AMERICAN CHAMBER OF COMMERCE IN KAZAKHSTAN

11 September 2026

AmCham Issue Brief

Online Platforms Law and Age-Related Restrictions for Social Media

SUMMARY

Digital platforms share the same sentiment concerns of lawmakers and parents about the necessity to protect minors online. The industry supports the objective of creating a safer digital environment for underage users and recognizes the importance of strengthening safeguards as technologies, user behavior, and online risks evolve.

This objective should also be considered in the context of Kazakhstan's ambition to become an AI-driven digital nation, in which younger generations will play an important role. A 2026 study conducted by the Zhastar Scientific-Research Center under the Ministry of Culture and Information found that young people aged 14-18 integrate digital tools into their studies more rapidly than other age groups and view AI as a natural part of their future professional environment. It is therefore important to provide a space for and protect children from online risks while ensuring that they can access digital learning, develop AI literacy, communicate, create, and benefit from emerging technological opportunities, including through digital platforms.

In this context, we recall that the age restrictions on access to digital platforms proposed in the draft legislation is not a viable approach to regulating youth safety. In our view, blanket age bans on social media platforms are counterproductive and fail to address the core safety risks they intend to mitigate. Instead, they introduce unintended consequences

- Banning teenagers from established, highly regulated platforms does not eliminate their desire for digital connection. Instead of keeping them safe, outright bans simply drive digitally native youth to bypass restrictions using VPNs, borrow adult accounts, or browse anonymously. This effectively displaces users into a "gray zone" of unregulated and unsafe digital platforms, where safety guardrails and parental supervision tools do not exist.
- Absolute account bans completely override the fundamental role of parents in guiding and supervising their children's digital wellbeing. Because no two families are identical, parents are best positioned to calibrate digital rules that match their family values and their child's unique maturity. By shutting down supervised pathways, bans remove a key incentive for platforms to innovate and build a protected, parent-supervised ecosystem, leaving parents with fewer tools rather than more. This has been recognised

recently by the French Constitutional Council, which found the French youth social media bill to be disproportionate that it did not provide any mechanism allowing parents or legal guardians to authorise access for their child to specific services, in particular, because it did not allow parents to account for the minor's age, level of maturity, family situation, and the nature of the service in question; and

- By replacing functional, visible product safeguards with hard barriers, account bans erode teenagers' trust in safety measures designed to protect them.

To protect minors online, platforms continuously develop protective measures informed by research and international best practices. They combine age-assurance tools, AI-based analysis, behavioral signals, user reports, and community guidelines with content and recommendation safeguards, restrictions on unwanted interactions and targeted advertising, safety notifications, and parental control mechanisms. These tools, applied throughout the user experience, are designed to protect minors in the digital space while enabling them to benefit from the opportunities it provides.

We believe these tools and approaches may also lay the foundation for the regulatory measures enabling young people to use digital tools while protecting users' privacy, safety and security.

PROPOSAL

1. Embracing Technologically Neutral Age Assurance over User Age Verification

None of the existing age verification tools deployed during the user registration process can simultaneously guarantee accuracy, targeted use, and personal data protection. Digital platforms continue to refine solutions that combine neutral age gates with privacy-preserving age estimation, allowing them to identify minor users while they use the platform.

Proposed mandatory age-filtering models require age verification not only for minors, but for all users generally, which in our view could be seen as an excessive and technically complex requirement. Specifically, forcing the mass collection of highly sensitive personal information, such as biometrics or government IDs, from the entire population violates principles of data minimization while simultaneously creating vulnerable, centralized database 'honeypots' that expose all users to severe cybersecurity risks.

Combining age self-declaration through a neutral age gate at registration with ongoing privacy-preserving age estimation is a more effective method for knowing whether users are teens or adults. This multi-layered age assurance waterfall relies on machine learning models that analyze existing, non-identifiable signals, such as account longevity, content viewing patterns, and search history, to dynamically apply minor protections.

In addition, platforms use AI tools and user reports to identify users who have misstated their age. When platforms suspect an account belongs to an underage user, they promptly apply protective restrictions, requiring suspected underage users to either add parental supervision or verify their age through secure, privacy-preserving methods (such as credit card verification, secure digital IDs, or encrypted, on-device selfie-based age estimation), suspending or blocking the account if verification is not completed. These tools work continuously and unlike a one-time registration mechanism, prevent access to content and features that are meant to be restricted for minors by users who intentionally misstated their age.

2. Content Restrictions & Recommendation Algorithm Regulation

Digital platforms share the government and societal concerns regarding the protection of the younger generation from age-inappropriate and harmful content. The industry works continuously with international and national experts in child development, adolescent psychology, and digital literacy to design safe algorithms, product architectures and community guidelines.

Users Under 13s: The strictest frameworks apply to audiences under 13 if such audiences are at all permitted on platforms. For example, on YouTube Kids, a specialized, standalone service designed specifically for younger children parental supervision is required and content undergoes rigorous screening and filtering to ensure it is appropriate for children. Personalized advertising and interactive features such as creation and comments are disabled.

Users Aged 13-17: For teenagers, platforms typically apply adaptive, graduated restrictions developed in consultation with external specialists and informed by parental feedback. On teen accounts, sensitive or mature content may be automatically filtered or entirely excluded from search results, short-form vertical feeds and dynamic recommendation sections.

Further, depending on the platform's architecture, teen accounts can either be protected by a complete block on direct messaging, or can be isolated from profiles that systematically publish mature content, preventing them from following or communicating with such accounts.

As recognized by the G7, recommendations can be designed to allow platforms to elevate high-quality, age-appropriate content and reduce exposure to riskier, low-quality content that may be inappropriate for young people.

Alternative methods of organization are far less likely to be useful or valuable for viewers than well-designed personalized recommendations. Chronological feeds can lead to spam and low-quality content surfacing higher in results. This could also make it easier for bad actors to take advantage of chronological ordering to reach more consumers with low quality or potentially

harmful content. In addition, a large portion of high-quality content, including canonical or educational videos, have been on the platform for years and would not be surfaced to users with a chronological feed. Trending feeds may not be relevant or useful for users. And contextual recommendations do not reflect an understanding of the user's journey or content needs and can further contribute to filter bubbles and exposure to less diverse content.

3. Social Interaction Restrictions

Beyond content, parents and users are also concerned about potential unwanted contacts with minors, particularly from users in other age groups. Digital platforms are consistently working to increase transparency around these interactions and restrict them beyond the teens' immediate, trusted social circle.

Privacy by Default Profiles: On some platforms default privacy settings restrict access to a minor's posted content to everyone except immediate followers they have personally reviewed and accepted. Furthermore, some platforms can proactively restrict younger users from connecting with or following accounts that systematically publish mature (18+) content, and minor accounts cannot accept follow requests from such profiles.

Regulating Content Creation: At the same time, platforms significantly regulate minors' ability to create and publish their own content. For example, on some platforms, teenagers under 16 are prohibited from conducting live broadcasts (live streams) independently without an adult visibly present, adult supervision or direct adult permission, and any newly uploaded videos are by default set to a private status (Private or Unlisted).

Restricting High-Risk Interactive Features: Similarly, for minor users, some platforms automatically restrict direct messaging capabilities, commenting, tagging, mentions, and the posting or sharing of external links or contact details to approved followers only or disable them entirely.

Proactive DM Safety Filters: On some messaging and social services, images containing nudity in direct messages (both incoming and outgoing) are blurred by default for all users under 16. Changing these settings requires parental approval through linked parental supervision accounts.

4. Advertising Algorithm Restrictions

Digital platforms recognize the potential risks of excessive commercial exposure on minor users and consistently implement elevated standards for regulating advertising tools. Leading services operate on the principle that children and teenagers require special protection from behavioral profiling and must not be exposed to aggressive marketing techniques or promotional materials for sensitive categories of goods and services.

Deactivating Personalized and Behavioral Ads: Traditional advertising mechanisms based on tracking browsing history, viewing habits, personal interests, and gender are disabled globally for users under 18 across many platforms. Platforms may also prohibit the use of commercial microtargeting tools, behavioral profiling, the uploading of third party databases, or using lookalike audience targeting to serve ads to teens. Consequently, minor users are shielded from personalized ad profiling, and ad delivery is shifted exclusively to a contextual basis (matching the topic of the video currently being viewed or search query) or restricted to basic regional parameters.

Strict Filters on Permissible Ad Categories: In addition to restricting targeting methods themselves, platforms may apply strict filters to permissible ad categories on teen accounts. Ads for gambling, alcohol and nicotine products, microloans and other high risk financial services, dating apps, and content capable of negatively impacting mental health (including weight-loss products, plastic surgery, and cosmetic procedures) may be completely blocked for teen accounts.

Curbing Impulse Spending and Commercial Features: To prevent financial exploitation and impulsive behaviors, platforms may restrict or deactivate mechanisms that drive impulse spending. For example, in-app purchases, microtransactions, and paid tipping (donations) during live streams may be either blocked, strictly regulated, or require parental permission.

5. Preventive Notifications & Safe Interface

Digital platforms recognize the digital wellbeing concerns that come with use of social media and have a number of different mechanisms to ensure safety of minors.

Combating Burnout and Screen Addiction: To prevent the risks of emotional burnout, screen addiction, and sleep disruption among teens, leading platforms use behavioral prevention mechanisms built directly into the user interface. For example, for minor accounts, platforms may automatically activate regular reminders to take a break (e.g., every 60 minutes of continuous use), alongside a built-in overnight "Sleep Mode" (or bedtime mode) that mutes notifications and reduces incentives for endless scrolling.

Real-Time Crisis Support and Intervention: In situations where minor users search for material on sensitive or high-risk topics (including mental health, depression, self-harm, eating disorders, or cyberbullying), immediate crisis intervention mechanisms may be triggered. Instead of standard search results, platforms can display dedicated safety prompts.

Proactive Technical Safeguards: Leading platforms also deploy proactive technical solutions to prevent more severe safety outcomes. For example, integrations with international tech initiatives and databases (such as NCMEC's Take It Down service) use digital hashing to proactively block the dissemination of intimate or sensitive images of minors before they are posted online. Platforms may also offer educational and informational modules to help teens

recognize online manipulation, phishing, and unfamiliar contacts, fostering digital safety skills among minors.

6. Parental Control Tools

Leading digital platforms enable parents and guardians to effectively exercise their parental rights and duties while participating in their teenagers' digital lives. Platforms consistently develop parental control tools designed to offer parents robust management mechanisms and transparency without overly intruding upon the child's personal privacy.

Maximum protection by default: For younger users (such as those under 13) baseline safety and privacy settings, including profile privacy, messaging restrictions, and strict content filters, may operate in a maximum protection state by default, and require direct, verified confirmation from a parent or guardian before they are changed.

Customizable digital boundaries: Supervision tools may allow parents to set daily app usage limits, schedule overnight "Sleep Mode" (which mutes notifications and sends automated replies), and regulate financial transactions and in-app purchases. Any significant administrative actions - such as starting live broadcasts, posting new media content, or attempting to modify account details and safety settings - may trigger automatic notification alerts for parents.

Supervising social circles safely: For platforms that support interactive social features or direct messaging, parents may gain access to metadata regarding their child's social circle. For example: they may be able to view a list of accounts their teen has messaged or added as friends, and receive notifications if their child reports someone or blocks a user. At the same time, the privacy of message contents is preserved.

Commercial transparency and controls: To shield minors from commercial pressures, platforms may provide parents with transparency tools to review ad history and configure commercial limits for their teen's account. This builds a protected environment while maintaining a balance between minor safety and digital autonomy.

CONCLUSION AND RECOMMENDATIONS:

In light of the above, we propose reconsidering the proposal to introduce age restrictions on registration and platform use for users under 16 years of age, in favor of establishing obligations for platforms themselves to deploy technological solutions that ensure minor safety.

The focus areas and approaches to user safety presented here are grounded in extensive, ongoing collaboration with child development specialists, parent communities, academic institutions, and government bodies, and are shared by leading market players.

While specific technical solutions may vary from platform to platform, the six pillars presented above collectively provide a foundation for the proportionate regulation of minors' access to social networks and digital platforms.

We would also like to emphasize that we continue to view the framework of authorized representatives for social platforms as a sufficient mechanism for cloud-based digital platforms operating in the Republic of Kazakhstan. In our view, this practice has proven effective in facilitating cooperation on content-related issues and, accordingly, does not necessitate establishing a physical local representative office in the country.

We appreciate the open and constructive dialogue with the authorities and remain committed to continuing working together with the authorities, law-makers, expert community and civil groups in the Republic of Kazakhstan to protect the safety of Kazakh youth online.

AMERICAN CHAMBER OF COMMERCE IN KAZAKHSTAN

ADDENDUM

Minor Safety Features by Global Platforms

GOOGLE:

Content Safeguards & Algorithmic Controls

- Dedicated Under-13 Experience (YouTube Kids): A standalone app built from the ground up for younger children. Content undergoes rigorous automated and human review, comments and content uploads are disabled, and parents have a dedicated dashboard to hand-pick approved channels.
- For pre-teens transitioning beyond YouTube Kids onto YouTube main, parents can link their child's account to their own Google Account and select from three strictly moderated content tiers: Explore (ages 9+), Explore More (ages 13+), and Most of YouTube (which still excludes mature, 18+ content).
- Google's recommendation systems for teens are guided by strict Teen High- and Low Quality Content Principles developed with child development experts. These systems actively reduce the repeated recommendation of sensitive topics (such as body comparison, physical idealization, or social aggression) to protect teen wellbeing, even if the individual videos do not violate Community Guidelines.

Social & Interaction Safeguards

- To completely eliminate stranger-contact and grooming risks, direct messaging is entirely disabled globally for all users under 18 across YouTube.
- For all registered teen accounts (ages 13–17), video uploads (including Shorts and longform videos) are automatically set to Private by default, ensuring their videos are not publicly discoverable unless explicitly changed.
- A teenager's personal "Liked Videos" playlist is set to private by default, eliminating public peer validation pressure and reducing visible metrics.
- Google maintains a very high bar for broadcasting. The minimum age required to host a livestream on YouTube is 16. Accounts under 16 cannot broadcast independently, and any streams featuring children under 16 without clear, visible adult supervision are promptly removed.
- On any content designated as "Made for Kids," interactive features—including public commenting, live chat, and notifications—are completely disabled by default to prevent uninvited peer or commercial contact.

Advertising & Commercial Safeguards

- Google does not permit personalized targeted advertising for any child or teen globally. For all users under 18, ad targeting based on age, gender, or inferred interests is completely disabled and cannot be overridden by parents. Minor accounts are served

strictly non-personalized, contextual ads based on the topic of the video currently being viewed.

- Across Google Search and YouTube, Google blocks sensitive ad categories from appearing on under-18 accounts.
- On YouTube Kids, Google strictly prohibits ads in additional categories such as food and beverages (F&B), religion, politics, or ads containing scary imagery or crude humor.

Wellbeing, Notifications & Crisis Support

- For all logged-in minor accounts (ages 13–17), Google automatically enables "Take a Break" and "Bedtime" reminders. These default to showing full-screen takeovers every 60 minutes of continuous viewing on YouTube, urging teens to log off. Furthermore, minors and parents can set daily time limits for how long they can scroll on the YouTube Shorts feed, including the ability to set the limit to zero.
- Google automatically silences notifications and suppresses notification vibrations between 10:00 PM and 8:00 AM for all accounts registered to users under 18.
- Additionally, autoplay is not enabled by default for minors.
- Google is a founding partner of NCMEC's Take It Down initiative. This service allows teens or their parents to generate a unique cryptographic digital fingerprint (a "hash") of an intimate image directly on their device. Google uses this hash to proactively block and prevent the image from being uploaded or shared across YouTube, Google Drive, or Google Photos, without Google ever seeing or storing the actual image.
- Google's "Be Internet Awesome" Program: A comprehensive, gamified digital literacy curriculum (featuring interactive games like Interland) designed to teach kids and teens how to identify online scams, handle encounters with strangers, and secure their personal data.

META:

Account & Content Safeguards

- **Under-13 Account Prohibition:** Meta strictly prohibits children under the age of 13 from creating or maintaining accounts across Instagram and Facebook.
- **Default Built-In Protections (Teen Accounts):** Teen Accounts automatically place young users into protected experiences across Instagram, Facebook, and Messenger to limit unwanted contact and restrict exposure to inappropriate content.
- **Strict Content Restrictions & Rating Criteria:** Teens are automatically placed into the strictest setting of Meta's sensitive content controls, limiting recommendations of sensitive content in Explore and Reels. Additionally, content recommendations are guided by 13+ movie ratings criteria, restricting teens from viewing 18+ content in Search or following accounts that post 18+ material.

Social & Interaction Safeguards

- **Default Private Account Settings:** Accounts for teens under 18 on Instagram and Facebook are set to private by default, requiring teens to accept new follower requests before non-followers can view or interact with their content.
- **Strict Direct Messaging Restrictions:** Teens are placed in the strictest messaging configuration, allowing direct messaging only from accounts they already follow or are connected to. Meta also applies additional DM protections to prevent potential unsafe contact from unconnected adults.
- **Tagging and Mention Controls**: Interaction features are restricted so that teens can only be tagged or mentioned by users they explicitly follow.
- **Anti-Bullying & Keyword Filtering:** The most restrictive version of Meta's anti-bullying tool, Hidden Words, is automatically enabled on Instagram to filter out offensive words and phrases from teens' comments and DM requests.

Screen Time & Wellbeing Safeguards

- **Daily Time Limit Reminders:** Automated notification prompts remind teens to exit Facebook and Instagram after completing 60 minutes of daily usage.
- **Overnight Sleep Mode:** Sleep Mode automatically activates between 10:00 PM and 7:00 AM on Facebook and Instagram, muting overnight notifications and issuing automatic replies to incoming direct messages.

Parental Control & Supervision Safeguards

- **Progressive Autonomy Controls:** Teen Accounts operate on progressive autonomy, requiring users under 16 to obtain supervising parental authorization before changing default safety settings to a less restrictive state.
- **Parental Insights & Tools:** Parental supervision tools provide caregivers with visibility and oversight, helping parents guide their teenagers' online experiences.

Age Assurance & Policy Enforcement Safeguards

- **Proactive AI & Text-Based Detection:** Meta utilizes proactive text analysis technology capable of detecting age admissions in 26 languages, alongside artificial intelligence models designed to spot age-lying and prevent adult-minor interactions.

Multi-Option Age Verification:

- **Multi-Option Age Verification:** When Meta detects a suspected age misrepresentation, or when a user attempts to change their listed age from under 18 to 18+, it prompts the user to confirm their age. Rather than mandating a single method, Meta offers a choice of privacy-preserving options, including facial age estimation (which does not require identity documents), verification via a trusted ID, or interoperable "Age Key" technology.

This multi-option approach is designed to establish age confidently while minimizing the collection of personal data and avoiding the exclusion risks that come with any single mandatory method.

- **High-Harm Proactive Enforcement Rate:** Proactive detection technologies identify and action 98% of high-harm violation content (such as CSAM, terrorism, or self-harm) before users report it.