California Consumer Privacy Act (CCPA)

Overview: The **CCPA** was enacted in **2018** as a response to growing concerns over consumer privacy. It provides California residents with greater control over their personal information and establishes strict requirements for businesses that meet certain criteria. These criteria include businesses that:

- **Generate over $25 million in annual revenue**,
- **Collect personal data from 50,000 or more consumers, households, or devices**, or
- **Derive a significant portion of their revenue from the sale of personal data**.

Key Provisions:

1. **Consumer Rights**:
    - **Right to Know**: Consumers have the right to request details about the **personal data** a business collects, including:
        - What types of data are collected,
        - The purpose of the data collection,
        - The sources of the data,
        - The third parties with whom the data is shared.
        - This is essential for transparency, especially when AI is involved in processing or analyzing personal data.
    - **Right to Delete**: Consumers can request the deletion of personal data that businesses have collected, with certain exceptions. This is critical for businesses using AI to ensure that they can **delete data used for AI training** upon request, unless it's needed for operational purposes.
    - **Right to Opt-Out**: Consumers can opt out of the **sale of their personal data**. This opt-out mechanism must be made easily accessible on the business's platform. For AI systems, businesses must ensure they provide a **clear opt-out for data used in AI algorithms**.
    - **Right to Non-Discrimination**: Consumers cannot be discriminated against for exercising their CCPA rights, such as requesting data deletion or opting out of sales. For AI, this means ensuring that consumers are not penalized or treated unfairly for exercising their privacy rights.
2. **Business Obligations**:
    - **Transparency**: Businesses must clearly disclose how they collect and use personal data in **privacy notices**. These notices must be updated regularly and include information on consumer rights.
    - **Consumer Rights Requests**: Businesses must have processes in place to enable consumers to easily request their data, request deletion, and opt out of sales. This is particularly important for businesses utilizing AI, as consumers may request the deletion of data used in AI models, impacting how data is managed for model training.
    - **Data Protection**: Businesses are required to implement reasonable security practices to safeguard consumer data against unauthorized access, breaches, and

other threats. This applies to data used in AI, including **training datasets** and **user-generated data**.

3. **CCPA and AI:**
    - **Data Transparency in AI**: Businesses using AI must ensure that they disclose how personal data is being used in **training AI models** and how the models make decisions. This includes transparency around whether the data is being used for predictive analytics or decision-making that could affect consumers, such as in hiring, credit, or other key areas.
    - **Consumer Control Over Data Used in AI**: The CCPA requires businesses to provide consumers with control over their personal data, which includes the ability to request deletion of data used for AI training or analysis. AI models should be designed to allow data to be **erased upon request**, ensuring compliance with consumer rights under the CCPA.
    - **Data Minimization**: The CCPA's emphasis on limiting data collection to only what is necessary for a business's legitimate purpose aligns with AI best practices of data minimization. Businesses should avoid collecting excessive data for training purposes, ensuring that only relevant data is used and safeguarded.

Considerations for AI Businesses:

- **Right to Know**: AI businesses must be prepared to disclose the data they collect and how it's used in machine learning models. This includes providing consumers with the option to learn how their personal information influences AI-driven decisions.
- **Opt-Out of AI Usage**: If AI models rely on user data for personalized experiences, businesses must provide an **easy-to-use opt-out mechanism** for consumers who do not want their data used for such purposes.
- **Data Deletion in AI Systems**: Businesses need systems in place to **delete personal data used in AI models** if a consumer requests it, as well as to **cease using that data for future model training**. This can be a challenge for AI systems that rely on large datasets, especially those that continually evolve with user data.
- **Minimizing Data Risk**: Ensuring **data security** is especially important in AI, as AI models can inadvertently expose sensitive consumer data if not adequately protected.