RightsCon Tunis 2019

BROUGHT TO YOU BY accessnow

RightsCon Tunis 2019 Learnings

Upholding Human Rights in the Digital Age

Today, every aspect of human rights is impacted by technology. No single issue can be considered in a silo, and the convergence of these issues affirms the complexities we face when defending human rights in the digital age. Now more than ever, it is crucial for policymakers, tech developers, people working in international organizations, development agencies, civil society, and all other stakeholders to come together and achieve shared understandings of how their work uniquely impacts human rights in the digital age.

Across each issue and sector, human rights must be at the center of every product design and policy decision. Respect for human rights and the needs of marginalized communities must be foundational, rather than an afterthought, if we hope to prevent avoidable and often irreversible harms.

RightsCon Tunis 2019: Learnings is a statement that considers each major topic of conversation at RightsCon 2019, outlining a starting point for centering human rights in each industry and body of work. We encourage the broader global stakeholder community to incorporate these ideas across sectors toward their own goals.

We understand and acknowledge that the richness and diversity of debate taking place among nearly 3,000 participants across 450 sessions cannot be fully captured here. However, it is our hope that it may begin to capture the thought leadership and essential conversations that took place throughout RightsCon 2019, highlighting the most important themes and learnings.

Artificial Intelligence, Automation, and Algorithmic Accountability

As automated decision-making tools proliferate and fundamentally modify the way our societies, institutions and markets work, it is important to acknowledge the existing body of universal, binding, and actionable human rights laws and standards as the foundation upon which these technologies must be designed, developed, and implemented. Preventing discrimination and other human rights abuses requires a commitment to fostering diversity, meaningful consultation with at-risk communities about the particular ways in which they could be impacted, and clear pathways for algorithmic accountability both in the public and private sector when the use of automated technologies undermine fundamental rights.

Forging Alternative Models for Business and Human Rights

Companies are responsible for assessing, understanding, and effectively mitigating the impact of their processes, products, and services on human rights, and for helping to remedy abuses. Business models that rely on the exploitation of users' personal data and privacy — as a basis for advertising revenue or a pathway to surveillance — are fundamentally contrary to human rights. Companies both large and small must adopt approaches that integrate human rights-by-design and empower users with autonomy over their data. Private and government investments should foster market diversification by supporting startups and small and medium-sized technology companies, as well as the development of new technologies that are human rights-respecting by design.

Tech for Public Good: Open Government and Smart Cities

The use of technology in public life should be centered around transparency, openness, and human rights, in particular, privacy and security, as the pillars of trustworthy public services that enhance the overall well-being of citizens. Technology that is deployed in urban or rural spaces must always be used equitably and inclusively, and never generate new pathways of exclusion. The development of smart cities and the implementation of safety and security programs must never come at the cost of individuals' freedoms through data collection and surveillance.

Countering Online Harassment, Hate Speech, and Violent Extremism

Current approaches to addressing problems with content moderation can harm human rights, and have often failed to protect vulnerable communities like women, LGBTQ people, ethnic minority groups and others at risk online. Any measures undertaken whether by companies or governments in an effort to remove online content that is considered harmful must serve a legitimate aim and adhere to the principles of legality and proportionality. When making decisions, governments and companies should carefully assess the potential detrimental impact on freedom of expression and access to information online before they deploy any new measure, in particular, to avoid any form of censorship. In addition, any regulation that risks impacting free speech online must be fully compliant with human rights law and developed and adopted through open democratic debate and in full transparency. Any individual impacted by these measures should be afforded due process and adequate remedy.

Lock and Key: Cybersecurity and Encryption

Governments should not pursue cybersecurity strategies that seek unilateral control over the internet and instead should focus on norms, regulations, principles, and practices that enable and promote the protection of individual users and their data. These measures should afford users the capacity and resources to defend themselves from cyber attacks and mitigate exposure to cyber risks.

Government intervention aimed to weaken or undermine encryption creates cybersecurity risks that can potentially interfere with the human rights of users, disrupt the digital economy, and harm the integrity of critical infrastructure. Therefore, investing in and adopting strong encryption tools that meet the highest international standards for cybersecurity practices is essential to ensure community safety.

Data Trust, Protection, and User Control

Countries around the world must adopt and enforce robust data protection laws to ensure users' personal data are safeguarded at all times. Policy-makers should create legal and regulatory frameworks that put individuals and their rights at the forefront, giving users meaningful and actionable control over their personal data. These frameworks should also require that connected products and online services protect privacy and data protection by design and by default. Data protection principles are especially crucial in the context of digital identity programs, which can bring about great benefits but also severe risk of harm to individuals who are marginalized and underserved — including refugees, migrants, and rural communities. Governments and technology companies should avoid compiling sensitive personal information in centralized databases, and ensure transparency and oversight in determining how data can be accessed.

Democracy, Conflict, and Shrinking Civic Space

Governments have an unwavering responsibility to respect civil society and to refrain from any attacks on those who seek to defend human rights, protect democracy, and promote access to information, especially during election cycles and other moments of public importance. Both the public and private sector must prevent and mitigate attacks meant to disrupt democratic and civic processes, which are especially prevalent in fragile democracies and conflict zones. Countermeasures include monitoring electoral processes for digital interference, understanding the impact of online platforms used as mediums for democratic participation, and empowering marginalized voices, especially in times of conflict, to be represented and respected both online and off.

Intersectionality on the Internet: Diversity and Representation

With approximately four billion individuals connected to the internet and four billion yet to come online, we are at an important inflection point in ensuring the internet is a space by and for everyone. Governments, tech companies, development agencies, civil society organizations, and all other stakeholders must broaden our understanding of who the internet does and does not serve, accounting for questions of accessibility and language, gender-based violence and discrimination, and more. It is critical that populations that are currently marginalized, such as indigenous peoples, LGBTQ individuals, religious and cultural minorities, and people of color, be at the forefront of decision-making processes that impact the future of digital spaces.

(un)Censored: The Future of Expression

Censorship continues to present one of the most severe threats to fundamental human rights in the digital age, and its consequences must not be overlooked. Government policies and companies' terms of service that authorize and legitimize the use of censorship in the name of security can be short-sighted and not fit for purpose. Restrictions to the free flow of information undermine democratic participation, limit education and innovation, and in some cases, even put lives at risk. Technologists, trainers, activists, and journalists are working diligently to empower users with the tools and knowledge necessary to safely circumvent censorship and to find creative pathways to communicate, get access to information, and keep their content accessible.

Turn It On and #KeepItOn: Connectivity and Shutdowns

The internet should be accessible to all, without favoring or discriminating against certain communities, websites, applications, or services. In pursuit of that goal, governments and telecommunications service providers — in consultation with civil society — should ensure connectivity initiatives respect human rights, benefit and empower local users, and support alternative internet infrastructures modeled on decentralization and resilience.

Equally important to bringing people online, governments and service providers must commit to keeping them there. Intentional network disruptions, including blocking of social media platforms and messaging applications, pose a serious threat to free expression, association, assembly, and access to information, alongside their negative impact on work, education, access to healthcare, and beyond. Telecommunications service providers should, at a minimum, commit to transparency around government requests for blocking, and judicial oversight bodies should assist to the greatest extent possible in enforcing legal obligations to refrain from shutting down the internet.

Justice, Jurisdiction, and the Rule of Law

The internet has imposed significant challenges to jurisdiction and sovereignty, while at the same time opening the door to abuse of people's rights and data on a massive scale. The lack of clarity around how data can and should move across jurisdictions has eroded the rights of people and the rule of law. Succinct legal and regulatory standards that include digital due process must be established to address these problematic realities. Civil society organizations are often confronted with governments that use their legislative and policy-making powers to de-fund, impede, or even force the disappearance of important actors and voices. To better defend themselves, civil society organizations must strengthen themselves by cooperating and forming better, more resilient networks.

The Future of Media in the Age of Misinformation

In the face of widespread misinformation wielded to undermine democratic discourse, cultivate polarization, and minimize the visibility of credible stories, traditional media sources should confront their eroding legitimacy and adopt new models for success. The media landscape must continue to diversify, empower readers with better tools and literacy skills, incorporate reliable fact-checking mechanisms, and deliver consistently higher quality reporting. Those confronting misinformation must also consider the privacy invasive business models that have contributed to its popularity and enabled its weaponization.

The Digital Disruption of Philanthropy

Funding relationship models should put recipients at the forefront of programmatic design and implementation. It is essential to foster financial sustainability and protection for recipients through healthy donor-grantee relationships. These models should adapt and respond effectively to state strategies that are aimed at undermining and degrading the financial health of organizations in order to disrupt the services of the people they serve.

Privacy, Surveillance, and Individual Security

Privacy is the cornerstone of human rights in the digital age, and users are entitled to adequate legal protections. It is the duty of product manufacturers and service providers to design and implement privacy by design. Governments must limit state-sponsored surveillance within, at, and across borders only to what is necessary and proportionate. Laws authorizing — or failing to limit — governments, legal authorities, and technology companies conducting online surveillance must be brought into alignment with international human rights obligations. Companies that create surveillance technologies must account for the human rights impact of their products on at-risk users and prevent the sale of these tools to known human rights abusers.

Show and Tell: Skill-building for Advocacy and Campaigning

Advocating for an open internet, free of persecution and harassment, is dependent on the participation and resilience of civil society. Increased investment in technical innovations, tools, and skills is essential to empowering civil society and expanding the movement for human rights in the digital age.

Individual and Organizational Wellness and Resiliency

The digital community is well-known to burn the candle at both ends: while many are energized by this intensity, burnout is a damaging reality in our space. Worse, advocates around the world are facing increasing challenges: closing civil society space, online harassment, and even physical risks and abuse by governments and armed groups. There is a real opening for change if we can reconnect with the purpose behind our work, join together to advance our well-being, and tap into the resources to transform our workplaces and advocacy spaces. Organizations, companies, and governments should create and maintain healthy workplace environments to support their sustainability and their overall mission. The civil society space needs to see harmful cultures eliminated and the focus put on establishing healthy habits and processes to create and strengthen work-life balance. Funders should support well-being initiatives and welcome advocates' efforts to create sustainable, resilient organizations.

The Impact of Technology on the Sustainable Development Goals

Digital technologies are core enablers of the United Nations Sustainable Development Goals, but their integration must be done responsibly, with full understanding and mitigation of their impact on privacy and other fundamental human rights. Further, the tech sector must account for its own impact on sustainable development, on issues ranging from the environment and human health to land rights to fair labor practices. The technology, human rights, and development sectors must work together, in coordination and cohesion, to effectively advance toward a more equitable and sustainable world for everyone.

To stay connected, join our movement, and for more information see AccessNow.org and RightsCon.org. You can sign up for our newsletter at https://www.accessnow.org/express.

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