

A comprehensive European framework for safe social media

3 September 2026

The upcoming State of the Union address on September 16 could mark a pivotal moment for European digital policy. Faced with the invalidation of France's blanket ban and growing national divergence, the European Commission could, according to Politico, be shifting toward a more flexible model of restrictions coupled with parental carve-outs.

Alternatively, the European Commission could build a structural framework grounded in "safety by default". By pairing the default removal of toxic design features with progressive age-gating and mandatory interoperability, the Commission could ensure "safe social for all", innovation, and genuinely empower the citizens it seeks to protect. Such a renewed framework would foster a competitive European tech ecosystem while providing robust, structural protections for minors.

This position paper outlines the structure and content of a proposed European framework that reconciles the developmental child-safety approach with market-correcting interventions, which are well legitimised in the United States as well, following the recent settlement of the *Meta* case.

By integrating [FOTI "Smarter Ban" strategy](#) with the [Special Panel's](#) recommendations, it balances strict protections for minors with the promotion of an open, innovative, and sovereign European tech ecosystem.

1. Imposing the "safe by design" principle

The foundation of this new framework would be the mandatory implementation of "safety by design" and "safety by default" for all social media and digital services accessible to minors.

Prohibition by Default of Toxic Features: Instead of a blanket ban, the framework should mandate that addictive and harmful design features (such as infinite scroll, autoplay, algorithmic recommenders optimised for engagement, push notifications, and tracking) are deactivated by default. This would ensure that social network services are not, by default, used to nourish a detrimental business model. Progressive access to these features should be granted only after successful age verification.

Shifting the Burden of Proof: Providers must proactively demonstrate that their products, services, and new functionalities are safe before they are deployed to the market and made accessible to minors. A positive side effect of this would also be to shift competition between social networks onto safer ground.

2. Gradual access age (starting at 13) and regulated feature rollout

To support a developmental approach to child safety, the framework establishes a harmonised, gradual age-access framework to prevent the fragmentation of the European Single Market.

Base Access Age of 13: A harmonised EU-wide access restriction should be established for children under 13. Below this age, children shall not be able to create an account and may only access highly restricted, safe social media environments under strict parental supervision or for structured educational purposes.

Controlled Access to Mature Features via Delegated Acts: From the age of 13, adolescents enter a stage of "evolving autonomy". Access to platforms would remain subject to strict safety controls by default. However, access to more complex or potentially risky functionalities should be strictly gated behind robust age verification. The exact parameters of these features would be defined through delegated acts, drawing directly on the ready-made framework of the October 2025 DSA Guidelines on protecting minors, which explicitly specify harmful design features.

National Precautionary Measures: While the EU-wide baseline is 13, Member States retain the right to introduce additional precautionary access restrictions for adolescents above 13, acknowledging varied cultural contexts across Europe.

3. Age assurance, parental controls, and empowering third-party tools

This framework should empower users and their families to reclaim control over their digital environments through third-party tools.

Privacy-Preserving Age Controls: This framework would mandate proportionate, accurate, and highly secure age-assurance systems. Crucially, these systems must uphold the highest data protection standards, ensuring that neither the platform nor the verification provider can track or identify the user.

Integration of Safety Apps and Plugins: Market demand clearly indicates that European citizens want safer social media, as evidenced by the millions of downloads of challenger safety tools. This framework could legally protect interoperability of third-party applications and plugins (such as One Sec, No Scroll, Opal, and Brick) that allow users to block addictive features, add friction, and enforce screen breaks.

Preventing Predatory Gatekeeping: Users should be empowered to select their preferred digital wellbeing application as a default system setting, ensuring that their choice of protective tool is respected across the device. This fosters genuine competition based on the quality and efficacy of the assistance provided, rather than the gatekeeping power of the platform owner.

This requirement is made necessary due to the habitual predatory behaviours of gatekeepers (i.e. “scherlocking”), who frequently suppress independent innovations that threaten their business models. The recent implementation of a ["Pause" feature](#) by Google serves as a telling illustration of this pattern; by integrating functionality pioneered by independent tools, the platform effectively undermines those same innovators rather than fostering genuine competition.

4. Full interoperability mandate

A safety-by-design mandate is insufficient if it only consolidates the monopoly power of dominant platforms. To truly protect users, the framework could mandate full interoperability with dominant social networks and operating systems.

Building Bridges: Currently, dominant firms can shut down their safety tools and alternative networks with impunity, mainly to preserve their toxic business model. The interoperability mandate would force gatekeepers and VLOPs to open their closed networks, providing independent safety tools (like One Sec), portability tools and safe-by-design European services with stable, guaranteed access.

To ensure functionality, this interoperability mandate must secure stable technical access. For digital wellbeing applications, this means requiring operating systems and social network services to provide dedicated APIs that allow for real-time, reliable, and privacy-preserving interception of app launches. Such APIs must ensure that third-party tools can operate with the same stability, technical priority, and latency as native platform features, preventing them from being arbitrarily suppressed by battery management or system restrictions. Such third-party providers, building on existing services, can also offer age-appropriate solutions that safeguard children's participation rights.

Safety Through Competition: By breaking the network lock-in through portability and interoperability, families could switch to healthier platforms or utilise external safety plugins without losing their connections and friends. This would ensure platforms compete on the quality and safety of their services, rather than holding users hostage of toxic environments.

5. Final provisions: National enforcement in European concertation

To ensure these rules are applied rapidly and effectively, this framework should establish a robust, shared enforcement architecture that leverages both local agility and European coherence.

National Dispute Resolution and Sanctions: This framework should empower judicial authorities and Digital Services Coordinators to swiftly handle complaints, resolve disputes, and impose local sanctions on providers that fail to comply with safety-by-design or interoperability mandates.

Concerted European Enforcement: To avoid inconsistencies and fragmented legal environments, national actions should be coordinated through EU mechanisms, such as the European Board of Digital Services. In cases of persistent infringement causing urgent harm, the European Commission could retain the power to coordinate with national authorities to seek judicial orders for temporary service restrictions, thereby providing a powerful deterrent against non-compliance.

About FOTI

FOTI (Future of Technology Institute) is an independent European think tank tackling digital markets and tech monopolies. We design market reforms, press for enforcement, and back credible challengers.

[Futureinstitute.tech](https://futureinstitute.tech)