Institute for Youth in Policy

5214F Diamond Heights Blvd #3055
San Francisco, CA 94109

+1 (509) 565-0545
eic@yipinstitute.org
www.yipinstitute.org

Data Privacy & Protection Trends in Social Media

Technology Policy, Institute for Youth in Policy

November 2025

I. Executive Summary

The advancement of social media and artificial intelligence is outpacing regulation, exposing users to data misuse, surveillance, and large-scale breaches. Since the 2000s, attention-based platforms have prospered with limited oversight. Although policies such as the EU's GDPR have served as digital policy benchmarks, regulation in the US remains fragmented at the state and federal levels. Social media platforms such as Meta, X, and TikTok face criticism for having opaque data practices and AI data use, prompting stricter surveillance such as the 2025 TikTok divestiture framework.

Young people are demanding more transparency, consent and ethical data use by companies. Youth grow increasingly distrustful of data-invasive platforms, yet many are not familiar with the privacy policies of various digital platforms. Policymakers are considering several strategies to federalize and enforce laws on data privacy and transparency. Social media platforms that prioritize the privacy of their users, transparency and consent will gain trust, whilst those that don't risk public disengagement, especially from youth. Ultimately, data privacy is now essential for user trust and app sustainability in the AI age.

II. Relevance

Data privacy and protection emerge are becoming increasingly important as more social media platforms become integrated into daily life. Current business practices by parent companies such as Meta and ByteDance have called into question issues such as aggressive data collection, manipulation and mining, along with the pervasive issue of data scraping and utilizing user data to train AI algorithms with users reporting automatic opt-in conditions. Issues such as these focus on the gathering and measurement of large amounts of user activity to extract meaningful insights and patterns that may go on to assist AI models in generating content and making decisions, potentially compromising on user trust and consent. The privacy policy and practices of big tech companies must align with expectations in transparency, and accountability to counter the current ambiguity surrounding data collection practices.

Enforcing regulatory compliance fosters trust and compliance from users and businesses alike. Consumer awareness is at a high, with a 2023 survey by the Pew Research Center indicating that 81% of U.S adults felt as if the data collected by companies will be used in ways that people are not comfortable with, and 70% saying that they have little to no trust in companies to make responsible decisions about how they use AI in their products. According to a 2025 analysis released by Usercentrics, compliance with regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) helps organizations and businesses mitigate the risks of unauthorized access to user data and the legal ramifications that could follow along with strengthening user trust.

This brief aims to contribute to this discussion through suggesting effective policy solutions that preserves the American digital ecosystem and national security interests.

III. Background

The rise of social media and digital advertising platforms such as Facebook, Google, Instagram, and TikTok has reshaped how personal data is collected and monetized. These platforms built business models around the extraction of user attention and information through algorithmic recommendation systems, which track digital behavior through cookies and app usage patterns. This data allows advertisers to target users with personalized ads that predict which messages will most influence their interests and purchases. The market cap of advertisements is ever-growing, with it reaching $259 billion in 2024; Facebook, for example, derives 98% of its annual revenue from advertising.

However, as the monetary value carried by user data grows, U.S. regulatory frameworks fail to keep pace. Federal privacy law in the United States remains fragmented as it is governed largely by sector-specific rules such as the Health Insurance Portability and Accountability Act (HIPAA) for health data or the Children's Online Privacy Protection Act (COPPA) for children's data, and an increasing patchwork of state-level legislation. CCPA took a step toward granting Americans more transparency and control over their digital information. Because the CCPA only applies to California residents, businesses operating across multiple states often maintain different compliance systems depending on the consumer's location. California's law has effectively become a de facto national standard, as companies frequently adopt CCPA-level protections nationwide rather than build separate systems. This inconsistency creates uncertainty about enforcement and raises compliance costs for businesses.

In contrast, the GDPR, adopted in 2016, established a comprehensive, rights-based approach to data protection, where data protection is treated as a fundamental human right. Although not globally applied, the GDPR demonstrates what a standardized, enforceable framework for digital protections could look like: it applies uniformly across all member states, strong monetary penalties exist (up to €20 million or 4% of the company's worldwide annual turnover), each state has a Data Protection Authority to enforce compliance, and people have a clearly-defined list of rights.

Despite state efforts and growing awareness, the U.S. continues to experience frequent and large-scale data breaches such as the 2013 Yahoo breach affecting 3 billion accounts and the 2025 exposure of a Chinese surveillance database containing 4 billion records. These incidents show that current safeguards remain inadequate, especially for youth whose digital footprints are far broader than those of older generations. This brief explores whether the United States can evolve toward a federal framework that meaningfully safeguards data privacy.

IV. Policy Problem

The rapid growth of social media has begun to outpace the regulations meant to protect users' personal data. Social media platforms such as TikTok, Meta, and X collect an extensive amount of user information, varying from browsing history to messages and targeted advertisements. However, the absence of a comprehensive federal data privacy framework in the United States has left users vulnerable to large-scale data breaches and unauthorized sharing of data. State-level laws, like the CCPA were the first steps taken by the California state government to address users' concerns and provide some level of protection. However, the act makes it difficult for national platforms to fully comply due to different

state rules regarding privacy and their complexity. This is because the CCPA, being the only act that provides the most protections for consumers, covers only eight of the fifteen data privacy protections identified by privacy advocates. Other states, such as Maine and Nevada, have closely followed but have fallen short in terms of covering consumer protections, while many states have pending or no legislation at all.

At the same time, platforms are increasingly using data to develop and train artificial intelligence systems, raising further concerns about transparency and how users' personal information is being repurposed beyond the original platform. For example, foundation models are large AI models that are trained on data collected from the internet. Many companies such as OpenAI, refuse to disclose the data they use, making it difficult to know if personal information or copyrighted materials are being used without the users' knowledge. Recent enforcement actions in the U.S. such as the Federal Trade Commission's $1.3 billion settlement with Meta over privacy violations on Facebook and Instagram, depict that even major platforms that are used worldwide can fail to protect sensitive information. Efforts such as the September 2025 TikTok executive order, which implements stricter U.S. data security measures, show that policymakers are beginning to shed light on this critical issue. However, there is still no set standard that clearly defines how personal data can be collected and used, leaving millions of users, particularly younger audiences, exposed to privacy risks.

V. Notable Stakeholders

I. President Donald J. Trump and the U.S Government. These stakeholders introduced and signed an executive order allowing TikTok to continue its operations, involving data collection and mining under strict conditions. Requirements such as limiting TikTok parent company's shareholder value and restricting access to American users' data were introduced in this legislation. This order was signed to prevent the popular social media platform from being banned in the United States.

a. As of September 2025 ByteDance, the Chinese parent company of TikTok, retains less than 20% ownership of the social media platform, and is also excluded from the security committee, under the new U.S joint venture. This renewed ownership structure and restrictions are essential to protect users' data privacy. By limiting ByteDance's ownership stake of TikTok, the company's financial influence and control over U.S. operations, such as the managing of user data, algorithm oversight and content moderation, would be significantly reduced. The value of this ties further into the geopolitical tension between the United States and China as concerns over foreign interference and surveillance drives American policymakers to prioritize domestic privacy protocols and control efforts.

II. Oracle and Consortium are the majority owners and operators of TikTok's U.S application, which ensures that the decision-making and security measures are managed domestically, with minority input from foreign stakeholders. Oracle acts as the platform's security provider and independently monitors the behavior and safety of all operations in the United States. This presence is essential as TikTok's diverse American user base, including adolescents, young adults and middle-aged adults, requires locally-governed security measures and protocols closely aligned with U.S. laws and user expectations. TikTok has 117.9 million monthly active users in the U.S., with over half of weekly active users aged between 18 and 34. Around 25% of U.S. users are aged 10–19, 22.4% are 20–29, and another 21.7% are 30–39, marking that this platform is not only utilized by adolescents, but by young adults and middle-aged adults as well. This domestic oversight can foster improved trust among all age groups who engage with the platform differently.

III. American Content Creators and Users; the over 117 million Americans who utilize the TikTok application for entertainment, business and profit-making initiatives.

- The privacy and security concerns of these users are the main concerns surrounding data privacy and protection trends on social media platforms. The protection of user privacy is vital as social media platforms collect vast amounts of personal and sensitive information, such as one's financial details or medical information, that when misused can lead to damaging results; issues such as identity theft, scams, financial loss and data manipulation. Events like these cause widespread panic and anxiety for Americans, as users suffering from privacy violations often experience stress, fear and loss of control over

IV. their personal information, which causes a significant impact on their mental and physical well-being. Businesses and platforms also lose the trust of their user base, leading to damages done to their reputation and substantial financial consequences stemming from both legal ramifications and poor public perception. The Government also faces challenges in offsetting foreign interference and surveillance that threaten public safety and national security. Data protection helps mitigate these possible data breaches and exploitation from ill-intentioned individuals along with mitigating instances of public unrest and concern.

V. Privacy Advocates such as Gibb Mura who filed class-action child privacy lawsuit against TikTok and their parent company ByteDance, as well as Federal Regulators who influence laws and regulatory efforts such as GDPR and Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA).

VI. Social Media Platforms are the comparable competitors who are also subject to privacy concerns and scrutiny along with increasing regulatory pressure.

- A. According to a 2025 study by Incogni, platforms such as Discord, Pinterest and Quora are found to have better data privacy records, while TikTok and Meta's platforms faced high penalties for poor privacy protection practices with Meta alone being hit with a record-breaking 1.2 billion euro fine by the GDPR in 2023. For instance, Discord was found to limit user data collection and refuses to have user data be utilized to train AI models. Pinterest was found to provide comprehensive opt-out options allowing their user base to control the usage of their data. Quora collects minimal user data and does not aggressively mine data or feed AI models.

VI. Impact on Young People

Over the years, young users have become increasingly wary about the ways their data is being collected, stored and used. When platforms are publicly flagged as "privacy-invasive" such as TikTok and Meta in Incogni's 2025 Privacy Rankings, distrust grows, not just in those platforms flagged but social media platforms as a whole. As a result, young people are pressuring brands to adopt more transparent and ethical approaches to data use and collection, or limiting and avoiding their use of platforms deemed unsafe.

This has resulted in young people adopting a more guarded behaviour online. The lack of privacy might encourage the youth to adopt anti-social online behaviour: sharing less, removing location tags, etc. Empirical research from Cornell University demonstrates this, as awareness of privacy risks is shown to suppress sharing, as well as limit personal expression and social engagement, particularly for millions of youth globally who use social media to open up freely and develop/find an identity.

Society is entering the new and fourth industrial age, characterized by AI, big data, and technological fusion. This is already raising new concerns about data misuse among young people globally. Knowing this, young people and adolescents are expressing increased discomfort with the geometric growth of AI's pervasiveness. This could create anxiety, exacerbating an already suffering sense of lack of control among the younger generation.

Additionally, young people worry about their "digital footprint," or information about a particular person that exists on the internet as a result of online activity. Old posts, photos, and videos could resurface later during sensitive and pivotal times like college admissions, job applications, or public scandals. Considering these factors, the fear of being targeted and manipulated by algorithmic content diminishes the youth's interest and trust in certain platforms.

Furthermore, the digital divide is the gulf between those who have ready access to computers and the internet and those who do not. This digital disconnect across the globe is deepening; hence, not every youth has equal digital literacy about the accessibility of privacy protections and how to use it. According to a UK Study by the Children's Commission for England, children aged 8-15 sign up for social media services without understanding the Terms & Conditions (T&C). In a survey by the UK regulator Ofcom (2020), 67% of adolescents aged 12-15 agreed that they "usually accept the T&Cs without reading them" due to the inaccessibility of these legal documents. In fact, many T&Cs are intensive in volume and difficulty, with Instagram notably having 17 pages and 5,000 words. Other youth-focused apps also have privacy policies written at an average grade reading level of 12.78 (college level), which is well above the RGL of many users.

On the contrary, platforms that invest in privacy will likely gain loyalty from users, especially youth. An example of this is the TikTok divestiture framework. In the pursuit of protecting national security and user data, the TikTok divestiture framework is a plan by the US government, requiring ByteDance (the Chinese parent company of TikTok) to sell or separate its US operations to an American-controlled entity. However, if implemented, the new US-based algorithms could hurt small creators, limiting their reach and monetisation opportunities.

Ultimately, we can expect to see young people demanding better tools for transparency and privacy. In the coming years, we can imagine that there'll be a rise in digital activism among youth, abandoning apps that mishandle data.

VII. Policy Options

Repeated data breaches and policy violations by major platforms have highlighted the need for more definite and enforceable policy solutions. Issues such as inconsistent state-level regulations, the use of users' data for AI training and algorithmic recommendations, and the limited consequences for violations depict that existing policies fail to adequately protect users' data and privacy rights. Therefore, there are several policy solutions that can address the ongoing concern regarding the transparency of data privacy and protection on social media platforms.

I. Create a Federal Data Privacy Standard with Opt-In Consent.

a. Currently, the U.S. uses a patchwork of state-level laws, such as the CCPA and the Virginia Consumer Data Protection Act, a law that provides Virginia residents with certain rights collected by businesses. A national framework would make privacy laws uniform across states, and this framework would consist of an opt-in consent standard, requiring companies to get explicit permission before collecting or sharing personal data. "Explicit" permission means that consent has to be obtained through an affirmative action, such as a pop-up notice requiring users to check a box before data collection.

II. Increase transparency and Accountability for Data Users.

There is also a need to improve transparency regarding how social media platforms repurpose user data used for reasons such as training artificial intelligence systems. While most companies send notifications when their terms of service change, the details of data collection and usage are buried in long and technical legal documents that few users read or fully understand. According to researchers, many large language models are trained on datasets that are inconsistently documented and poorly understood, also opening the door to legal and copyright risks. This lack of transparency in data documentation mirrors the main issue that social media users face today: they hardly know when or how their data is being used. To address this, companies could be required to provide clear and easy-to-read "data use summaries." If more companies begin following similar measures, this policy can expand to all major social media companies, allowing users to easily see what information is collected, how it is being repurposed, and whether this data is being shared with third parties.

III. Strengthen Federal Enforcement and Accountability.

a. It is difficult to properly gauge how companies are held accountable when they break policies and regulations. The FTC itself acknowledges that companies collect a vast amount of consumer information, only a fraction of which consumers proactively share. Commercial surveillance is the collection and analysis of mass data, which could potentially raise the risks and stakes of data breaches and inaccuracies in the automated systems and algorithms that analyze it. To address this, FTC's statutory authority must be expanded so that the agency can impose escalating fines, issue probationary monitoring, and require mandatory independent audits. Furthermore, the FTC is already taking action by issuing the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking. The ANPRM is hoping to provide results regulating companies' data privacy and data security practices. Allowing the FTC to issue higher sanctions or conduct ongoing privacy audits could push companies to take data protection more seriously. Therefore, stronger enforcement, as seen with the ANPRM, highlights that stronger enforcement is feasible.

VIII. Policy Options

The September 2025 executive order highlights a significant attempt in balancing the national security of the United States; preserving the digital economy and landscape for American citizens. The future of data privacy and protection in social media will be continuously shaped by the evolving landscape of strict regulation, demands for transparency and the integration of advanced technologies. Businesses should prioritize incorporating improved privacy protection methods and operations, such as minimally collecting user data under clear guidelines and conducting regular business assessments and privacy audits to hold themselves accountable. These efforts would align with the rising consumer expectations, such as improved user control over their data, transparent privacy policies that align with regulation along with accessible explanations and minimal data collection, when it comes to handling their data and the increase in regulatory efforts.

The United States' TikTok deal marks a precedent in regulating how digital technology platforms can be managed through the enforcement of data sovereignty, which outlines how data produced on the platform within the boundaries of the United States is handled. Upholding data privacy and enforcing regulatory compliance will not only assist in minimizing the risks of data misuse, but also help foster a digital environment in which users are respected and protected. This essential focus on protecting user data and regulating business operations will be monumental in maintaining trust and safety, for not just the tens of millions of American TikTok users, but also for the broader digital ecosystem as well as regulatory efforts and privacy-enhancing technologies are further utilized to safeguard personal information in the digital space.