****

**Children’s Rights and the Digital Environment**

The continual growth of the digital environment poses unprecedented opportunities and risks for children. The expansion of the internet and social media platforms has provided children with new avenues to access information and exercise their freedom of expression. For some children, access to information online about LGBTI issues or sexual and reproductive health information is transformative and literally life-saving. Online activism by children has also empowered millions of children to mobilize to advocate for themselves and issues of critical importance such as climate change, gun violence, and other threats to their safety and future.

At the same time, the digital environment can put children at particular risk, particularly due to their emotional and cognitive immaturity. Online sexual exploitation jeopardizes children’s safety and well-being, and violent groups have used online propaganda and social media platforms in attempts to recruit and manipulate children.

Human Rights Watch supports the Committee on the Rights of the Child’s decision to draft a General Comment concerning children’s rights in the digital environment, and offers this submission outlining key issues that should be taken into account.

**I. Privacy and data protection**

Every child has a right not to be subjected to arbitrary or unlawful interference with his or her privacy or correspondence.[[1]](#endnote-1) Protecting children from violence, sexual exploitation, or other harm is a legitimate state aim that can, in certain circumstances, justify interferences with children’s privacy or correspondence. However, any such interferences should be necessary and proportionate to achieving the legitimate aim in question, and should only take place in accordance with publicly available laws that clearly lay out the circumstances under which such interference might be permitted.

As appropriate and in an age-sensitive manner, special consideration should be given to ensuring that children are consulted in the development of laws affecting them and that the laws are available in a form they can understand.

It is critical for states’ surveillance and data-protection laws to take account of children’s rights. Unfortunately, massive state surveillance programs—in addition to threatening the rights of adults—may not take due account of whether the people surveilled may be children. In the United States, for example, federal surveillance laws and policies usually do not specifically take account of children’s rights, or even acknowledge that children may be caught in the dragnet. States should ensure that all their surveillance activities are necessary and proportionate in respect not only of adults, but also of children. The Committee may wish to consider whether a surveillance or data-collection program in which a state does not, or for technical reasons cannot, distinguish between information belonging to adults and children may intrinsically infringe upon children’s rights.

Similarly, states should adopt data protection laws to prevent abuses of private information by both government and corporate entities—and those laws should impose meaningful safeguards for children. The European Union’s General Data Protection Regulation (GDPR) recognizes that “children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.”[[2]](#endnote-2)

By contrast, in the United States, the Children’s Online Privacy Protection Act restricts website operators’ and online services’ collection of information from children under the age of 13—but does not include protections for children over this age.[[3]](#endnote-3)

In accordance with the need for data protections as well as the right to protection from “unlawful attacks on … honour and reputation,”[[4]](#endnote-4) the Committee should consider offering guidance on what states should do to ensure that children and their guardians have rights-compliant means of preventing and addressing harms arising from data that may expose children to sexual shaming on internet platforms or other attacks on their human dignity.

Further, children may be particularly at risk of identity theft and subsequent fraud, rendering the adequate protection of their personal data by government and businesses even more important.[[5]](#endnote-5)

**II. Freedom of expression and access to information; freedoms of thought and opinion**

Every child has the right to freedom of expression, and the freedom to seek, receive, and impart information and ideas of all kinds through any medium.[[6]](#endnote-6) Any government interferences with these rights must be lawful and necessary “for respect of the rights or reputations of others” or “for the protection of national security or of public order…, or of public health or morals.”[[7]](#endnote-7) The Convention on the Rights of the Child also provides that states “shall ensure that the child has access to information and material from a diversity of national and international sources.”[[8]](#endnote-8)

Russia’s 2013 “gay propaganda law”[[9]](#endnote-9) has had a stifling effect on access to affirming online education and support services, with harmful consequences for LGBTI youth. The legislation bans the “promotion of nontraditional sexual relations to minors”—a reference understood to mean a ban on providing children access to information about LGBT people’s lives. The ban includes information provided via the internet, and the law has been used by the Russian government to shut down websites that provide valuable information and services to teens.

For example, Deti-404 is an online group that offers psychological support, advice, and a safe online community for LGBT children, including those who experience violence and aggression because of their real or perceived sexual orientation or gender identity. The site has gained tens of thousands of members. Elena Klimova, who launched Deti-404, has been charged under the “gay propaganda” law three times for operating the site and forced to change its digital location or re-launch the group to keep it functioning. Since a 2016 court decision, the group’s website has been formally blocked in Russia.[[10]](#endnote-10)

Despite the restrictions, the internet remains a critical resource for LGBT youth in Russia—as it is for many children around the world.[[11]](#endnote-11)“The main source of information for me is the internet,” 17-year-old Veronika A. told Human Rights Watch. Nora T. told us that when she began to question her sexual orientation at age 14, she scoured the internet for articles by psychologists.

For some, the most important information they find online is that they are perfectly normal the way they are. “The most useful thing I found online [was] that being LGBT [is] absolutely normal. Apparently, I was lucky, because now I often come across negative information, negative statements about LGBT,” said Irina R., 15.

Other children in Russia have explained to Human Rights Watch how the internet offered them privacy and the freedom to explore the questions they had without risking an abusive encounter with an adult or peer. “I’ve been looking for information on the internet. Gender identity and sexual orientation are not topics about which you can ask teachers or read any books in the school library,” Vasily A., a 15-year-old transgender boy, told us.

Government-sponsored schools are agents of the state. In some countries, schools may be crucial in providing students with means of receiving and sharing information and opinions online, including by supplying devices; access to e-mail, chat, and browsing programs; and other hardware or software that facilitates digital learning and communication. However, this development also increases the ability of schools and other government entities to monitor children’s expression in a manner that may violate their rights, including by disproportionately hindering them from expressing opinions or beliefs. Software and services offered by the private sector in countries such as the United States may also enable schools and other government bodies to monitor children’s online lives even when children are not using school-owned devices—for example, when they publicly post or “like” items on social media using their own computers or mobile phones.[[12]](#endnote-12)

Although states have positive obligations to prevent violence at school, government entities should also respect, protect, and fulfill children’s free expression and other rights when taking steps to protect children’s safety. Human Rights Watch is concerned about government programs designed to counter or prevent “extremism” or “gang” activity that may deter children from expressing themselves, seeking or receiving information, or formulating opinions or thoughts in line with their rights.[[13]](#endnote-13) We are also concerned about school monitoring activities that may stigmatize students with mental health conditions and disproportionately interfere with—or, in effect, punish—their exercise of online free-expression rights.[[14]](#endnote-14) We note as well that automated tools for inferring and flagging children’s mental health, emotional states, or intentions based on online speech may not be fully capable of accounting for the use of slang, references to popular culture, hyperbole, or other features common to children’s online expression.[[15]](#endnote-15)

We emphasize that any government monitoring of students’ communications—including on school-owned devices—should respect privacy and free-expression rights and should therefore be restricted to what is lawful and necessary to achieving a legitimate aim. Schools and other government bodies should take particular care to ensure that they do not monitor, punish, or stigmatize online speech in a discriminatory manner.

Violent groups have used the internet and online propaganda to recruit and manipulate children. They may use email, chat rooms, e-groups, message boards, video recordings, and social media platforms, and sometimes cartoons, video games, or tailored messages designed to appeal to children. They may track the online behavior of specific internet users to identify children vulnerable to their propaganda and then, like targeted advertising, tailor their narrative. Children who engage in internet searches to learn more about Islam, for example, can end up being contacted and “groomed” by Islamic State (ISIS) recruiters seeking to build a relationship.[[16]](#endnote-16)

The Optional Protocol on Children and Armed Conflict requires state parties to provide children recruited by armed groups “all appropriate assistance for their physical and psychological recovery and their social reintegration.” The Paris Principles state that “children who have been associated with … armed groups should not be prosecuted or punished … solely for their membership.”[[17]](#endnote-17) Children accused of crimes committed while associated with armed groups “should be considered primarily as victims … not only as perpetrators.”[[18]](#endnote-18)

More generally, the CRC states that any prosecution of children for criminal acts should prioritize the best interest of the child and be conducted with the objective of rehabilitating the child and promoting the child’s reintegration and assumption of a constructive role in society. Children should only be detained as a last resort and for the shortest appropriate period of time.

Children may exercise their curiosity about issues related to terrorism, unaware that they are accessing proscribed content, or express themselves without being aware that their posts could be considered criminal offenses. In August of 2016 a teenage boy in Tajikistan was convicted of incitement to join ISIS and sentenced to a prison term of ten years and six months. According to a local report, the boy, a tenth-grade student, distributed Islamic State photos and video content on social media, and called on citizens of Tajikistan to participate in “extremist activity.” He was convicted of “urging compatriots to join the ranks of militants.”[[19]](#endnote-19) In Jordan, authorities arrested a 16-year old on charges of spreading ISIS propaganda. The boy said an ISIS supporter approached him on Facebook. The boy had few friends and said he saw the recruiter as a sympathetic listener and gateway to a virtual community. He told interviewers: “I was only a supporter in my heart and online; I never planned to take any action.” In March 2017, United Nations University interviewed two children detained by Jordanian authorities on terrorism-related charges for activity with the Islamic State; the children were accused of engaging with ISIS only over social media and claim never to have met any of its members or engaged in any terrorist activity offline.[[20]](#endnote-20) Such cases raise questions about whether states are treating online activities by children in a manner adequately sensitive to their development and rights.

Some governments, including those of France, Germany, Morocco, Spain, and the UK, have criminalized expression perceived to support the aims of violent extremist groups as “apology for terrorism” or “glorification of terrorism.” [[21]](#endnote-21) In Italy, a top court has ruled that a “like” on Facebook can constitute apology for terrorism.[[22]](#endnote-22) In May 2018, the UN Special Rapporteur on the promotion and protection of human rights while countering terrorism expressed concern at evidence that French laws criminalizing “apology for terrorism” had been used extensively against children.[[23]](#endnote-23) In 2015, French authorities charged a 16-year old boy with apology for terrorism after he posted to Facebook a cartoon deemed to satirize the murder of *Charlie Hebdo* cartoonists.[[24]](#endnote-24) To the extent that states apply them to children, these laws risk excessively or arbitrarily interfering with children’s free expression rights and prioritizing criminal punishment over measures that may better reflect the best interests of the child.

Counter-terrorism laws and measures, including “apology for terrorism” laws, should be carefully reviewed to ensure that they do not violate children’s rights to freedom of expression. UN Secretary-General Ban Ki-Moon stated that “laws should only allow for the criminal prosecution of direct incitement to terrorism, that is, speech that directly encourages the commission of a crime, is intended to result in criminal action and is likely to result in criminal action.”[[25]](#endnote-25) UN experts on freedom of expression have also stated that “criminal responsibility for expressions relating to terrorism should be limited to those who incite others to terrorism; vague concepts such as ‘glorifying’, ‘justifying’ or ‘encouraging’ terrorism should not be used.”[[26]](#endnote-26)

**III. Freedoms of association and assembly**

Any restrictions on children’s freedoms of association and assembly must be lawful as well as necessary to achieving a legitimate aim.[[27]](#endnote-27) We also recall in this context that the CRC obligates states parties to “ensure that the child is protected against all forms of discrimination or punishment on the basis of the … activities … of the child’s parents, legal guardians, or family members.”[[28]](#endnote-28)

Regarding the collection of data about “assemblies or their organizers and participants,” two UN Special Rapporteurs have written that “given the intrusiveness of such methods, the threshold for these [legal] tests is especially high.”[[29]](#endnote-29)

Many online activities generate data that may reveal where children have been or with whom they have associated. For example, mobile telephones continuously generate location data as part of their functioning, social media posts may include geo-tagging, and photographs may create a record of relationships or proximity. Schools, law enforcement, or other government entities may also use facial recognition technology to record where children have been, and with whom.

Human Rights Watch is concerned that through these technologies, government entities may engage in monitoring that unlawfully, unnecessarily, or inaccurately intrudes on children’s free-association rights. Children may appear in photographs with or generate location data while in proximity to family members or friends whom governments treat as suspicious (e.g., suspected “extremists” or gang members). They may attend controversial but lawful protests, including as they formulate and begin to express their own political opinions or other beliefs. Any state recording or monitoring of this information should take place in accordance with the rights requirements outlined above as well as due regard for children’s right to family life and the development of their personalities.[[30]](#endnote-30)

Human Rights Watch is also concerned that private technologies marketed to parents to track children’s locations may be misused as a tool of control by abusive family members, human traffickers, or others who may seek to prevent children from communicating or associating with others in accordance with their rights. States and businesses should adopt strong safeguards to prevent such misuse.

**IV. Discrimination**

Online monitoring that violates rights may pose a particular threat to girls and children who belong to minority or disempowered groups. Some children may be at particular risk of rights deprivations due to intersectional discrimination—for example, girls or LGBT youth who also belong to disempowered racial, ethnic, religious, or linguistic groups.

The CRC recognizes children’s right to education, as well as the importance of their “access to scientific and technical knowledge.”[[31]](#endnote-31) States should ensure that all children—including girls—have access to computer science and internet literacy education on an equal basis.

**V. Responsibilities of businesses**

A range of private companies offer tools for government surveillance generally, or for government or parental monitoring of children in particular. Pursuant to the United Nations Guiding Principles on Business and Human Rights, we recommend that the Committee affirm that states should “tak[e] appropriate steps to prevent, investigate, punish” and ensure redress for rights abuses that may arise as a result of the market for these tools.[[32]](#endnote-32) This market should be regulated by law to prevent and address the emergence and adoption of rights-harming software that may affect children.[[33]](#endnote-33)

In accordance with the Guiding Principles, businesses should also respect human rights when collecting, monitoring, accessing, storing, searching, or sharing information about children, and “should address adverse human rights impacts with which they are involved.”[[34]](#endnote-34) In particular, businesses should take steps to ensure that the tools they offer contain strong safeguards to prevent undue or discriminatory interferences with children’s privacy, free-expression, or other rights. They should take active, reasonable steps to inform themselves regarding whether any entity may be misusing their products to harm rights and take remedial action accordingly.

1. Convention on the Rights of the Child (CRC), art. 16; *see also* International Covenant on Civil and Political Rights (ICCPR), art. 17. [↑](#endnote-ref-1)
2. Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, April 27, 2016, Recital 38. [↑](#endnote-ref-2)
3. 15 U.S.C. § 6502(a), Pub. L. 105-277. Regarding this law, see generally Federal Trade Commission, “Complying with COPPA: Frequently Asked Questions,” <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>. [↑](#endnote-ref-3)
4. CRC, art. 16(1). [↑](#endnote-ref-4)
5. See, e.g., Kelli B. Grant, “Identity theft isn’t just an adult problem. Kids are victims, too,” CNBC, April 24, 2018, <https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html>. [↑](#endnote-ref-5)
6. CRC, art. 13(1). [↑](#endnote-ref-6)
7. CRC, art. 13; *see also* ICCPR, art. 19(2)-(3). [↑](#endnote-ref-7)
8. CRC, art. 17. [↑](#endnote-ref-8)
9. Russian Federal Law No. 135-FZ, “Aimed at protecting children from information promoting the denial of traditional family values,” June 29, 2013. [↑](#endnote-ref-9)
10. For more on Russia, *see* No Support: Russia’s ‘Gay Propaganda’ Law Imperils LGBT Youth, Human Rights Watch report, December 11, 2018, <https://www.hrw.org/sites/default/files/report_pdf/russia1218_web2.pdf>. [↑](#endnote-ref-10)
11. *See also* “The Nail that Sticks Out Gets Hammered Down”: LGBT Bullying and Exclusion in Japanese Schools, Human Rights Watch report, May 2016, <https://www.hrw.org/sites/default/files/report_pdf/japan0516web_0.pdf>. [↑](#endnote-ref-11)
12. See, e.g., Aaron Leibowitz, “Could Monitoring Students on Social Media Stop the Next School Shooting?”, *New York Times*, September 6, 2018, <https://www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html>. [↑](#endnote-ref-12)
13. See, e.g., Open Society Justice Initiative, *Eroding Trust: The UK’s PREVENT Counter-Extremism Strategy in Health and Education* (2016), <https://www.opensocietyfoundations.org/sites/default/files/eroding-trust-20161017_0.pdf>; Aaron Leibowitz and Sarah Karp, “Chicago Public Schools Monitored Social Media for Signs of Violence, Gang Membership,” *ProPublica Illinois*, February 11, 2019, <https://www.propublica.org/article/chicago-public-schools-social-media-monitoring-violence-gangs>. [↑](#endnote-ref-13)
14. See, e.g. Lynn Jolicoeur and Lisa Mullins, “To Detect Threats And Prevent Suicides, Schools Pay Company To Scan Social Media Posts,” *WBUR News*, March 22, 2018, <https://www.wbur.org/news/2018/03/22/school-threats-suicide-prevention-tech>. [↑](#endnote-ref-14)
15. See, e.g., Ben Conarck, “Sheriff’s Office’s social media tool regularly yielded false alarms,” *Florida Times-Union/Jacksonville.com*, May 30, 2017, <https://www.jacksonville.com/news/public-safety/metro/2017-05-30/sheriff-s-office-s-social-media-tool-regularly-yielded-false>; and Center for Democracy & Technology, “Mixed Messages? The Limits of Automated Social Media Content Analysis,” November 2017, <https://cdt.org/files/2017/11/Mixed-Messages-Paper.pdf>. [↑](#endnote-ref-15)
16. UNODC, *Handbook on Children Recruited and Exploited by Terrorist and Violence Extremist Groups: The Role of the Justice System*, 2017, p 13. https://www.unodc.org/documents/justice-and-prison-reform/Child-Victims/Handbook\_on\_Children\_Recruited\_and\_Exploited\_by\_Terrorist\_and\_Violent\_Extremist\_Groups\_the\_Role\_of\_the\_Justice\_System.E.pdf [↑](#endnote-ref-16)
17. Principles and Guidelines on Children Associated with Armed Forces or Armed Groups (“The Paris Principles”), January 30, 2007, <http://www.unicef.org/protection/files/ParisPrinciples310107English.pdf>, at. 8.7. [↑](#endnote-ref-17)
18. Ibid, at 3.6. [↑](#endnote-ref-18)
19. “В Таджикистане впервые осудили школьника за пропаганду экстремизма,” Regnum, August 4, 2016, https://regnum.ru/news/accidents/2163156.html [↑](#endnote-ref-19)
20. Mara Revkin, “I am Nothing Without a Weapon,” in Siobhan O’Neil and Kato van Broeckhoven, eds., Cradled by Conflict, UN University, 2018, p. 128. [↑](#endnote-ref-20)
21. Amnesty International, *Dangerously Disproportionate: The Ever-Expanding National Security State in Europe,* 2017. <https://www.amnesty.org/download/Documents/EUR0153422017ENGLISH.PDF> See also Morocco Penal Code, Article 218-2. [↑](#endnote-ref-21)
22. *The Local*, “A Facebook “like” can constitute apology for terrorism, rules Italy’s top court,” December 13, 2017, https://www.thelocal.it/20171213/a-facebook-like-can-constitute-apology-for-terrorism-rules-italys-top-court [↑](#endnote-ref-22)
23. United Nations Office of the High Commissioner for Human Rights, “Preliminary findings of the visit: UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism concludes visit to France,” May 23, 2018. [↑](#endnote-ref-23)
24. Christophe Turgis, “Charlie Hebdo: a Nantes, un adolescent de 16 ans poursuivi pour “apologie due terrorisme” sur Facebook,” *France Info,* January 17, 2015. [↑](#endnote-ref-24)
25. Report of the Secretary-General, “The protection of human rights and fundamental freedoms while countering terrorism”, A/63/337, 28 August 2008, para. 62 [↑](#endnote-ref-25)
26. Article 19, “Special Rapporteurs warn against restrictions on freedom of speech in conflicts,” 4 May 2015, <https://www.article19.org/resources.php/resource/37952/en/special-rapporteurs-warn-against-restrictions-on-freedom-of-speech-inconflicts> [↑](#endnote-ref-26)
27. CRC, art. 15; *see also* ICCPR, arts. 21-22. [↑](#endnote-ref-27)
28. CRC, art. 2(2). [↑](#endnote-ref-28)
29. United Nations Human Rights Council, “Joint report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies,” U.N. Doc. A/HRC/31/66, February 4, 2016, para. 74. [↑](#endnote-ref-29)
30. ICCPR, art. 17; CRC, art. 16. [↑](#endnote-ref-30)
31. CRC, art. 28. [↑](#endnote-ref-31)
32. United Nations Office of the High Commissioner on Human Rights, *Guiding Principles on Business and Human Rights* (2011), U.N. Doc. HR/PUB/11/04, Principle 1. [↑](#endnote-ref-32)
33. *Ibid.* [↑](#endnote-ref-33)
34. *Ibid.*, Principle 11. [↑](#endnote-ref-34)