Biometric privacy laws OEMs should be tracking

# 9 STATES, 10 BIOMETRIC DATA PRIVACY LAWS

OEMs face a patchwork of state biometric data privacy laws that may apply to data on their products. What does this mean for OEMs when it comes to data privacy?

With the increasing use of biometric data, it’s important for OEMs to understand the implications and legal ramifications. While there are many data privacy laws, here are some highlights of what OEMs should be aware of:

1. **New York**
   - **Key Action Item**: Disclosures, notice of data breaches, and consent requirements. Both consumers and the state can bring lawsuits in response to alleged violations of the law.

2. **Illinois**
   - **Key Action Item**: The law prohibits a business from selling personal information, and businesses must provide notice of the sale. Consumers have various rights under the law, including the right to instruct a business not to sell their personal information.

3. **Oregon**
   - **Key Action Item**: The law applies to any business that conducts business in Oregon and obtains, licenses, maintains, or stores biometric identifier data or biometric data. The broad scope of the law includes violations of the law.

4. **California**
   - **Key Action Item**: The law includes additional rights under the California Consumer Privacy Act (CCPA), specifically the right to instruct a business not to sell personal information.

5. **Arizona**
   - **Key Action Item**: The law prohibits a business from selling personal information and includes requirements for disclosure and consent.

6. **Texas**
   - **Key Action Item**: The law includes provisions for breach notification, security, and the right to instruct a business not to sell personal information.

7. **New York City**
   - **Key Action Item**: The law includes provisions for breach notification, security, and the right to instruct a business not to sell personal information.

8. **Washington**
   - **Key Action Item**: The law includes provisions for breach notification, security, and the right to instruct a business not to sell personal information.

9. **Arkansas**
   - **Key Action Item**: The law includes provisions for breach notification, security, and the right to instruct a business not to sell personal information.

A possible trend on the horizon: Zeroing in on geolocation data privacy

As geolocation data becomes more prevalent, it’s important for OEMs to understand the implications and legal ramifications. Why this law is significant for OEMs:

- Geolocation data is “personal information” under the CCPA.
- Both consumers and the state can bring lawsuits in response to alleged violations of the law.
- Significant for OEMs.

Key action items for OEMs

- Develop policies, procedures, and best practices.
- Invest in state-of-the-art technical and organizational data protection.
- Engage with regulatory compliance experts to identify and mitigate risks.

Looking for tips and best practices?

OEMs should consider the following tips and best practices:

1. **Compliance Audits**: Conduct regular audits to ensure compliance with relevant data privacy laws.
2. **Data Mapping**: Identify and map all data sources, including geolocation data.
3. **Data Minimization**: Only collect and process the minimum amount of data necessary.
4. **Data Retention**: Only retain data for as long as necessary, and then take reasonable steps to destroy it.
5. **Data Security**: Implement robust security measures to protect data at rest and in transit.

OEMs are responsible for managing data privacy risks, and understanding the implications of geolocation data privacy laws is crucial for maintaining compliance.