THE EUROPEAN HUMAN RIGHTS AGENDA IN THE DIGITAL AGE

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

Access Now Europe is a leading civil society voice in Europe that advocates for policies which defend and extend the digital rights of users. Based in Brussels since 2010, the team focuses on a broad range of issues at the EUlevel, including **privacy and data protection, freedom of expression, artificial intelligence, surveillance and national security, Net Neutrality**, and more.

The protection of digital rights is an important issue worldwide, and it is vital in Europe. Because the EU can set positive global standards, furthering these rights in Europe is critical for people all around the world. As one of the few NGOs working fulltime on digital rights policy in Brussels, Access Now Europe provides a crucial counter-voice to the growing clamour of corporate lobbyists.

Our work in the EU is reinforced by cooperating with national and international digital rights groups from across Europe. We are a proud member of **European Digital Rights (EDRi)**, working now for many years in collaboration with established and emerging organisations and individuals. Our work with European groups takes place both within the EDRi network, relying on the expertise and experience of more than 30 civil rights organisations, and through numerous partnerships with NGOs for targeted actions and campaigns.

The Europe policy team

In our locally registered office in Brussels, our policy team consists of:

Fanny Hidvégi	Estelle Massé	Eliška Pírková	Daniel Leufer
Europe Policy Manager and Legal Counsel	Europe Senior Policy Analyst and Global Data Protection Lead	Europe Policy Analyst	Mozilla Fellow on Artificial Intelligence

Nine years of digital rights advocacy in Europe

Over the past several years, the Brussels team has become a trusted source of analysis and information for both citizens and policy makers, and we have seen progress on multiple fronts. From the fight against the Anti Counterfeiting Trade Agreement, to the improvement of Net Neutrality rules in the Telecoms Single Market and the advancement of privacy protections in the Data Protection Reform Package, the work of Access Now Europe, combined with that of our allies and partners, has been crucial to secure the fundamental rights of users in the European Union over the past year.

This work, coupled with the reliable and timely policy analysis provided by the Brussels team, has led Access Now to deliver evidence to the European Parliament, the Body of European Regulators of Electronic Communications (BEREC), the European Data Protection Supervisor (EDPS), the Article 29 Working Party, and the European Data Protection Board. The Brussels team liaises on a regular basis with members of the European Parliament from all political families, European Commission officials, including high-ranking directors and commissioners, and representatives from member states to the Council of the EU.

Our team members serve on important advisory expert groups such as the European Commission's Multistakeholder Working Group on the Implementation of the General Data Protection Regulation, the High Level Expert Group on Artificial Intelligence, and the Berlin Working Group on data protection, and our European policy staff frequently provides expert opinions for European Parliament committees.

The next five year of digital rights in Europe

To ensure the full enjoyment of fundamental rights online and offline, the European Union and its member states must provide effective protections for democracy, the rule of law, and fundamental rights. To achieve effective, meaningful, and rights-respecting digital policies, it is necessary that EU member states observe their negative and positive obligations to protect the human rights of all individuals within their jurisdiction, whether online or off. The enforcement of fundamental rights

must be strengthened through measures such as collective redress mechanisms, capacity building for regulators and courts, and the promotion and enabling of a healthy and sustainable civil society.

Building on our experience - whether challenges or successes - we will continue our work on human rights in the digital age in Europe and beyond. Access Now has put forward concrete policy recommendations in the areas of (1) data exploitation by private entities, (2) content governance, (3) artificial intelligence, (4) surveillance powers, and (5) connectivity.

1. The EU must protect people against the exploitation of data by private entities

Privacy and data protection are the cornerstones of human rights in the digital age. As public and private entities increasingly collect, retain, analyse, and track people's data, the EU has a duty to rein in the unlawful data and privacy-invasive practices that have multiplied online.

Recommendations:

- ➔ **Address and remedy the negative impacts** resulting from **data-driven and privacy-invasive business models and the concentration of power** in a handful of private companies in the online economy.
- ➔ **Regulate the online advertising economy** to limit the pervasive overbroad collection of data that leads to profiling and targeting of people.
- ➔ **Address disinformation and misuse of personal data** in the context of elections and political debate through a systemic approach that includes the **strengthening of online privacy protections**.
- ➔ **Develop a comprehensive and ambitious reform** to ensure the **confidentiality of electronic communications** and strengthen **safeguards against tracking**.
- ➔ **Avoid the promotion or creation of self-regulatory models** including **public-private partnerships for data collection and sharing** which limit users' avenues for remedy and are often inadequate to protect human rights.
- ➔ **Ensure a robust and harmonised enforcement of the GDPR** across the EU, including by making sure supervisory authorities are adequately resourced and reviewing all existing adequacy decisions for transfer of data to third countries.

2. The EU must strengthen the protection of freedom of expression and opinion on the internet

The internet remains a valuable tool for global access to information and an unparalleled public space for individuals, communities, and organisations to express themselves. In recent years, the amount of illegal online content has triggered numerous regulatory responses across the EU. While concerns about such content are legitimate, addressing societal phenomena such as online hate speech or terrorist content is not a simple matter of deletion or blocking. Without effective protection of the right to freedom of expression, oppressive behaviours and censorship will diminish its democratising force.

Recommendations:

- ➔ **Adopt a harmonised and human-rights-centered legal framework** to regulate **intermediary liability for illegal online content.**
- ➔ **Avoid incentives that lead to censorship** and **refrain from illegitimate restriction of freedom of expression online**.
- ➔ **Develop tailored policies**, legislative or otherwise, that are **legitimate, proportionate,** and fit for the sector and problem at hand. **Avoid one-size-fits-all policy solutions**.
- ➔ **Avoid overbroad definitions** and categorisations of illegal online content.
- ➔ **Do not promote the use of automated proactive measures for content monitoring** and recognition without addressing **the limitations of the technology.**
- ➔ **Improve and enforce meaningful transparency of content governance practices** exercised by both online platforms and state actors **through clear reporting obligations.**
- ➔ **Enable access to an effective remedy** for all online users, including access to judicial redress.
- ➔ **Encourage and support online platforms** in **developing human-rights-based content moderation and curation policies** for user-generated content.

3. The design, development, and deployment of AI systems in the EU must respect human rights

With the increasing investment in and proliferation of automation-based technologies, the EU must enforce and develop the highest human rights compliance standards for emerging technologies and AI systems that are designed, developed, or deployed in the European Union.

Recommendations:

- ➔ **Develop** a set of **binding, horizontal criteria** for determining whether the use of an automated decision-making or AI system should be permitted and **create a framework for sector- and domain-specific application** of those criteria, including the further development of **mandatory human rights impact assessments** and due diligence processes.
- ➔ **Ban mass-scale citizen scoring** and develop stronger **limitations on the use of biometrics for facial recognition, movement detection,** and similar technologies. **Introduce a moratorium on the use of facial recognition technology that enables mass surveillance**.
- ➔ **Provide clarity on safeguards**, **red lines**, and **enforcement mechanisms**.
- ➔ **Do not apply the objective of "boosting AI uptake" indiscriminately to all areas of society.** Pursue this objective only **where there is clear evidence of benefit balanced against an assessment of potential harms.**
- ➔ **Require that all AI projects and initiatives** that are funded by the European Union or by public investment **conform to the standards of "Trustworthy AI", and are assessed** to ensure that they meet the criteria on legal compliance, ethics, and socio-technical robustness**.**
- ➔ **Clarify the legal component of "Trustworthy AI"** through a comprehensive mapping of existing legislation that applies to AI development and deployment, and the identification of legal uncertainties and gaps.
- ➔ Following the mapping, **update existing legislation or adoption of complementary framework, where needed,** particularly in the fields of safety, liability, and consumer and data protection law.
- ➔ **Evaluate and update current enforcement mechanisms** with regard to human rights compliance in both public and private deployment of AI.

- ➔ **Build fundamental rights** considerations, alternative and parallel modelling, and testing **into** all phases of **public procurement** processes ("Preparation and Planning, Publication, Selection Evaluation and Award, Contract Implementation") and into technical specifications.

- ➔ **Create independent centres of expertise on AI** on a national level to monitor, assess, conduct research, report on, and provide advice to government and industry in coordination with regulators, civil society, and academia about the human rights and societal implications of the use of algorithms, automated decision-making systems, or AI.

4. The EU must reform government surveillance to respect human rights

The EU and its member states are increasingly seeking to solidify and exercise control over internet infrastructure and services. Although this is undertaken in pursuit of legitimate aims, a large number of security measures are reshaping the internet into a fragmented, militarised space and putting freedoms at risk. With populism on the rise and at a time where authoritarian regimes double down on repressive policies and practices online, it is essential for the EU to uphold its democratic values and move away from simplistic approaches that undermine human rights and civil liberties under the pretext of preventing terrorism and protecting national security.

Recommendations:

- ➔ **Oppose border surveillance measures** that seek to **indiscriminately track** and **initiate the reform of all Passenger Name Records frameworks** to bring them in line with the EU Charter and EU jurisprudence.

- ➔ The Commission must **resist attempts to re-introduce disproportionate data retention regimes** in accordance with the jurisprudence of the Court of Justice of the EU on that matter.

- ➔ Foster police and judicial cooperation within the EU by improving existing frameworks and EU institutions and **prioritise the reform of Mutual Legal Agreement Treaties** in cross-border law enforcement cooperation instead of creating frameworks that lower and circumvent democratic safeguards and due process.

- ➔ **Conclude the reform of the EU export control regime** and **impose a moratorium on the sale, transfer, and use of surveillance technology** until human rights-compliant regulatory frameworks are in place in the EU. These should include robust reporting and transparency obligations, protections for security research, and the removal of export controls on encryption.

- ➔ **Continue to strongly protect the use of encryption** as a crucial tool to protect the right to privacy, confidentiality of communications, and freedom of expression of all users, including that of protected groups, journalists, and lawyers.

5. The EU should foster connectivity and protect the openness of the internet

By adopting the Net Neutrality law in 2015, the EU has become a global leader in the protection of a free and open internet for everyone. Access to the unfettered internet is the precondition to the exercise of human rights online. Guaranteeing the openness of the internet will only become more vital as the internet is further integrated into every aspect of our lives.

Recommendations:

- ➔ **Member states should provide adequate resources** and powers to regulatory authorities for the **harmonised enforcement of the Net Neutrality law.**
- ➔ **BEREC should further clarify its guidelines to ensure the ban of zero rating practices** in the EU.
- ➔ In the development of **5G strategies and measures, Net Neutrality rules must be respected**.
- ➔ **Actively condemn internet shutdowns and network discrimination**, both inside the EU and around the world, in particular through Electoral Observation Missions.
- ➔ **Propose legislation on Corporate Social Responsibility** going beyond the Directive on non-financial reporting

For more information, please contact:

Fanny Hidvégi
Europe Policy Manager | fanny@accessnow.org
Estelle Massé
Senior Policy Analyst and Global Data Protection Lead | estelle@accessnow.org
Eliška Pírková
Europe Policy Analyst | eliska@accessnow.org

November 2019