR, CCPA, BIPA)?
- Are there policies and procedures in place to ensure ongoing compliance with data protection laws?
- Has the organization faced any legal actions or fines related to data privacy or biometric data collection?

4 **Risk management and incident response:**

- Does the organization have a formal incident response plan in place for data breaches involving biometric data?
- How often are security audits and risk assessments conducted?
- What training is provided to employees regarding data protection and privacy practices?

5 **Third-party vendors and partnerships:**

- Are third-party vendors involved in the collection, processing or storage of biometric data?
- What due diligence is performed on third-party vendors to ensure they adhere to data protection standards?
- Are there contractual agreements in place with vendors regarding data security and breach notification?

6 **Technology and system integrity:**

- What technologies and software are used for facial recognition and biometric data processing?
- How often are these systems updated and patched to address vulnerabilities?
- Are there measures in place to prevent and detect unauthorized access to biometric systems?

As data collection technology develops and compliance requirements grow, we expect it to become a key focus of cyber insurance underwriters in 2025 and beyond. Those organizations that can demonstrate a robust risk management strategy will be best able to transfer the risks associated with facial recognition technology and other data collection practices.

Insurance | Risk Management | Consulting

AJG.com **The Gallagher Way.** Since 1927.