Introduction by Department of Technology AIT Draft

In recognition of the increasing integration of artificial intelligence (AI) technologies into social media, video games, and other digital platforms, and in response to growing concerns over user privacy, data security, and the ethical use of AI, the federal government hereby establishes this regulation to protect the rights of consumers and ensure transparency in the use of personal data for AI purposes.

As AI continues to shape the digital landscape, it is essential that companies utilizing these technologies do so in a manner that respects the privacy, security, and informed consent of their users. This regulation mandates that social media, video game companies, and other digital platforms that collect, process, or share user data for AI modeling, training, or development must provide clear, separate, and identifiable AI Terms (AIT) to ensure consumers understand how their data will be used. Furthermore, it offers an opt-out option for users who do not wish for their data to be included in AI systems, and introduces a specific warning for instances where data may be used to develop AI for military purposes.

This regulation aims to create a balance between technological innovation and individual rights, providing a framework for companies to responsibly deploy AI while safeguarding public trust in these emerging technologies. By establishing clear guidelines for transparency, consent, and accountability, this regulation will foster a digital ecosystem that both encourages innovation and protects the fundamental rights of users in an increasingly AI-driven world.Federal Regulation on AI Data Use and User Privacy in Social Media and Video Game Companies

Section 1: Purpose and Scope

This regulation establishes legal standards and responsibilities for social media and video game companies that utilize artificial intelligence (AI) technologies and collect, process, share, or transfer user data to model, train, or develop AI systems. The regulation also mandates the inclusion of separate AI Terms (AIT), an opt-out option for consumers, and specific disclosures for military applications. The goal is to protect user privacy, promote transparency, and ensure responsible use of AI technologies.

Section 2: Definitions

For the purposes of this regulation, the following definitions apply:

1. Artificial Intelligence (AI): Any computational technology, system, or process that simulates human intelligence to perform tasks such as decision-making, pattern recognition, data analysis, or predictive modeling.

2. User Data: Any information collected from users, including but not limited to personal identifiers, behavioral patterns, preferences, social interactions, location data, biometric information, and in-game or online activity.

3. Data Processing: Any operation involving user data, including its collection, storage, analysis, modification, sharing, or deletion.

4. Third Party: Any entity other than the original data controller that processes, stores, or uses the data.

5. AI Modeling and Training: The process of using data to build, refine, or optimize AI systems for performance or predictive accuracy.

6. AI Terms (AIT): A clearly separate and identifiable section in website and software agreements that outlines the company's use of AI, how user data will be used, and user rights regarding the AI system.

Section 3: AI Terms (AIT) Requirements

(a) Separate AI Terms Section:

- All companies using AI technology for data modeling, training, or development must include a separate and clearly identifiable section titled "AI Terms" (AIT) on their websites, software, or any digital platforms where data collection occurs.
- The AIT must clearly state how AI technology is being used, what user data will be collected, how it will be processed, and if the data will be shared with third parties or used for AI modeling.

(b) Content of AI Terms (AIT):

- The AIT must explain:
  1. The specific types of data collected for AI purposes.
  2. How the data will be used in AI modeling and training.
  3. Whether the data will be shared with third parties for AI purposes.
  4. Whether the AI modeling involves military or government applications (if applicable).
  5. User rights, including the ability to opt-out (see Section 6).

(c) Visibility and Access:

- The AIT must be easily accessible and prominently displayed during the registration or sign-up process, and not buried in general terms and conditions.

- The AIT must be updated whenever changes are made to data collection or AI processing practices, with users notified of such updates.

Section 4: Data Collection and Use

(a) Consent for Data Collection:

- Companies must obtain explicit and informed consent from users before collecting any data intended for AI modeling, training, or development.
- Consent must be explicitly tied to the AIT and clearly distinguishable from general terms of service agreements.

(b) Data Minimization:

- Companies shall only collect data necessary for the specific AI-related purposes outlined in the AIT.
- Data irrelevant to the AI model's development or training should not be collected.

Section 5: Data Sharing with Third Parties

(a) Disclosure of Data Sharing:

- Companies must clearly disclose in the AIT any plans to share user data with third parties for AI training, modeling, or development.
- Third parties must adhere to the same privacy, security, and consent standards required by this regulation.

(b) User Control Over Data Sharing:

- Users must be provided with the option to opt out of data sharing with third parties for AI-related purposes without penalty or restriction to their service usage.

Section 6: Opt-Out Option for AI Data Use

(a) Right to Opt-Out:

- All users must be given the option to opt out of having their data used for AI modeling, training, or development.
- The opt-out process must be simple, clearly available in the AIT section, and cannot involve any penalty or loss of service functionality for the user.

(b) Notification of Opt-Out:

- Users who opt-out of AI data use must receive a confirmation that their data will no longer be used for AI training or modeling purposes, both internally and with third parties.

(c) Data Retention for Opt-Out Users:

- Any user data collected prior to opting out must be deleted or de-identified within 30 days of the opt-out request, unless the data is required for legal or contractual obligations.

Section 7: Military Application Warning

(a) Special Warning Label for Military AI Use:

- If any user data is used, or is intended to be used, to train or model AI systems for military purposes or government surveillance, companies must include a prominent warning label in the AIT.
- The label must explicitly state:

"WARNING: User data collected through this platform may be used for AI modeling or training for military purposes or government surveillance applications."

(b) User Consent for Military AI Use:

- Separate explicit consent must be obtained from users before any of their data is used for AI models with military applications. The consent must clearly disclose the nature of the military use and its potential impact on user privacy and security.

Section 8: Data Security and Privacy

(a) Security Measures:

- Companies must implement industry-standard data security measures, including encryption, access controls, and monitoring systems to protect user data from unauthorized access, modification, or loss.
- These security protocols apply both to internally processed data and data shared with third parties.

(b) Data Anonymization and De-Identification:

- User data shared with third parties for AI modeling must be anonymized or de-identified unless explicit consent is obtained from the user.
- Re-identification of anonymized data is strictly prohibited unless explicitly agreed upon by the user.

Section 9: Accountability and Transparency

(a) Transparency Reports:

- Companies must issue annual transparency reports outlining their AI data collection and sharing practices, including the type of data collected, the purposes for AI modeling, and any third parties or military entities involved.
- Reports must be publicly available and include summaries of data breaches affecting AI data.

(b) Internal Review and Audits:

- Companies must conduct internal audits of their AI-related data practices to ensure compliance with this regulation and the AIT.
- Audits must assess whether collected data aligns with the declared AI purposes and whether user privacy has been adequately protected.

Section 10: User Rights

(a) Right to Access and Data Portability:

- Users shall have the right to access their data collected for AI purposes and request a copy of their data in a machine-readable format for portability to another platform or service.

(b) Right to Deletion and Correction:

- Users may request deletion or correction of any personal data collected for AI modeling, except where data is retained for legal obligations or essential service functions.

Section 11: Penalties and Enforcement

(a) Penalties for Non-Compliance:

- Violations of this regulation will result in civil penalties, including fines based on the severity and scope of the violation.
- Intentional violations of user consent or failure to provide a military AI warning will result in escalated penalties, including potential criminal charges.

(b) Enforcement Authorities:

- The Federal Trade Commission (FTC) and other relevant agencies will oversee enforcement and investigations of complaints filed under this regulation.

Section 12: Effective Date

This regulation will take effect six months from the date of adoption, with an additional grace period of six months for companies to achieve compliance.