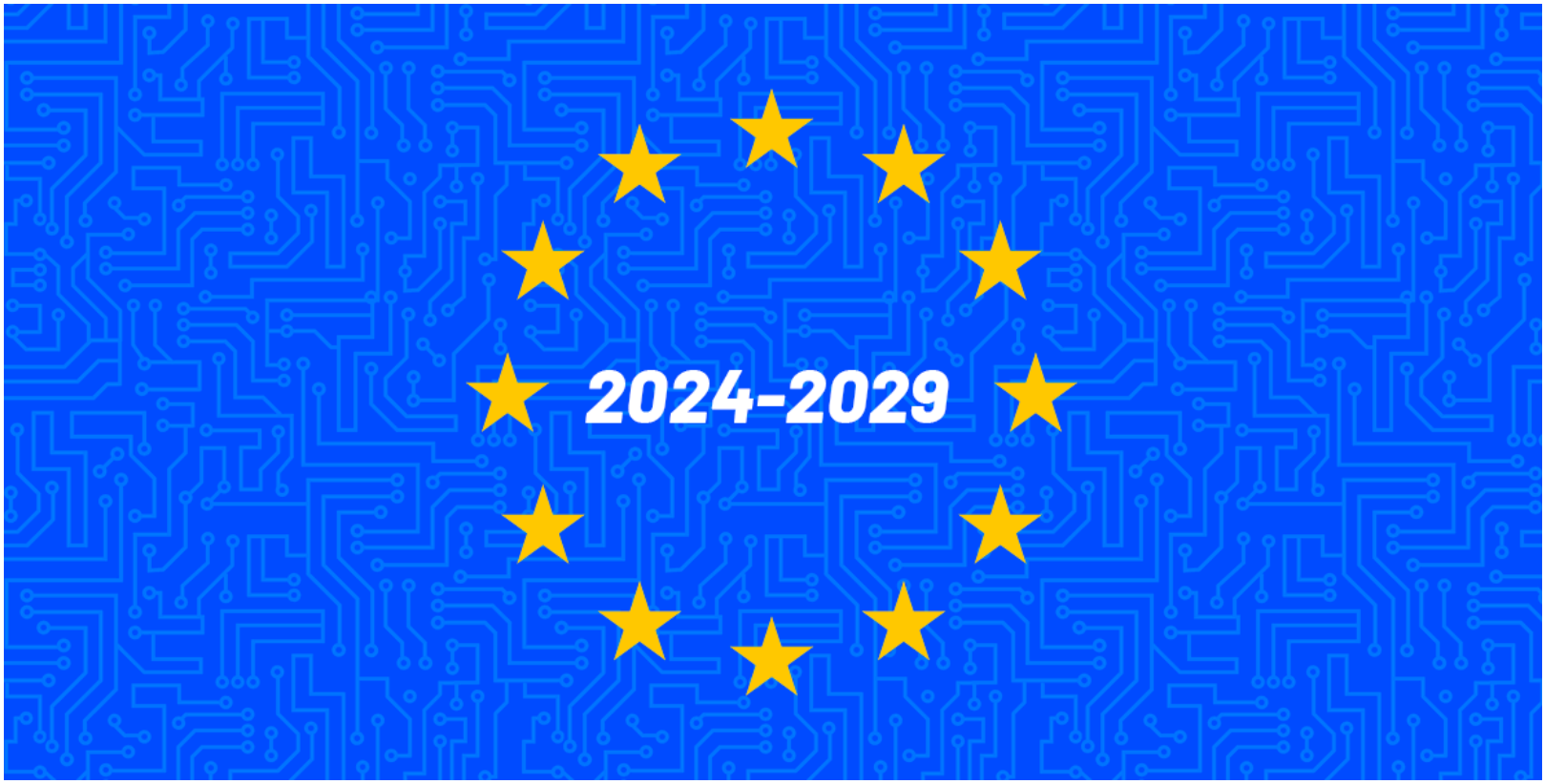

A Fundamental-Rights Centered EU Digital Policy

EFF's Recommendations 2024-2029

ELECTRONIC FRONTIER FOUNDATION

Published 2024
A publication of the Electronic Frontier Foundation, 2024. "A Fundamental-Rights Centered Digital Policy EFF's Recommendations for the EU 2024-2029" is released under a Creative Commons Attribution 4.0 International License (CC BY 4.0).

Contact
Christoph Schmon, International Policy Director: christoph@eff.org
Svea Windwehr, Assistant Director of EU Policy: svea@eff.org
Media inquiries: press@eff.org

EU Transparency Register
805637038375-01

Contents

I. A Fundamental Rights Centered EU Digital Policy.....4

II. Ensure enforcement of platform regulations is fundamental rights- and user-centered.....6

III. Create the conditions for fair digital markets that foster choice, innovation, and fundamental rights..... 7

IV. Adopt a privacy-first approach to fighting online harms..... 8

V. Protect users' right to secure and private communication, and protect against surveillance everywhere.....9

I. A Fundamental Rights Centered EU Digital Policy

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. EFF's mission is to ensure that technology supports freedom, justice, and innovation for all people of the world.

EFF's technologists, activists, and attorneys have unique and extensive experience defending free speech online, fighting illegal surveillance, advocating for users and innovators, and supporting freedom-enhancing technologies. EFF advises policymakers and educates the press and the public through comprehensive analysis posts and reports, educational guides, activist workshops, press briefings, and more. Civil society plays a crucial role in informing policymaking processes, keeping watch over government and corporate entities, and sharing stories about how users are affected by regulation with those responsible for legislating. Our work is strengthened by a vast network of concerned members and partner organizations spanning the globe. In the European Union (EU), we are proud to collaborate with many different civil society organizations with diverse areas of expertise and are an active member of European Digital Rights (EDRi).

Looking Back

Over the past decade, the EU has established itself as a frontrunner in the regulation of online services and new technologies. Regulatory initiatives of the past two mandates have covered a broad range of issues, including platform governance, media freedom, contestable digital markets, cybersecurity, artificial intelligence, and child safety.

In our EU policy work, EFF has advocated for fundamental principles like transparency, openness, and information self-determination. We emphasized that legislative acts should never come at the expense of protections that have served the internet well: Preserve what works. Fix what is broken.

Recognizing the internet's global reach, we have also stressed that lawmakers must consider the global impact of regulation and enforcement, particularly effects on vulnerable groups and underserved communities.

We are also serious about tackling the dominance of Big Tech and have therefore supported new tools and smart legislation that help to enhance competition, challenge the power of very large online platforms, and give users more control and choice. These efforts address the walled gardens into which users of a few powerful companies find themselves locked, and the ways users are tracked across the web without their consent.

We are equally serious in opposing proposals, in the EU and around the world, that jeopardize fundamental online security for users, particularly efforts to weaken encryption. Together with our allies in the EU, we have proposed solutions to ensure that users benefit from improved security and that their right to private communication is respected, not eroded by surveillance. We believe the EU is uniquely positioned to foster an environment where freedom of expression and privacy thrive, through balanced policies that resist censorship and uphold human rights. Legal mandates that restrict access to lawful speech, hinder private and free communication, or lead to government intrusion in users' private lives, especially endangering vulnerable communities, are not compatible with these values.

Looking Ahead

The next five years will be a pivotal time for EU digital policy making. European regulation continues to have huge ramifications around the world. Following the adoption of extensive new EU tech legislation, we are now entering a new era focused on the enforcement of these initiatives. Given the important role of standardization and the growing relevance of global policy fora, achieving the goals of EU regulatory instruments will increasingly require cooperation at the international level.

The EU and its Member States must adopt a rights-respecting approach to the enforcement of key laws such as the Digital Services Act (DSA), the Digital Markets Act (DMA), the General Data Protection Regulation (GDPR), and the AI Act (AIA). The European Commission's enforcement agenda in particular must center on user rights and fair competition and follow the principles of proportionality and political independence. When enforcing existing regulations and exploring new initiatives, the EU must adopt an inclusive approach, recognizing that European regulatory regimes affect users globally.

The internet, and the legislation that governs it, are ours to shape. Any reform or legislative action should be guided by a commitment to proportionate and human rights centered regulation that upholds freedom of expression, fosters innovation, and safeguards privacy—essential elements for building a just and equitable society.

Accordingly, we are concerned by recent shifts in EU policymaking that could undermine these objectives. Recent developments signal a dangerous move towards expanding surveillance powers, justified by narratives framing complex digital policy issues as primarily security concerns. These approaches invite tradeoffs that risk undermining the privacy and free expression of users in the EU and beyond.

As the EU's 2024–2029 mandate commences, we present policy recommendations to help ensure that the EU digital policies and their enforcement protect free expression, innovation, and privacy online.

II. Ensure enforcement of platform regulations is fundamental rights- and user-centered

2022 marked an important year for digital rights across the EU, as the DSA came into force seeking to foster a safer and fairer digital space. EFF supports many aspects of this landmark bill, including the preservation of important principles that helped to support online expression, new standards for platforms' processes, and better procedural rights for users.

However, as is the case for other recent EU laws relevant to digitalization and new technologies, the success of the DSA will depend on how social media platforms comply with their new obligations, how European authorities enforce the new rules, and whether civil society organizations will have a say in that enforcement. The latter is particularly true for those rules that are ambiguous or offer opportunities for abuse.

- Prioritize rights-respecting enforcement: Stakeholders should take a rights-respecting approach to the enforcement of the DSA, especially with regards to potential negative effects of cross-border content removal requests by law enforcement authorities, the appointment of trusted flaggers, and the handling of harmful but lawful content. We are concerned about the DSA's requirement that service providers proactively share user data with law enforcement authorities and the powers it gives government agencies to request such data. We caution against the misuse of the DSA's emergency mechanism and the expansion of the DSA's systemic risks governance approach as a catch-all tool to crack down on undesired but lawful speech. The co-regulatory model of the DSA should be considered an opportunity to include European and non-European civil society voices and rights defenders and adopt a human rights-centered enforcement model.

- Champion media freedom and information plurality: The EU should strengthen the rights of journalists and media freedom through balanced enforcement of the European Media Freedom Act (EMFA). The Commission must make sure that the EMFA does not give powerful media outlets and platforms unfettered ability to negotiate the visibility of lawful content or subject platforms to undue government pressure under the guise of fighting disinformation. European policymakers must foster an enforcement reality that inspires trust in the media and limits the use of spyware against journalists.

- Consider the Brussels effect: EU lawmakers should integrate global perspectives when assessing the impact of legislative proposals and enforcing existing laws. Laws such as the DSA have extraterritorial effects that should be considered for a truly user rights-focused enforcement agenda. The DSA relies on robust checks and balances to guarantee effective oversight, the rule of law, and the protection of fundamental rights—principles that should guide its application and advocacy in

international contexts. Likewise, the EU's global regulatory influence affects users beyond the EU. Their voices must be heard and their needs considered through active dialogue to mitigate unintended consequences.

- Empower civil society: It is crucial to recognize the vital role of civil society organizations in supporting regulatory oversight and holding oversight bodies accountable. Actively include civil society organizations and human rights defenders in stakeholder dialogues, EU expert groups, and the board of Digital Services Coordinators to strengthen and inform policymaking.

III. Create the conditions for fair digital markets that foster choice, innovation, and fundamental rights

Prompted by economic uncertainties across the EU and fears of increased interdependence, "competitiveness" and "sovereignty" have emerged as some of the major themes of the new EU mandate. These concepts are important but must be updated to include a public interest approach to shaping digital markets. Rather than reverting to protectionist stances on industrial and competition policy, the EU should aim to create the conditions for real competition and digital markets that would benefit users, business, and society more broadly.

- Focus DMA enforcement on provisions that prioritize user rights and choice: Some DMA provisions show great potential to help rein in the power of gatekeepers, give users more choices, and make digital markets more competitive. But the DMA is only as good as its enforcement. The EU's robust enforcement agenda should focus on what benefits users most: App store freedom, user choice, and interoperability. Only a competition policy that keeps users' needs front and center will help align market forces and innovation to better serve users' security and privacy.

- Foster interoperability: Interoperability is an important tool to promote competition and prevent monopolists from shutting down user-empowering innovation. The DMA takes an important first step by requiring gatekeeper platforms to support interoperability, including for app stores and messaging services, though technical and policy challenges remain. In its review of the DMA, the European Commission should explore fostering interoperability between social networking services to enable more user choice, consulting technical experts and civil society in the process. Regulating gatekeepers is only one instrument to make digital markets more competitive and foster innovation. The EU should consider adopting policies to champion alternatives and strengthen the public interest internet and open-source projects, with a focus on fostering an open internet. It should avoid undue interference in the interconnection market, such as mandatory network fees and

similar measures, which could undermine the principles of neutrality and lead to a fragmented internet.

- Counter the emerging generative AI oligopoly: The generative AI stack is characterized by power concentrated in the hands of a few companies supplying the hardware, compute power, and models underlying most AI applications. EU industrial policy and the enforcement thereof must challenge these emerging monopolies.

IV. Adopt a privacy-first approach to fighting online harms

Regulators are increasingly focused on a range of risks associated with the design and use of online platforms, such as addictive design, the effects of social media consumption on children's and teenagers' mental health, and dark patterns limiting consumer choices. These concerns are important: No one wants to live in a world where children are exploited and consumers misled. However, proposed solutions like mandatory age verification have unintended consequences that will undermine the privacy and fundamental rights of all users. We believe that many of these concerns share a common root: The excessive collection and processing of users' data. The EU should seize the opportunity to build upon landmark regulations like the GDPR and the DSA to address online harms and promote digital fairness through a privacy-first approach.

- Ban targeted ads: Companies must be prohibited from targeting ads to a person based on their online behavior. These ads are especially dangerous because they incentivize all businesses to harvest as much consumer data as possible, either to use it for targeting ads or to sell it to someone who will. Contextual ads will benefit publishers, users, and competition in digital markets.

- No deceptive design: Companies must be prohibited from presenting people with user interfaces (sometimes called "dark patterns") that have the intent or substantial effect of impairing autonomy and choice. This protection is also necessary to ensure that consent is genuine and that online environments are fair.

- No pay-for-privacy schemes: Just as you shouldn't have to trade your privacy for the ability to use a service, you shouldn't have to pay extra for the ability to use it without being surveilled. Privacy must not be a commodity that only the wealthy can afford. This safeguard is necessary to ensure that "consent" is truly voluntary.

- No age verification: Children's safety is important. At the same time, there is little evidence that online age verification tools can help achieve this goal. Instead, age verification tools undermine the fundamental rights of all users, exacerbate structural discrimination, and create a false sense of security. The implementation of the eIDAS Regulation must protect fundamental rights, including privacy, free

expression, and participation, and must pursue the highest levels of data protection and security, particularly in the context of age verification.

- Address privacy-invasive personalization: The EU should tackle abusive data collection practices that undermine explicit consent and user autonomy in platforms' personalization features and algorithmic recommender systems. Strengthen user control by ensuring clear choices over personalization and data sharing.

V. Protect users' right to secure and private communication, and protect against surveillance everywhere

For years, we have observed a worrying tendency of technologies designed to protect people's privacy and data being re-framed as security concerns. Even though their access to data has never been broader, law enforcement authorities continue to peddle the tale of the world "going dark." This is exacerbated by global trends of state-sponsored deployment of spyware, proliferation of surveillance, and criminalization of ethical hacking and security research. The EU must reverse the trend and set global standards by adopting progressive security and digital policy anchored in fundamental rights.

- Protect encryption: The EU must protect encrypted communication and resist any attempts to circumvent end-to-end encryption through backdoors or client-side scanning.

- Prioritize the rights-respecting enforcement of the AI Act: The goals of the EU's AIA are to ensure that "AI systems respect fundamental rights, safety, and ethical principles." However, the new provisions on biometric surveillance leave many questions open: Law enforcement exceptions risk undermining key safeguards, such as limitations on face recognition and predictive policing. The EU should therefore prioritize robust, rights-based enforcement of the AIA that protects against discrimination and surveillance through AI systems. In particular, any rights-affecting algorithmic decisions about a person must be subject to adequate safeguards to ensure transparency, explainability, and fairness. Machine learning technology is generally not fit for such decisions.

- Tackle the harms caused by biometric surveillance: Member States must make use of their prerogatives to ban biometric surveillance under national law. EU agencies must refrain from employing biometric surveillance, especially in particularly sensitive contexts such as Europe's borders.

- Don't reintroduce data retention: Requiring telecom and internet service providers to retain user data is incompatible with fundamental rights. Data retention regimes expand the ability of governments to surveil their citizens, ultimately damaging individuals' privacy, anonymity, and free expression. The EU must adhere to its own values and refuse to reintroduce data retention rules.

- Uphold fundamental rights in global fora: The EU has a mandate to prevent cybercrime and enhance international cooperation to tackle serious offenses. We urge the EU Commission to only support binding rules that are compatible with international human rights and grounded in the principles of legality, necessity and proportionality, due process, and the rule of law. EU legislation and international treaties should contain concrete human rights safeguards, robust data privacy standards, and sharp limits on intrusive surveillance powers, including in the context of global cooperation.