Stop Killing Digital Freedom Semplified

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, the EU, or private companies.
   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 to profile users unless they have given *informed, opt-in* consent. No more "agree or you can't use our service" ultimatums.
   This protects sensitive personal data from being mined and weaponized.
3. **Guaranteed Access to Legal Digital Content**
   Protect consumers and creators from arbitrary takedowns or geo-blocks. If it's legal, it stays accessible.
4. **Rock-Solid Free Speech Protections**
   Defend the right to satire, humor and honest opinion online—within the bounds of local laws—without fear of reprisal or shadow-bans.
5. **Fair Online Billing Law**
   Stop payment processors from censoring platforms by cutting off services.
   - **Selective-Service Option**: Higher compliance requirements, stricter oversight.
   - **Universal-Access Option**: No additional demands, but processors can't exclude customers arbitrarily.
6. **Clamp Down on Payment-Processor Monopolies**
   Pass anti-monopoly rules that prevent processors from blackmailing platforms with vague demands, mass withdrawals, or censorship threats, directly or through third parties.
7. **Universal VPN & Encryption Rights**
   Ensure every EU citizen can legally use VPNs and strong encryption—no country can ban them or force backdoors. Security is not optional; it's fundamental.
8. **No DNS/IP Takedowns Based Solely on Private Copyright Claims**
   Insert a clause stipulating that **any content-access blocking at the DNS or IP level in the EU must originate exclusively from impartial judicial orders**, not private requests from rightsholders (e.g. streaming platforms or labels). These orders must be:
   • Transparent and publicly documented, in compliance with **Art. 9 of the Digital Services Act** (DSA).
   • Accompanied by **prior notice to the blocked party**, who in turn must have access to an **effective and timely legal remedy**.
   • **Proportionate**—targeting only the specific illegal content, **not entire IPs or domains** that affect legitimate services.-
   • Protection from foreign agents and claims—foreign claims about takedowns should not be acknowledged as valid.-
9. **Explicit Legal Immunity for VPN, DNS & Encryption Services**
   Guarantee that providers of encryption tools, VPNs, and public DNS services are **not liable for content routed through them and cannot be forced to act as private censors or**

surveillance gates. Only judicial authorities—not third parties, including copyright holders—may impose obligations affecting their neutrality.

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.