



accessnow



**United Nations Independent Expert on Protection against Violence and
Discrimination based on Sexual Orientation and Gender Identity
Written Submission: Anti-LGBTQ+ Repression**

31 January 2024

Introduction

Access Now¹ and the Electronic Frontier Foundation (EFF)² welcome this opportunity to provide information to the United Nations (U.N.) Independent Expert on protection against violence and discrimination based on sexual orientation and gender identity (IE SOGI) to inform the Independent Expert's thematic report to be presented to the U.N. Human Rights Council at its fifty-sixth session.³ Access Now, as an ECOSOC accredited organization, routinely engages with U.N. Special Procedures in support of our mission to extend and defend digital rights of users at risk around the world. The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development.

This submission addresses the trends, challenges, and problems that people and civil society organizations face based on their real and perceived sexual orientation, gender identity, and gender expression. Article 17 (privacy), Article 19 (free expression), and Article 26 (equality before the law) of the International Covenant on Civil and Political Rights (ICCPR)⁴ and General Comment No. 34⁵ require immediate efforts to address and mitigate the effects of discriminatory laws that impede freedom of expression and privacy. Our examples underscore the extensive impact of such legislation on the LGBTQ+ community, and the urgent need for legislative reform at the domestic level.

1. Laws and draft legislation restricting freedom of expression

Uganda

1. In May 2023, Ugandan President Museveni signed the Anti-Homosexuality Act (AHA) into law.⁶ It introduced new restrictions that put LGBTQ+ peoples' fundamental freedoms at risk, and

¹ Access Now, About Us, available at <https://www.accessnow.org/about-us/>.

² Electronic Frontier Foundation, About EFF, <https://www.eff.org/about>.

³ United Nations Independent Expert on Protection against Violence and Discrimination based on Sexual Orientation and Gender Identity, Call for Input: Protection against violence and discrimination based on sexual orientation and gender identity, in relation to the human rights to freedom of expression, association and assembly, available at <https://www.ohchr.org/en/calls-for-input/2024/call-input-protection-against-violence-and-discrimination-based-sexual>, 2024.

⁴ United Nations Human Rights, Office of the High Commissioner on Human Rights, International Covenant on Civil and Political Rights, available at <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.

⁵ United Nations Human Rights Committee, General comment no. 34, available at <https://digitalibrary.un.org/record/715606>, 12 September 2011.

⁶ CNN, Ugandan president signs one of the world's harshest anti-LGBTQ bills into law, available at <https://edition.cnn.com/2023/05/29/africa/museveni-assents-homosexuality-bill-intl/index.html>, 29 May 2023.

was labeled by the U.N. as one of the harshest anti-LGBTQ+ laws in the world.⁷ Section 11 (1) of the AHA restricts individuals, organizations, and media outlets from expressing support for LGBTQ+ rights or discussing LGBTQ+ issues. Broadcasting companies like MultiChoice have already announced that they will stop airing LGBTQ+ content in Uganda in compliance with the law.⁸ This imposes undue restrictions on the right to free expression, which contravenes Article 19 of the ICCPR as it interferes with the ability to impart information and ideas on the basis of content—specifically targeting expressions related to LGBTQ+ identities.

2. Further, Section 14 requires all people to report prohibited acts to the police. This has exacerbated surveillance and censorship of pro-LGBTQ+ speech, and forced people in Uganda to censor themselves to avoid being targeted or arrested.⁹ Since the law passed, the Human Rights Awareness and Promotion Forum (HRAPF-Uganda) has documented over 200 instances where people have been targeted due to their real or perceived sexual orientation or gender identity.¹⁰ Interactions and content on social media like text messages, as well as intimate videos and pictures, are being used as digital evidence to arrest and charge people under the AHA. In July 2023, for example, one person’s messages on social media were used as evidence to charge them with the “offense of homosexuality” under Section 2 (1) of the AHA.¹¹

Russia

3. In June 2013, Russian President Putin approved amendments to the Federal Law No. 135-FZ, ‘On the Protection of Children From Information Liable to be Injurious to their Health and Development,’ also known as the ‘anti-gay propaganda law.’ In the *Case of Bayev and Others v. Russia*, the European Court of Human Rights noted that Russia’s adoption of laws that seek to “protect the morals, health and the rights of others, specifically minors” encouraged homophobia, and held that these laws are “incompatible with the notions of equality, pluralism and tolerance in a democratic society.”¹²
4. The amendment introduced Article 6.21 on the ‘Promotion of Non-Traditional Sexual Relations to Minors’ into the Russian Code of Administrative Offences, which prohibits the use of mass media and the internet to spread information about “non-traditional sexual relations” to

⁷ United Nations Human Rights, Office of the High Commissioner on Human Rights, Uganda: UN experts condemn egregious anti-LGBT legislation, available at <https://www.ohchr.org/en/press-releases/2023/03/uganda-un-experts-condemn-egregious-anti-lgbt-legislation>, 29 May 2023.

⁸ The Washington Blade, Companies pull out of Uganda, NGOs suspend services after Anti-Homosexuality Act signed, available at <https://www.washingtonblade.com/2023/06/13/companies-pull-out-of-uganda-ngos-suspend-services-after-anti-homosexuality-act-signed/>, 13 June 2023.

⁹ openDemocracy, Queer Ugandans reveal devastating impact of anti-gay law, available at <https://www.opendemocracy.net/en/5050/uganda-anti-homosexuality-act-gay-law-impact-month/>, 4 July 2023.

¹⁰ HRAPF-Uganda, Violation Reports, available at <https://hrapf.org/violation-reports/>.

¹¹ HRAPF-Uganda, HRAPF’s Report on enforcement of the AHA for July 2023, available at <https://hrapf.org/mdocs-posts/hrapfs-report-on-enforcement-of-the-aha-for-july-2023/>, 9 August 2023.

¹² European Court of Human Rights, Case of Bayev and Others v. Russia, available at <https://globalfreedomofexpression.columbia.edu/cases/case-bayev-others-v-russia/>, 20 June 2017.

minors.¹³ In July 2017, Evdokia Romanova, a member of the Youth Coalition for Sexual and Reproductive Rights (YCSRR), was arrested and charged under Article 6.21 for sharing links on her personal Facebook and VKontakte accounts that referred to topics like the same-sex referendum in Ireland, and thus allegedly created an appealing image of non-traditional sexual orientation.¹⁴ In 2022, the Russian Parliament passed an updated anti-gay propaganda law to include LGBTQ+-related information that is targeted at all people, not just minors.¹⁵ Authorities in the country have since used the law to crack down on LGBTQ+ people online. For example, in April 2023 a vlogger was arrested and charged for posting videos that depicted “non-traditional sexual relations.”¹⁶

5. These threats to freedom of expression are also linked to breaches of privacy. In 2019, amendments made to Russia’s Federal Laws on Communications and Information Technologies and Information Protection, also known as the ‘Sovereign Internet Law,’ came into force and expanded the state’s control over the internet.¹⁷ For example, Article 46 requires all internet service providers to install “technical equipment for counteracting threats to stability, security, and the functional integrity of the internet” on their networks.¹⁸ This kind of technology, such as Deep Packet Inspections (DPI),¹⁹ allows the government to filter and analyze internet traffic in real-time, including decrypting or analyzing content like instant messages, web browsing history, file transfers, and other data. In enabling authorities to monitor and intercept the content of digital communications without adequate legal safeguards or oversight, this law denies individuals in Russia fundamental rights recognized in Article 17 of the ICCPR.

Iraq

1. In 2023, the Ministry of Interior in Iraq launched a committee to clamp down on “indecent content” online, and established a platform that enables people in Iraq to report or denounce content that allegedly “violates public morals, contains negative and indecent messages and undermines social stability.”²⁰ Between 10 January and 13 February 2023, the judge at the

¹³ Human Dignity Trust, Briefing on Russia’s Federal ‘Anti-Propaganda’ Law 2014, available at <https://www.humandignitytrust.org/resources/briefing-on-russias-federal-anti-propaganda-law-2014/>, 24 April 2014.

¹⁴ Amnesty International, Russian Federation: LGBT activist charged with homosexual propaganda: Evdokia Romanova, available at <https://www.amnesty.org/en/documents/eur49/7085/2017/en/>, 12 September 2017.

¹⁵ openDemocracy, Explainer: What does new ‘gay propaganda’ law mean for LGBTIQ+ Russians?, available at <https://www.opendemocracy.net/en/5050/russia-gay-propaganda-law-amendments-explainer/>, 24 November 2022.

¹⁶ CNN, Russia arrests Chinese LGBTQ blogger for violating so-called same-sex ‘propaganda’ law, available at <https://edition.cnn.com/2023/04/07/europe/russia-chinese-lgbtq-blogger-arrested-intl/index.html>, 7 April 2023.

¹⁷ Official Internet Portal for Legal Information, Federal Law No. 90-FZ of May 1, 2019 “On Amendments to the Federal Law ‘On Communications’ and the Federal Law ‘On Information, Information Technologies, and Information Protection’”, available at <http://publication.pravo.gov.ru/Document/View/0001201905010025?index=2>, 1 May 2019.

¹⁸ DGAP, Deciphering Russia’s “Sovereign Internet Law”: Tightening Control and Accelerating the Splinternet, available at <https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law>, 16 January 2020; CEPA, The New Iron Curtain Part 4: Russia’s Sovereign Internet Takes Root, available at <https://cepa.org/article/the-new-iron-curtain-part-4-russias-sovereign-internet-takes-root/>, 5 April 2022.

¹⁹ Access Now, Taxonomy of a shutdown: 8 ways governments restrict access to the internet, and how to #KeepItOn, available at <https://www.accessnow.org/publication/internet-shutdown-types/>, 2 June 2022.

²⁰ The New York Times, As Iraq Tries to Chill Critics, Its Newest Target Is Social Media, available at <https://www.nytimes.com/2023/07/16/world/middleeast/iraq-dissent-free-speech-social-media.html>, 16 July 2023.

Third Investigative Court in Al-Karkh charged 14 individuals with offenses for publishing “indecent” or “immoral” content on social media under Article 403 of the Iraqi Penal Code, which criminalizes published material that “violates public integrity or decency.”²¹ Under international human rights law, including Article 19 of the ICCPR which Iraq has ratified, the right to freedom of expression is recognized as a fundamental human right, even for “expression that may be regarded as deeply offensive.”²²

2. In March 2023, Access Now and EFF, alongside a coalition of regional and international organizations, raised concerns with authorities in Iraq that the Ministry of Interior committee and platform may be used to crack down on legitimate and protected peaceful speech due to the wide and overly broad scope of their work, and that individuals in Iraq may start to self-censor for fear of prosecution.²³ Another letter from Access Now and other civil society groups to the Iraqi Communications and Media Commission urged authorities to drop the draft Regulation No. 1 of 2023 for Digital Content in Iraq as it did not meet standards required by Article 19 of the ICCPR.²⁴ The draft proposal comes at a time when the LGBTQ+ community in Iraq is facing amplified risks in an environment of impunity.²⁵ For example, popular Iraqi TikTok personality Noor BM faced repeated online abuse and was ultimately shot and killed in Baghdad.²⁶

2. Laws, policies, and practices regulating internet use, access, and content

Cybercrime laws

3. In the digital age, expansive cybercrime and surveillance legislation threatens the rights of LGBTQ+ people and leads to systemic suppression of LGBTQ+ identities by compelling individuals to censor themselves for fear of severe reprisal. This looming threat is even more pronounced in countries like Iran, where same-sex conduct is punishable by death, and Egypt, where merely raising a rainbow flag can lead to arrest and torture.²⁷

²¹ Iraq, Penal Code of 1969, available at <https://www.refworld.org/docid/452524304.html>.

²² United Nations Human Rights Committee, General comment no. 34, available at <https://digitallibrary.un.org/record/715606>, 12 September 2011.

²³ Amnesty, Joint statement: Iraqi authorities must cease chilling crackdown on free speech, available at <https://www.amnesty.org/en/wp-content/uploads/2023/03/MDE1465112023ENGLISH.pdf>, 3 March 2023.

²⁴ Access Now, Stop the assault on free speech, drop the draft digital content regulation in Iraq, available at <https://www.accessnow.org/press-release/digital-content-regulation-iraq/>, 16 March 2023.

²⁵ Human Rights Watch, Iraq: Impunity for Violence Against LGBT People, available at <https://www.hrw.org/news/2022/03/23/iraq-impunity-violence-against-lgbt-people>, 23 March 2023.

²⁶ CNN, Prominent Iraqi TikToker fatally shot in Baghdad amid crackdown on LGBTQ community, available at <https://edition.cnn.com/2023/09/27/middleeast/iraq-lgbtq-shot-intl/index.html>, 28 September 2023.

²⁷ Electronic Frontier Foundation, The Growing Threat of Cybercrime Law Abuse: LGBTQ+ Rights in MENA and the UN Cybercrime Draft Convention, available at <https://www.eff.org/deeplinks/2023/09/growing-threat-cybercrime-law-abuse-lgbtq-rights-mena-and-un-cybercrime-draft>, 29 September 2023.

4. In August 2023, King Abdullah II of Jordan approved the Cybercrime Law of 2023, despite opposition from civil society organizations.²⁸ When the draft legislation was tabled in parliament in July 2023, civil society organizations including Access Now, EFF, and SMEX identified the draft law’s potential impact on freedom of expression, access to information, and its enabling of government overreach.²⁹
5. The law’s provisions are vague and overbroad, creating criminal penalties for “inciting immorality,” “contempt for religion,” and “exposing public morals.” International human rights law requires that legislation must be sufficiently precise to enable individuals to foresee whether a particular action is unlawful. Moreover, terms like “immorality” and “public morals” can serve as euphemisms for diverse sexual orientations and gender identities. That association is likely to lead to the systemic suppression of LGBTQ+ people, which will not only infringe on the right to free expression but also violate the principles of equality and non-discrimination.
6. Additionally, the Jordanian law criminalizes the use of VPNs to circumvent censorship, and requires social media companies with over 100,000 subscribers in Jordan to establish offices in the country.³⁰ As EFF has noted, such requirements create room for states to exert significant pressure on platforms to comply with the state's agenda.³¹ This can contribute to silencing of oppressed groups. These provisions can also deter individuals from accessing information and expressing themselves freely online, particularly LGBTQ+ individuals and human rights defenders who rely on anonymity and digital security tools to safeguard their online activities from government surveillance and social discrimination. As the Special Rapporteur on Freedom of Expression highlighted in 2015, anonymity and encryption are crucial to both free expression and privacy.³²

Child online protection laws

7. Section 3 of the draft Kids Online Safety Act (KOSA) in the U.S. requires social media platforms to “prevent and or mitigate” harm to children, including policing information about mental health disorders, use of illegal substances, and virtually any other content state officials consider “harmful.”³³ If the law passes, platforms are likely to over-censor and/or seek to limit

²⁸ Access Now, An Open Letter to the King of Jordan: Repeal the 2023 Cybercrime Law, available at <https://www.accessnow.org/press-release/open-letter-to-the-king-of-jordan-repeal-the-2023-cybercrime-law/>, 2 August 2023.

²⁹ Electronic Frontier Foundation, Jordan's King Should Reject the Country's Draft Cybercrime Law, available here <https://www.eff.org/deeplinks/2023/08/jordans-king-should-reject-countrys-draft-cybercrime-law>, 14 August 2023.

³⁰ Access Now, Jordan’s new proposed cybercrimes law will strongly undermine digital rights, available at <https://www.accessnow.org/press-release/jordans-cybercrimes-law/>, 24 July 2023.

³¹ Electronic Frontier Foundation, YouTube, Facebook and TikTok Put Human Rights In Jeopardy in Turkey, available at <https://www.eff.org/deeplinks/2021/01/youtube-and-tiktok-put-human-rights-jeopardy-turkey>, 9 January 2021.

³² United Nations Human Rights, Office of the High Commissioner, A/HRC/29/32: Report on encryption, anonymity, and the human rights framework, available at <https://www.ohchr.org/en/documents/thematic-reports/ahrc2932-report-encryption-anonymity-and-human-rights-framework>, 22 May 2015.

³³ Marsha Blackburn, Blackburn, Blumenthal Introduce Bipartisan Kids Online Safety Act, available at <https://www.blackburn.senate.gov/2023/5/blackburn-blumenthal-introduce-bipartisan-kids-online-safety-act>, 2 May 2023.

children’s access altogether. In particular, given that many U.S. communities are actively banning books with LGBTQ+ themes and accusing people providing healthcare to trans children of ‘grooming,’ access to social media can be a vital avenue to potentially life-saving information and communication channels for vulnerable youth.³⁴ As noted by Fight for the Future, “KOSA is basically a blank check for extreme right-wing attorneys general to bully platforms into suppressing content that they don't like.”³⁵

Trusted flagger relationships

8. Government authorities deploy a variety of tactics to surveil communities, quash dissent, and control the flow of information. In some instances, social media companies have established partnerships with law enforcements to facilitate content removal and/or access to account information. These “trusted flagger” relationships have enabled governments to censor marginalized communities, including LGBTQ+ people.³⁶ In Kenya, for example, media reports have revealed that TikTok made a closed-door agreement with the government to develop a framework to censor LGBTQ+ content.³⁷
9. In 2022, the European Union adopted the Digital Services Act (DSA). The DSA contains a number of progressive and novel measures on content governance and platform accountability. However, it also allows public authorities, including law enforcement agencies, to gain the status of trusted flaggers. In practice, this means that law enforcement agencies will have direct access to the platform and may demand swift content removals. Access Now, EFF, and other civil society groups raised concerns that such a measure may establish a dangerous precedent and disproportionate impact of content removals on historically oppressed and marginalized groups, including LGBTQ+.³⁸

Recommendations

States

- Urgently revisit, reform, and repeal any laws that criminalize LGBTQ+ identities or expressions. This includes the criminalization of consensual sexual relations between people of the same sex and any other disproportionate surveillance legislation that unjustly restricts the rights to

³⁴ Electronic Frontier Foundation, The Kids Online Safety Act is Still A Huge Danger to Our Rights Online, available at <https://www.eff.org/deeplinks/2023/05/kids-online-safety-act-still-huge-danger-our-rights-online>, 2 May 2023.

³⁵ Vice, Congress Is Pushing An Online Safety Bill Supported By Anti-LGBTQ Groups, <https://www.vice.com/en/article/qjv3qp/congress-is-pushing-an-online-safety-bill-supported-by-anti-lgbtq-groups>, 3 August 2023.

³⁶ Electronic Frontier Foundation, Online Platforms Should Stop Partnering with Government Agencies to Remove Content, available at <https://www.eff.org/deeplinks/2022/08/online-platforms-should-stop-partnering-government-agencies-remove-content>, 12 August 2022;

Electronic Frontier Foundation, How YouTube’s Partnership with London’s Police Force is Censoring UK Drill Music, available at <https://www.eff.org/deeplinks/2022/08/how-youtubes-partnership-londons-police-force-censoring-uks-drill-music>, 25 August 2022.

³⁷ Pink News, TikTok reportedly in talks with Kenyan government to remove LGBTQ+ content, available at <https://www.thepinknews.com/2023/09/28/tiktok-kenya-government-remove-lgbtq-content/>, 28 September 2023.

³⁸ Access Now, Joint statement: The EU DSA must follow a human rights-centred enforcement process, available at <https://www.accessnow.org/press-release/joint-statement-dsa-human-rights/>, 6 July 2023.

privacy and free expression. Such legal reforms are crucial to eliminating systemic barriers to equality, as well as safeguarding human rights and fundamental freedoms of LGBTQ+ people.

- Proactively scrutinize and oppose any bills that propose to criminalize or discriminate against LGBTQ+ identities or expressions. Before a bill is passed into law, legislators must ensure public consultation and assess potential impacts on human rights in light of the state's international obligations.
- Develop and implement concise training programs for law enforcement, judiciary, and government officials that are centered around upholding the principles of free expression, privacy, and due process in the context of sexual orientation and gender identity (SOGI). These programs should provide practical guidance on non-discriminatory treatment of LGBTQ+ persons, emphasizing the critical importance of protecting their rights to privacy and free expression. Equal focus should be given to due process standards in the handling and disclosing of personal data—ensuring any action is legally justified, legitimate, necessary, proportionate, and maintains the dignity of LGBTQ+ communities
- Ensure that regulations governing online platforms have a clearly defined scope, focus on transparent processes on platforms, and ensure that users benefit from effective legal protection against arbitrary government interference with their right to private life.
- States should avoid developing legislations that hold social media platforms liable for third party content, and should make sure that online intermediaries continue to benefit from comprehensive liability exemptions. Any additional obligations must be proportionate and must not curtail free expression and innovation.
- Strengthen or introduce data protection and privacy laws to classify SOGI-related data as sensitive, necessitating robust protections due to its profound risk of harm and discrimination arising from its misuse.
- Institute rigorous human rights standards as a prerequisite for law enforcement accessing or utilizing SOGI-related data or using their surveillance powers. Such access must be prescribed by law, necessary, have a legitimate aim, and be proportionate to the investigation of serious crimes, as long as such crimes align with human rights law and respect the principles of the UN Charter.³⁹ Prior judicial authorization, backed by clear evidence of the necessity and relevance to active criminal investigations, should be a non-negotiable requirement.
- Require law enforcement agencies to publish comprehensive transparency reports regarding SOGI-related data access requests. These reports should detail the nature of the data sought,

³⁹ Electronic Frontier Foundation, Necessary and Proportionate, available at <https://necessaryandproportionate.org>.

the legal basis for the requests, and their outcomes. The transparency reports should include referrals notifying platforms about potential violations of their terms and conditions. It should be disclosed whether such notices were acted on and the number of demands or requests that did not lead to action.

- Guarantee that individuals will be informed of law enforcement's access to their SOGI-related data, except in extraordinary situations where such disclosure could compromise a criminal investigation. Provide a straightforward, accessible, and effective remedy for individuals to contest or appeal unwarranted data access or use of surveillance powers.
- Establish ongoing audits and independent oversight mechanisms to monitor law enforcement's SOGI-related data access and surveillance practices. This oversight should assess adherence to human rights law and standards, implications for privacy and individual rights, and protections for the dignity of LGBTQ+ individuals.

Private sector

- As part of the human rights due diligence measures, companies should conduct and publish human rights impact assessments to identify existing and future systemic human rights risks stemming from content recommender systems and content moderation algorithms, with specific regard to LGBTQ+ people.
- Involve language experts, civil society groups, and local experts in the development of automated content moderation systems to ensure that their training adequately captures the nuances and variations of diverse languages and contexts and therefore, avoid discriminatory bias.
- Refuse to secretly collaborate with state authorities to moderate content, and include in the company's annual transparency reporting a country-by-country breakdown of the formal or informal reporting documenting formal or informal working relationships with state actors regarding content moderation and access to user information.
- Conduct in-depth, nuanced, and contextualized human rights due-diligence before launching features, products, and platforms that put sexual and gender minorities at risk. This ensures that the lived experiences of marginalized communities are taken into account in the design and development of companies' products.



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, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

For more information, please contact: un@accessnow.org



The Electronic Frontier Foundation (EFF) (<https://www.eff.org>) is the leading nonprofit organization defending civil liberties in the digital world. 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.

For more information, please contact: info@eff.org