September 2022

UN roundup and delegate guide: digital rights at the United Nations

HRC50 kicked off in a heated context. The now-former UN High Commissioner for Human Rights, Michelle Bachelet, announced the end of her term — coinciding with her infamous official visit to China. A number of governments and NGOs urged her to set the record straight on China's human rights crisis, and at the end of August, we saw the release of a long-awaited report alleging crimes against humanity, including allegations of extensive forms of intrusive surveillance and control, and calling for accountability for State actions against Uyghurs. Meanwhile, despite Russia's attack on Ukraine and resignation from the HRC, Russia retained observer status at the HRC and has continued to remain vocal during negotiations. In addition, the mandate for the Independent Expert on violence and discrimination on the basis of sexual orientation and gender identity (SOGI expert) was fortunately renewed, even as gender and sexual orientation remains a contentious "point" of debate among some UN Member States.

Despite the heat of these and other debates, the international community managed to make progress on key digital rights issues, as HRC50 piggy-backed off several noteworthy UN digital rights outcomes from our annual RightsCon summit:

- **UN experts jointly demanded attention to digital rights during conflict and humanitarian crises**: For a fourth year in a row, UN Special Procedures issued a joint statement ahead of RightsCon (see 2021, 2020, 2019 statements). This year's statement focused on digital rights during crises, citing "*shrinking civic space and rising digital authoritarianism through internet shutdowns, targeted surveillance, cyber and physical attacks on critical broadcast and communications infrastructure, the use of drones by domestic law enforcement, as well as disinformation and smear campaigns.*"
- **The UN High Commissioner strengthened her call for a spyware moratorium**: Michelle Bachelet reiterated her call for a moratorium on the export, sale, transfer, and use of surveillance technology until human rights safeguards are in place, adding "***or servicing of"*** to encompass additional actors. This was a welcome addition, particularly in the wake of the one year anniversary of the Pegasus Project revelations.
- **UN Human Rights previewed a major internet shutdowns report to hear from and engage directly with those impacted**: UN Human Rights' Peggy Hicks joined RightsCon for the *Fireside Chat: Local-to-global efforts to flip the switch on internet shutdowns*, leveraging the summit to *"bring the conversation [on shutdowns] to where it's happening."*

More action in New York

Even before HRC50 began, there were signs of an increasing emphasis on digital rights among participants in State-led multilateral UN initiatives in New York City, site of the UN headquarters and traditionally a place where participants focus more on political, financial, and security initiatives than on rights-based initiatives.

On 23 May 2022, the United States, under its Presidency of the UN Security Council, held the first-ever digital-focused **UN Security Council** **meeting** on technology and security under maintenance of international peace and security. Citing to Access Now and our #KeepItOn campaign (40:10-41:14), U.S. Ambassador Linda Thomas-Greenfield (who also served as Security Council President in May 2022), emphasized the need to "*ensure technologies serve as a force for positive change and not as a tool misused to perpetrate human rights abuses, fuel hatred, and exacerbate conflict.*" We anticipate the UN Security Council will put more focus on technology, international peace, and security going forward, as emerging technologies become intertwined with conflict situations. We are already witnessing leadership by specific countries, such as the United States and Kenya, who held an Arria Formula Meeting on countering online hate speech that we had the privilege to address.

Another promising development was the highly anticipated appointment of the UN Envoy on Technology (UN Tech Envoy), Amandeep Gill, on 10 June 2022. We welcomed this appointment, which has unfortunately been a largely closed-door process. We are among many well-wishers eager to engage with Gill and his office, particularly to gain more clarity regarding the upcoming UN Global Digital Compact initiative stemming from the UN Secretary General's Common Agenda and his Roadmap for Digital Cooperation.

These highlights are just the tip of the iceberg. Following are relevant updates on five main topics:

(1) **internet shutdowns**;
(2) **disinformation**;
(3) **surveillance and spyware**;
(4) **new and emerging technology**; and
(5) **cybercrime and cybersecurity**.

In addition, we address the impact of sanctions on digital rights.

After providing a summary, we offer tailored recommendations to help delegates take the next steps for advancing international norms and standards to protect human rights worldwide.

(1) INTERNET SHUTDOWNS AND CONNECTIVITY

On 23 June 2022, the now-former High Commissioner for Human Rights launched her highly anticipated **report on internet shutdowns** (A/HRC/50/55). The High Commissioner remained clear in her messaging: *States should refrain from imposing internet shutdowns and instead maximize internet access and remove barriers in order to facilitate online communication — an essential enabler of human* *rights in the digital age*. This messaging further solidified clearly established international norms regarding internet shutdowns (see for e.g. the UN Secretary General's Roadmap for Digital Cooperation A/74/821 at para 41). The High Commissioner's report, published pursuant to the resolution on ***The promotion, protection and enjoyment of human rights on the Internet*** (A/HRC/RES/47/16 at OP17), uniquely analyzes the trends, causes, and legal implications and impacts of internet shutdowns on a range of human rights, and notably included an emphasis on economic, social, and cultural rights. The report notes that *"the #KeepItOn coalition, which monitors shutdowns episodes across the world,* ***documented 931 shutdowns between 2016 and 2021 in 74 countries****, with some countries blocking communications repeatedly and over long periods of time."* Overall, the report moves the needle forward from a normative statement to suggest concrete measures to combat internet shutdowns, including a call to establish a "*collaborative mechanism for the systematic collection of information on mandated disruptions in which States, civil society and companies all contribute*" (A/HRC/50/55 at para 65). In conclusion, the High Commissioner's latest shutdowns report places the devastating impacts of internet shutdowns into the international spotlight, and also serves as an important advocacy tool for activists and allies around the world to use to combat internet shutdowns.

States continued to advance and maintain language on connectivity and condemn internet shutdowns in resolutions during the last Human Rights Council session. Brazil, Canada, Fiji, Namibia, Netherlands, and Sweden led the resolution on ***Freedom of opinion and expression*** **(Expression Resolution)** (A/HRC/RES/50/15). This year's iteration of the resolution was dedicated to the overarching theme of *digital and information literacy for the enjoyment of the right to freedom of opinion and expression*. It therefore includes important language on digital literacy (OP8(j)-(m); OP10), and connectivity (OP7), and maintains existing language on internet shutdowns (OP(8)(o)). As our civil society partners rightfully note, while the resolution addresses the timely theme of digital literacy, it does so at the expense of failing to address other core issues that critically undermine the right to freedom of expression. Such core issues include "criminal defamation and strategic lawsuits against public participation" (so-called SLAPPs). While streamlining and concision matter, we echo our civil society colleagues and call on States' to ensure that future resolutions — focused on freedom of expression and beyond — do not solely focus on narrowly defined themes, particularly regarding human rights online, at the expense of failing to encapsulate persistent and emerging issues both online and offline.

Switzerland and **Costa Rica** led the biennial resolution on ***The promotion and protection of human rights in the context of peaceful protests*** **(Protest Resolution)** (A/HRC/RES/50/21) which was adopted by consensus. We are pleased that the final text includes several operative paragraphs on internet shutdowns in the context of peaceful protests (OP3, OP16-17 and OP28). During informals surrounding this resolution, we witnessed both States and other civil society leverage the UN High Commissioner's newly launched report on internet shutdowns to strengthen language on internet shutdowns in the text.

We welcomed the latest resolution on the ***Situation of human rights in Belarus*** **(Belarus Resolution)** (A/HRC/RES/47/19), which extends the mandate of the UN Special Rapporteur. We particularly note OP4 of the renewed text which *"urges the Belarusian authorities to ensure a conducive environment for the functioning of genuinely independent media, both online and offline, including unhindered access to* *an open, interoperable, reliable and secure Internet."* While internet shutdowns are not explicitly mentioned, this text is arguably stronger than the previous Belarus Resolution from the HRC49 (A/HRC/RES/49/26), which *"expresses continuous serious concern about other ongoing severe politically motivated acts of repression against independent media and civil society, including through [...] the blocking of independent media websites and Internet shutdowns"* (OP5). This may partially be due to the fact that, since the previous resolution, the human rights situation in Belarus has worsened with the forced closure of human rights organizations and the detention and imprisonment of many human rights defenders. As highlighted in our submission to the UN Special Rapporteur on Freedom of Peaceful Assembly and of Association for his consideration for his HRC50 report, in Belarus since 2021, governmental authorities liquidated 344 NGOs, and 208 NGOs decided to initiate the liquidation process themselves in a fear of further persecution. We commend the UN Special Rapporteur for drawing attention to such issues in his HRC50 report on Access to resources (A/HRC/50/23).

We welcomed the resolution on the ***Situation of human rights of Rohingya Muslims and other minorities in Myanmar*** (**Myanmar Resolution**) A/HRC/RES/50/3. Myanmar's online space has been shrinking since the coup, particularly impacting Rohingya Muslims and other minorities in Myanmar. In 2021, people in Myanmar faced constant internet shutdowns. When the coup began, the shutdowns affected internet and voice connectivity, as well as non-military television and radio channels, across the country, and systematically evolved over time. Now, shutdowns take many forms, including curfew-style blackouts that disrupt connectivity through the nights, and the targeted shutting down of mobile internet services. Notably, there are reports of shutdowns constantly implemented in regions where armed conflict and military violence are most severe.[1] We therefore welcome the Myanmar Resolution's call on "*Myanmar to lift the shutdown of Internet and telecommunications services fully in all areas of Myanmar, including Rakhine State, and to repeal article 77 of the Telecommunications Act in order to avoid any further cutting of Internet and telecommunications access and the stifling of the rights to freedom of opinion and expression, including freedom to seek, receive and impart information, in accordance with international human rights law*" (OP12).

We delivered an oral statement on Myanmar highlighting the targeted communication blackouts by the military junta during the HRC50 Interactive Dialogue with the UN Special Rapporteur on Myanmar. Our statement underscores the importance of the international community standing in solidarity with the people of Myanmar and carrying out concrete measures to hold military leaders accountable for their crimes. We raised the alarm that the military junta could potentially require the IMEI (International Mobile Equipment Identity) number of phones to be registered, potentially giving them the power to collect data to track and locate people whenever they want. We also urged private companies to comply with their human rights obligations and take speedy, targeted, and efficient steps to protect the people of Myanmar.

At HRC50, the Council adopted Universal Periodic Review (UPR) country reports from the Council's 40th UPR session (UPR40) as well as Myanmar from the Council's 37th UPR session (UPR37). Access Now, with the support of our civil society partners, submitted six digital rights-focused stakeholder

[1] For the latest updates on Myanmar's Digital Dictatorship see: Access Now, Resist the Digital Coup in Myanmar, available online at: https://www.accessnow.org/spotlight/myanmar/ (2022).

submissions on Syria (including our participation in the UPR Info Pre-Session on Syria), Venezuela, Zimbabwe, Uganda, South Sudan, and Sudan ahead of UPR40, and Myanmar ahead of UPR37. We welcome more State recommendations addressing the impact of human rights online and offline. In light of our recommendations, we particularly appreciate **Canada's** recommendation to **Uganda** (A/HRC/50/11) to *"respect freedom of expression online, including by ending the practice of enforcing Internet shutdowns and taxing the use of social media"* and **Lithuania's** recommendation to **Sudan** (A/HRC/50/16) to *"investigate the physical and digital attacks against, and the harassment of journalists, media workers and human rights defenders, and ensure freedom of expression."* We further welcome **Finland's** recommendation to **Myanmar** (A/HRC/47/13) to "*review and amend all laws that violate the rights to freedom of expression, association and peaceful assembly, as well as digital rights*," but we nonetheless regret that there were no State recommendations made to Myanmar regarding internet shutdowns, especially considering the dire impact of shutdowns in the region.

On 15 July 2022, during the UN High-Level Political Forum (HLPF), Access Now and Internet Society hosted a virtual side event: *Preserving an open Internet to achieve the SDGs: The Internet as an enabler for achieving SDGs 4 and 5*. The speakers examined: efforts to expand unrestricted, inexpensive, and dependable access to the internet, how such efforts contribute to the UN Sustainable Development Goals 4 (education) and 5 (gender equality), and the challenges that undermine their achievement. It was noted that States' often view the internet as a threat to be contained and splintered rather than a resource to expand universally.

Recommendations

1. Strengthen the language in both country-specific and thematic resolutions to (1) condemn internet shutdowns and (2) expand connectivity to open, secure, interoperable, and universally accessible internet;
2. Ensure resolutions do not solely focus on narrowly defined themes, particularly regarding human rights online, at the expense of failing to capture persistent and emerging issues both online and offline;
3. Leverage existing language on internet shutdowns as captured in UN Human Rights Council and General Assembly resolutions as well as regional mechanisms such as the African Union (see e.g. A/HRC/Res/49/21; A/HRC/Res/47/16; A/HRC/Res/47/23; ACHPR/Res.362(LIX)2016);
4. Strategically leverage the findings and recommendations from the UN High Commissioner's shutdowns report for bilateral and multilateral engagement and negotiations with States ahead of and during government-mandated internet shutdowns;
5. Issue public thematic and country specific statements that highlight instances of network disruptions and coordinate through embassies in countries where network disruptions are taking place to jointly urge States to refrain from and cease such measures (see for example the 2020 Joint Statement on Internet Shutdowns in Belarus, the 2017 Freedom Online Coalition Joint Statement on State Sponsored Network Disruptions, and the G7 Foreign and Development Ministers' Meeting Communique);
6. Since it is clear that human rights violations online enable and escalate offline violence, we therefore recommend that more States prioritize and make explicit recommendations regarding the impact of internet shutdowns during the UPR and treaty body processes;

7. Meaningfully contribute to and adequately fund existing and new initiatives that collect information on mandated internet disruptions worldwide; and
8. Refrain from duplicating civil society-led and other existing multi-stakeholder initiatives that combat internet shutdowns. Instead, work within these established mechanisms through meaningful and inclusive collaboration.

(2) DISINFORMATION

We continued to witness a high level of attention on the spread of disinformation with a particular emphasis on State-sponsored disinformation in the Russia-Ukraine conflict. Pursuant to the resolution on the ***Role of States in countering the negative impact of disinformation on the enjoyment and realization of human rights*** (the Disinformation Resolution), (A/HRC/RES/49/21) on 28 June the Human Rights Council convened a high-level panel discussion on countering the negative impact of disinformation on the enjoyment and realization of human rights. This was the first opportunity for the Human Rights Council to focus on the role of States in countering the negative impact of disinformation. The panel gathered an impressive line up of high-level speakers to discuss policies and actions taken to counter disinformation. Speakers also proposed recommendations on the best ways to address the issue from a human rights-based perspective.

Recommendations

1. Strengthen the language in both country-specific and thematic resolutions to condemn the spread of State-sponsored disinformation campaigns while ensuring a free, open, interoperable, reliable and secure Internet where diverse voices are heard, and in full respect of human rights;
2. Leverage existing language on disinformation as captured in UN Human Rights Council and General Assembly resolutions (see for example A/HRC/RES/49/21 and A/RES/76/227);
3. Strategically leverage the findings and recommendations from UN Special Procedures (see for example A/HRC/47/25) and the findings of the high-level panel for bilateral multilateral engagement and negotiations with States; and
4. Issue public thematic and country-specific statements that condemn the spread of State-sponsored disinformation campaigns (see for example the 2020 FOC Joint Statement on Spread of Disinformation Online and the Statement on behalf of the Chair of the Freedom Online Coalition: A call to action on state-sponsored disinformation in Ukraine).

(3) SURVEILLANCE AND SPYWARE

The arbitrary or unlawful use of surveillance technologies violates human rights and causes real-world harm. The rampant abuse and culture of impunity surrounding surveillance technology also contravenes well-established international norms. Access Now and our civil society partners have previously urged UN Member States to denounce spyware abuses and mandate comprehensive measures to investigate and prevent further violations linked to the sale, export, and use of such spyware and cases of targeted surveillance. Since then, some States have made huge strides to combat the arbitrary or unlawful use of surveillance technologies. **Costa Rica** became the first State to publicly call for the *"immediate moratorium on the use of spyware technology until a regulatory framework that protects human rights is implemented."*

The previously mentioned **Expression Resolution** contains language on the arbitrary or unlawful use of surveillance technologies in the context of digital, media, and information literacy risks (OP2, OP8(j)). While this language is welcomed, we witnessed stronger efforts advanced during HRC50 negotiations surrounding the previously mentioned **Protest Resolution**. The Protest Resolution specifically incorporates strong language to protect online protests and address violations of the right to privacy. We commend the core group for developing strong language against the use of spyware and facial recognition technology against protesters that we can build upon in future texts at both the Human Rights Council and the General Assembly. In particular, the Protest Resolution protects protesters from the use of spyware (like NSO Group's), "facial recognition and biometric surveillance" (OP29) and "less lethal weapons" (OP30-31). We welcome these advancements and commend Switzerland and Costa Rica for their diplomatic efforts, particularly previous drafts of the resolution, which included an initial **call for a global moratorium on the sale, transfer, and use of such targeted surveillance technologies**. We were nonetheless disappointed that such strong language did not remain in the final text due to hostile last-minute amendments.

In light of the deteriorating human rights situation in **Belarus**, during our oral statement we called upon UN Member States to immediately stop providing censorship and surveillance technologies to the Belarusian regime and to help support and protect Belarusian civil society (both inside the country and in exile) through financial, technological, and visa assistance. We also urged tech companies to consult with civil society on human rights impacts of sanctions to avoid sanction overcompliance and to provide Belarusian activists with affordable and secure digital tools and services to circumvent surveillance and censorship.

The impact of targeted surveillance on women can be particularly grievous, given that cultural, political, societal, economic, and gender power asymmetries often grant authorities opportunities to weaponize the information they extract through defamation, blackmail, and doxxing. In our submission to the UN Special Rapporteur on Freedom of Opinion and of Expression for consideration in her HRC50 report, we highlight surveillance as a form of gender-based violence by recounting the hacking of two women human rights defenders from **Bahrain** and **Jordan,** perpetrated using NSO Group's Pegasus spyware. For women targets, digital surveillance is a ticking bomb. They live in fear of how their personal information, including private photos, videos, and conversations, could be used against them at any given point, opening the door for harassment and abuse. This is especially worrying in regions, such as MENA, where governments have routinely used doxxing of women and LGBTQ+ activists in order to smear and intimidate them into silence.

We, along with other civil society organizations, highly commend the UN Special Rapporteur on Freedom of Opinion and of Expression's important HRC50 report ***Reinforcing media freedom and the safety of journalists in the digital age*** (A/HRC/50/29). We particularly welcome the Special Rapporteur's finding that "*women journalists have been disproportionately targeted in some countries and have experienced severe harm from targeted digital surveillance, which operates as a form of* *gender-based violence*" (para 46) and the recommendations to protect women journalists from gender-based online violence (paras 118 - 121). The UN Special Rapporteur on Freedom of Opinion and Expression's push for holistic, gender-responsive solutions is particularly timely as we plan ahead for the upcoming Commission on the Status of Women (CSW67). Next year, CSW67 will prioritize the theme of *innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls.*

Biometric technologies are increasingly being deployed worldwide. Biometric identifiers, including fingerprints, iris scans, and facial geometry, have become increasingly popular as a means of enrolling individuals into systems and then authenticating users. Biometric data is vulnerable to hacking just like other authentication methods. However, unlike a password, biometric indicators cannot simply be reset or changed as needed. This poses a higher security risk, since it becomes increasingly difficult to repair the damage done by leaks or hacks of biometric data, and thus restore sanctity to biometric-based systems. In June 2021, Access Now, Amnesty International, European Digital Rights (EDRi), Human Rights Watch, Internet Freedom Foundation (IFF), and Instituto Brasileiro de Defesa do Consumidor (IDEC) called for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance. These tools have the capacity to identify, follow, single out, and track people everywhere they go, undermining our human rights and civil liberties — including the rights to privacy and data protection, the right to freedom of expression, the right to free assembly and association (leading to the criminalization of protest and causing a chilling effect), and the rights to equality and non-discrimination. In China, the United States, Russia, England, Uganda, Kenya, Slovenia, Myanmar, the United Arab Emirates, Israel, and India, surveillance of protesters and civilians has harmed people's right to privacy and right to free assembly and association.

In our recent submission to the UN Office of the High Commissioner for Human Rights for their consideration in the newly released report to the Human Rights Council 51st session (HRC51) on the right to privacy in the digital age, we therefore focused on the use of biometrics for identification and authentication. In our submission, we made recommendations to States, the private sector, and international organizations, including **calling on the High Commissioner to issue a moratorium on the processing of biometrics in identity systems.** Specifically, digital identity systems should not collect or use biometrics for the authentication/verification of an individual's legal identity and check for duplicate records until it can be proven that such biometric data processing is completely safe, inclusive, not liable to error, and is the only proportional method of authentication available for the purpose of the system.

While resolutions may be renewed with a different thematic focus, we should not lose sight of important developments from previous iterations. The HRC49 **Myanmar Resolution** (A/HRC/RES/49/23) contained notably important language on the right to privacy while drawing on issues such as hacking, surveillance, collecting personal data, and the use of biometric technologies (see e.g. OP25). Such important language was unfortunately not recaptured in this session's Myanmar Resolution. Nonetheless, delegates should rely on the privacy rights language adopted in the HRC49 Myanmar Resolution for future resolutions, whether country or thematic resolutions.

Recommendations

1. Strengthen the language in both country-specific and thematic resolutions to denounce spyware abuses and mandate comprehensive measures to investigate and prevent further violations linked to the sale, export, and use of such spyware and cases of targeted surveillance;
2. Leverage existing language on surveillance and spyware abuses as captured in UN Human Rights Council and General Assembly resolutions (see for example A/HRC/50/21; A/HRC/RES/45/18; A/76/173; A/HRC/RES/48/4; A/RES/75/176);
3. Join existing State-led initiatives, including the multilateral “Export Controls and Human Rights Initiative" to take spyware threats seriously;
4. Join efforts led by States, such as Costa Rica, to place an immediate moratorium on the use, sale, servicing, and transfer of surveillance technologies produced by private firms until adequate human rights safeguards and regulation are in place. To support this transition, Access Now and other civil society organizations have developed 13 Principles to guide law enforcement and policymakers in ensuring respect for human rights in surveillance activities;
5. Advance international norms to recognize unlawful or arbitrary surveillance as a form of gender-based violence (see for example A/HRC/50/29 and A/HRC/44/52);
6. Leverage existing language on biometric technologies as captured in UN Human Rights Council and General Assembly resolutions (see for example A/HRC/RES/49/23; A/HRC/RES/48/4); and
7. Call upon States, the private sector, and international organizations to clearly articulate the objectives, needs, and benefits of any digital ID programs and independently evaluate necessary safeguards with audit reports being made public. Biometric data should not be collected until such biometric authentication is proven to be completely safe, inclusive, not liable to error and is the only method of authentication available for the purpose of the program.

(4) NEW AND EMERGING DIGITAL TECHNOLOGIES

Through State-led initiatives, such as **Denmark** and the **Republic of Korea**, the UN continues to examine the opportunities and challenges of new and emerging digital technologies with regard to the promotion and protection of human rights (see for example A/HRC/RES/41/11).

The explosion in digital technologies is playing a major role in reshaping cities into so-called smart cities. Local governments must ensure that such technological developments favor inclusive, resilient, and sustainable use. On 24 June 2022, Access Now's Peter Micek participated in an HRC50 side-event ***Smart cities and human rights: pitfalls and opportunities*** organized by the Geneva Cities Hub, Geneva Rights Platform, and the University of St. Gallen. The workshop took stock of the human rights deliverables under the UN and identified good practices of smart city projects in Chile and Switzerland to realize human rights and recommend measures that could be envisaged more generally by the Human Rights Council and other intergovernmental bodies.

September 2022

The mandate for Ahmed Shaheed, the former UN Special Rapporteur on Freedom of Religion or Belief, recently concluded. We commend Shaheed for his insightful contributions as UN Special Rapporteur, particularly his recent General Assembly report ***Respecting, Protecting and Fulfilling the Right to Freedom of Thought*** (A/76/380), which highlights how we must prevent emerging technologies from being used and abused to infer, manipulate, or influence people's thoughts. The Special Rapporteur states that "*ostensibly, modern technologies pose a global and multi-sectoral challenge for freedom of thought, given their increasingly ubiquitous and developing ability to infer one's thoughts, even if this ability is currently relatively inconsistent and inaccurate.*" He cautioned that contemporary legal frameworks are unprepared for such new and emerging technologies and that they require human rights compliance.

We provided input on this report and strongly supported the ban of practices that adversely impact people's absolute right to freedom of opinion and freedom of thought, by influencing their thoughts and opinions without their knowledge or consent. We argued that States must not directly or indirectly protect business models of large online platforms that rely on surveillance-based advertisement and that violate international human rights law. The intrusion of AI systems into the forum internum must be cut off at the root by prohibiting emotion recognition.

Recommendations

1. Ban human rights-abusive methods of surveillance-based advertisement that violate absolute rights to freedom of thought and freedom of opinion. Such a ban should be complemented by stronger enforcement of data protection laws, including the General Data Protection Regulation, competition regulation, and consumer protection legislation.
2. Ban the conception, design, development, deployment, sale, import, and export of emotion recognition technologies, in recognition of their fundamental non-compliance with international human rights standards and discriminatory impact on historically marginalized and oppressed groups.
3. The private sector must fully comply with criteria of legally mandated meaningful transparency. In practice and at minimum, private companies should disclose meaningful information about parameters used to determine and target the recipient to whom the advertisement is displayed, including the category and source of personal data uploaded to the online platform, and the legal basis for uploading this personal data pursuant to the legal basis for uploading this personal data as established by data protection regulatory framework.
4. Promote the use of strong encryption, particularly in publicly accessible communication technologies, which offer online security, privacy, and anonymity without discrimination. As secure communication technologies are essential to the promotion and development of human rights, resources must be allocated to ensure that individuals and communities, particularly those at risk, engaged in human rights protection and interacting with international organizations and civil society, have access to encrypted communication channels.

(5) CYBERCRIME AND CYBERSECURITY

Approaches to cybersecurity policy should be user-centric, systemic, and anchored in open and pluralistic processes. Cyberwarfare adversely impacts a range of human rights and cyber operations targeting journalists, civil society organizations, and human rights defenders are particularly alarming and should be prohibited in all circumstances. Individuals who work in defense of civil liberties, rights, and democracy are themselves a form of "critical infrastructure" that must be safeguarded as we enhance legal structures on cybercrime and cybersecurity; these defenders are often providing direct, essential services and advocating for the needs of the most vulnerable.

Between 30 May to 10 June 2022, the UN Ad Hoc Committee on Cybercrime (AHC on cybercrime) held its second substantive session. The session involved "*a first reading of the provisions on criminalization, general provisions, and provisions on procedural measures and law enforcement in accordance with the road map and mode of work of the Committee*." Access Now contributed to questions on criminalization, procedural measures, and law enforcement, through both written and oral interventions. The third substantive session was subsequently held in New York between 29 August to 9 September 2022 . We contributed to *provisions on international cooperation* through an oral intervention. We recognize that while international cooperation measures are crucial, they also risk adversely impacting the rights to privacy, data protection, and other fundamental human rights. We therefore stressed that any international legal framework on cybercrime cooperation must ensure appropriate legal standards, accountability, remedy, authentication, and oversight in legal assistance — including a clear role for judicial institutions. We specifically recommended that the AHC on cybercrime adopt the definitions and procedural safeguards outlined in the International Principles on the Application of Human Rights to Communications Surveillance.

On 27 July 2022 we addressed the third substantive session of the OEWG on ICTs II. We suggested that the OEWG on ICTs II document best practices at the national level for government and private sector stakeholders to engage *with civil society*, as well as the threats and systemic challenges that may face the *civil society information security community*. We stressed that *"cyber threats to human rights defenders, journalists, and humanitarian actors must be referred to in the report,"* recognizing that *"international humanitarian law applies to cyberspace and that international law does apply to cyber offensive activities."* We supported the joint call made by Switzerland on behalf of itself and 16 other States, and emphasized that *an explicit mention of international humanitarian law, and the role of the ICRC, must be added to the Report.* We also stated that *"the report must recognize that digital rights violations —including those taking the form of cyberattacks that enable and escalate offline violence, and the calculated attacks targeting digital systems essential to people's safety, rights, and wellbeing — are unacceptable."*

Recommendations

1. Embed international humanitarian law in legal frameworks concerning cyberspace and cyber offensive activities;
2. Guide any new initiative related to encryption and secure communications tools that play a key role in deterring unauthorized access to communications and data, and preventing crime,

by the May 2015 report of the former UN Special Rapporteur on Freedom of Opinion and Expression (A/HRC/29/32);

3. Ensure data sharing initiatives adhere to principles of dual-criminality, proceed in writing under standard protocols, and raise, not lower, protections against arbitrary or unlawful interference;
4. Use our Universal Implementation Guide for the Necessary and Proportionate Principles, which provides a detailed, step-by-step guide to creating a legal authorization and disclosure process for data requests;
5. Ensure international efforts to harmonize approaches to cybercrime avoid including content or speech related provisions, and focus on a global consensus approach to cyber-dependent crimes (international cooperation measures are crucial, but also risk impacting privacy and other fundamental human rights); and
6. Ensure the inclusion of voices from humanitarian actors, human rights defenders, and the digital security community, who assist civil society in digital safety, in international discussions around cybersecurity and responsible State behavior, to prepare for the new threat actors and heightened cyber disruptive activity we face in 2022.

A NOTE ON SANCTIONS

Sanctions have become a go-to tool for foreign policymaking, with the U.S., U.K., and the E.U. in lockstep. Yet, we continue to witness little to no meaningful discussions at multilateral institutions like the UN Human Rights Council about the adverse impact of sanctions on human rights. It is long overdue. We, along with our partners, continue to conduct research into the impact of sanctions on human rights, and the specific harms caused by "overcompliance," which are detailed in several of our recent UN submissions, including our submission to the UN Special Rapporteur on the negative impact of the unilateral coercive measures on the enjoyment of human rights. The UN Special Rapporteur will report on "secondary sanctions, civil and criminal penalties for circumvention of sanctions regimes, and over-compliance with sanctions" and "unilateral sanctions in the cyber world," as well as exploring calls to establish a universal and uniform system of indicators for identifying and assessing the specific impact of unilateral sanctions – those imposed by States or groups of States outside the context of international sanctions authorized by the UN Security Council. We look forward to engaging the UN human rights system to advance digital rights in tech sanctions regimes, and reduce corporate overcompliance with State sanctions in ways that leave people and communities disconnected and vulnerable online. Whether in Ukraine or Myanmar, the openness and security of digital spaces matters for human rights. We continue to engage in bilateral discussions and advocacy campaigns regarding the impact of State sanctions on digital rights.

Recommendations

1. We call on states issuing sanctions, including the vast and growing lists responding to Russia's invasion of Ukraine, to request a review of their sanctions policies and practices for consistency with their commitments to international human rights law and norms.

2. We call on the OHCHR to update its excellent 2012 report on unilateral coercive measures for the digital age, with attention to the human rights impacts of tech sanctions and the role of the tech sector in their implementation.

CONCLUSION

As we look ahead to the coming UN processes and sessions, we hope to help bring more civil society voices to the UN. Now, more than ever, world leaders must hear directly from those impacted by the weaponization of the internet against people targeted for persecution, discrimination, human rights abuses, ethnic cleansing, and other atrocities. We hope this brief can serve as a go-to guide for UN delegates and other stakeholders as we continue to advocate for this openness, so we can together build a more powerful platform for civil society worldwide.

September 2022

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***

Peter Micek | General Counsel and UN Advocacy Manager | peter@accessnow.org |

Laura O’Brien | Senior UN Advocacy Officer | laura@accessnow.org |