Stop Killing Digital Freedom Full

This initiative demands that EU institutions and member states stop censoring the internet and guarantee true online freedom of expression. In the wake of the UK's **COSA legislation,** the **OSA legislation,** the US's **KOSA legislation**—all widely criticized not only for curbing free speech but also for creating major security risks by discouraging the sharing of critical information— and the U.S. **BEARD Act**—which allows copyright holders to demand site-blocking orders without oversight—we propose the following concrete measures:

1. ## No Mandatory Biometric IDs
   Ban any requirement for biometric identification on social networks or online platforms—whether imposed by governments, EU institutions, or private companies—as per **Article 5(1)(h) of Regulation (EU) 2024/1689 – the AI Act**, which prohibits real-time remote biometric identification in publicly accessible spaces even for law enforcement, with only narrow exceptions; and as mandated by **Article 9 of Regulation (EU) 2016/679 (GDPR)**, which treats biometric data as a special category and forbids processing except with explicit consent.
   With this we include officially issued and government recognized documents and age verification though biometrics and IDs.
   Exception: Secure services where identity is essential (e.g., banking portals, official government/EU sites).
2. ## AI Profiling Only with Explicit Consent
   Prohibit the use of AI, including profiling and automated decision-making, unless users provide **explicit, informed, opt-in consent**, in strict alignment with **Article 22 of Regulation (EU) 2016/679 (GDPR)**, which grants individuals the right not to be subject to solely automated decisions that have legal or similarly significant effects—unless covered by a contract or otherwise legally authorized. Any system based on such profiling must also implement **human-in-the-loop safeguards**, the possibility to contest the outcome, and meet transparency duties under **Articles 13–15, 21, and 35 GDPR**.
   This protects sensitive personal data from being mined and weaponized.
3. ## Guaranteed Access to Legal Digital Content
   Guarantee access to legal digital content throughout the EU by outlawing **arbitrary, non-transparent content removal** or geo-blocking by platforms, in compliance with the **Digital Services Act (Regulation (EU) 2022/2065)** — specifically **Articles 8–10** on notice-and-action procedures, **Article 17** on appeal rights, and enhanced **transparency reporting** obligations. These provisions, combined with **Article 11 of the EU Charter of Fundamental Rights** (freedom of expression and information), ensure that content which is lawful remains accessible and that users can effectively challenge unjust removals.
4. ## Rock-Solid Free Speech Protections
   Defend the right to satire, humor and honest opinion online as guaranteed by **Article 11 of the Charter of Fundamental Rights of the EU** (freedom of expression and information). Platforms and intermediaries must enforce their terms of service in a **diligent, proportionate and objective** manner (§14 of the **Digital Services Act (Regulation (EU) 2022/2065)**), providing a **clear Statement of Reasons** for any moderation action (§17), and a **free, user-friendly internal complaint-handling procedure with timely remedy and escalation rights**, in line with §20.
   These safeguards ensure that lawful humor or critique cannot be arbitrarily limited, demonstrated by the "platform must pay regard to fundamental rights" principle already embedded in DSA's **Recital 38**.

5. Fair Online Billing Law

   Stop payment processors—even those operating cross-border under **PSD2 (Directive EU 2015/2366)**—from terminating financial services to platforms on a speech-related or arbitrary basis, which would otherwise constitute an **unfair trading condition or exclusionary practice** under **Article 102 TFEU**.

   We propose requiring processors to offer two service tiers:

   - **Selective-Service Tier**, where platforms consent to additional transparency and oversight obligations;
   - **Universal-Access Tier**, where **no processor may refuse service arbitrarily or on political grounds**, and may only unlink services based on **clear, public, non-discriminatory criteria** (similar to obligations currently imposed on "gatekeepers" under **Article 5 of the Digital Markets Act (Regulation 2022/1925)**).

     This principle aligns with ongoing Competition Commission scrutiny of Visa/Mastercard's opaque fee structures and dominance in the EU payments market.

6. Clamp Down on Payment-Processor Monopolies

   Introduce ex-ante and ex-post **anti-monopoly provisions**, enabling the European Commission and national competition authorities to sanction payment networks whose dominance leads to **vague, arbitrary requirements, mass contract withdrawals**, or **indirect censorship of platforms or users**—in breach of **Article 102 TFEU**.

   This would mirror enforcement against established dominant platforms, such as the Apple Pay **"self-preferencing" case**, where the Commission is evaluating whether app exclusion constitutes abuse of dominance.

   Platforms should also be able to invoke **structural or behavioral remedies**, including **access to alternative processors**, data portability, and meaningful **switching rights**, consistent with **DMA Article 5 and 6 obligations** applied to gatekeepers.

   The expansion of EU competition investigations into **payment processor fees and exclusionary practices in 2024–25** provides urgent momentum for this reform.

7. Universal VPN & Encryption Rights

   Guarantee that all EU citizens have the right to use strong encryption and Virtual Private Networks (VPNs), without interference or mandatory backdoors.

   Based on **Article 5(1) of the ePrivacy Directive (2002/58/EC)**, which enshrines the confidentiality of electronic communications—recognizing encryption as a core tool for protecting privacy and as a personal security tool.

   Reinforced by **Recital 35 of the draft ePrivacy Regulation (subject to finalization)** and by the **Charter of Fundamental Rights**, especially **Article 7 (Respect for private and family life)** and **Article 8 (Protection of personal data)**—which the European Commission has described as including the "fundamental right to encryption"

   No Member State may enact laws that prohibit the use of encryption tools—such as VPN clients, DNS-over-HTTPS providers, or end-to-end messengers—or require vendors or carriers to weaken them. Users must never be forced to decrypt or expose communications as a condition of access.

   No Member State may enact laws that allows government, companies and the EU itself, to access private communication without a noticed, transparent, due process, without a reasonable reason—that has to be proved reasonable by an impartial judicial review—and a warrant—given the ability for the offended party to appeal to it in a fair process and defend itself.

8. No DNS/IP Takedowns Based Solely on Private Copyright Claims

   Require that any DNS or IP-level blocking in the EU occurs only after impartial judicial review—not at the request of private parties—and that it respects transparency, notice, and

remedies.
Aligned with **Article 9 of the Digital Services Act (Regulation EU 2022/2065)**, which limits emergency blocking measures to cases where **public authorities or courts issue orders**, and mandates **prior notice to users**, **proportionate targeting**, and public justification.
Consistent with the **Copyright Directive (2019/790)**, particularly **Article 23** (treated as part of **Directive 2001/29/EC Article 8(3)** and **Enforcement Directive 2004/48 Article 3**), which directs Member States to provide injunctions **only via judicial bodies**, and prohibits ex-parte blocking based on private claims alone—for exactly the reasons stated by the CJEU in cases such as Scarlet, Netlog, and Telekabel
It's also requested that **Takedowns must**:

- Originate from an **authorized public or judicial order**, not copyright holders;
- Include **written notice** to the affected party;
- Be **disproportionate**, targeting specific infringing content—not entire domains or IP ranges;
- In the case of foreign claims, be enforceable **only if recognized in EU law**, preceded by due process.

9. Explicit Legal Immunity for VPN, DNS & Encryption Services

Affirm that providers of VPNs, public DNS resolvers, and encryption tools have legal protection from liability for content routed through their systems and cannot be forced into censorship roles.
Echoes the **safe-harbor regime of Directive 2000/31/EC ("e-Commerce Directive")**, in which **Article 14** shields hosting and mere-conduit providers from liability if they lack actual knowledge or act expeditiously upon notice—and **Article 15** prohibits general monitoring requirements, meaning no obligation to inspect traffic or filter data (e.g. universal IP or DNS scanning).
Reiterated and refined by the **Digital Services Act**, which preserves intermediary immunity for **"providers of mere conduit or access or caching or hosting"**, again barring national or private impositions on their neutrality or forcing them to act as platforms or filters.
Also protected under **Charter Articles 7 and 8**, because forcing encryption tools to act as surveillance gateways would violate both privacy rights and data-protection principles.
Prevent exceptions for artificial intelligence profiling or metadata scanning.

We then ask the EU to register this ECI by 01/10/2025 and to ensure that the laws are made and amended before the start of 2026.

By enshrining these principles in EU law, we'll safeguard our digital rights, bolster security, and keep the web open, free—and inconvenient for censors, both politically and economically.
The open web isn't just a luxury: it's the backbone of democracy, innovation and security. Let's ensure EU laws protect—not punish—our right to connect, share, and create.