Freedom Online Coalition Working Group 1 “An Internet Free and Secure”

RECOMMENDATIONS FOR HUMAN RIGHTS BASED APPROACHES TO CYBERSECURITY

The following recommendations have been developed as a part of the mandate of the Freedom Online Coalition Working Group 1 “An Internet Free and Secure”[1] to bring a human rights framing to ongoing debates on cybersecurity[2] through the development of meaningful multistakeholder outputs that enhance and feed into existing cybersecurity processes.[3]

The Working Group sees these recommendations as a first step towards ensuring that cybersecurity policies and practices are based upon and fully consistent with human rights – effectively, that cybersecurity policies and practices are rights-respecting by design. The recommendations build on the Working Group’s definition of cybersecurity[4] and on existing frameworks, recommendations, and commitments to human rights in cybersecurity (Annex).

The Working Group encourages all stakeholders to incorporate the following definition in their cybersecurity policies and deliberations:

Preamble:

International human rights law and international humanitarian law apply online and well as offline. Cybersecurity must protect technological innovation and the exercise of human rights.

Definition:

Cybersecurity is the preservation – through law, policy, technology, and education – of the availability, confidentiality* and integrity* of information and its underlying infrastructure so as to enhance the security of persons both online and offline. (*as defined by ISO 27000 standard.)*

The Working Group commends these recommendations to all stakeholders - governments, international organisations, the private sector and civil society, including academic and technical communities - involved in cybersecurity policy development and implementation.

[1] https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/

[2] The Working Group is conscious of various terms used in this context, but is using the term cybersecurity for the reasons elaborated in the following article: http://isnblog.ethz.ch/intelligence/cybersecurity-and-the-problem-of-definitions

[3] As per the Working Group Term of Reference, these recommendations represent the views of the Working Group, and do not necessarily represent the views of the Freedom Online Coalition or its members.

[4] The elements of the definition and its background are further elaborated here: https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/blog8/

RECOMMENDATIONS

1. Cybersecurity policies and decision-making processes should protect and respect human rights.
2. The development of cybersecurity-related laws, policies, and practices should from their inception be human rights respecting by design.
3. Cybersecurity-related laws, policies and practices should enhance the security of persons online and offline, taking into consideration the disproportionate threats faced by individuals and groups at risk.
4. The development and implementation of cybersecurity-related laws, policies and practices should be consistent with international law, including international human rights law and international humanitarian law.
5. Cybersecurity-related laws, policies and practices should not be used as a pretext to violate human rights, especially free expression, association, assembly, and privacy.
6. Responses to cyber incidents should not violate human rights.
7. Cybersecurity-related laws, policies and practices should uphold and protect the stability and security of the Internet, and should not undermine the integrity of infrastructure, hardware, software and services.
8. Cybersecurity-related laws, policies and practices should reflect the key role of encryption and anonymity in enabling the exercise of human rights, especially free expression, association, assembly, and privacy.
9. Cybersecurity-related laws, policies and practices should not impede technological developments that contribute to the protection of human rights.
10. Cybersecurity-related laws, policies, and practices at national, regional and international levels should be developed through open, inclusive, and transparent approaches that involve all stakeholders.
11. Stakeholders should promote education, digital literacy, and technical and legal training as a means to improving cybersecurity and the realization of human rights.
12. Human rights respecting cybersecurity best practices should be shared and promoted among all stakeholders
13. Cybersecurity capacity building has an important role in enhancing the security of persons both online and offline; such efforts should promote human rights respecting approaches to cybersecurity.

Explanatory note

Concerns related to specific practices - including surveillance and content control - are addressed in these recommendations in two ways. First, to the extent that cybersecurity is used to advance other *unrelated* objectives such as censorship or surveillance activities, Recommendation 5 specifically highlights that cybersecurity-related laws, policies and practices should not be used as a pretext to violate human rights. Moreover, with regard to content control and surveillance activities *relating* to cybersecurity, Recommendations 1 and 2 highlight that cybersecurity laws, policies, practices, and decision-making processes should protect and respect human rights.

ANNEX - **Existing frameworks, recommendations and commitments**

Cybersecurity and cybercrime challenges are increasing in frequency and complexity and there is a need for all stakeholders to work together to address these in a manner that preserves human rights, particularly privacy and free expression. The call for cybersecurity policies to be developed in a more open and inclusive manner with greater protections for human rights has been growing and now requires action, especially of the FOC member community. The Working Group members believe that these recommendations build on existing frameworks, statements and commitments, as outlined below, and offer guidance for their realization.

On the need for cybersecurity policies and practices to be consistent with human rights and the rule of law

The Human Rights Council (HRC) has addressed human rights issues online in its Resolutions on The Promotion, Protection and Enjoyment of Human Rights on the Internet. In 2012, the HRC affirmed "that the same rights that people have offline must also be protected online, in particular freedom of expression".[3] In 2014, the HRC importantly outlined how governments should respond to cybersecurity threats, calling on States to "address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of freedom of expression, freedom of association, privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the Internet."[4]

The UNGA Resolution on The Right to Privacy in the Digital Age notes similarly, that "the same rights that people have offline must also be protected online, including the right to privacy".[5] The UNGA Report A/68/98 also established that international humanitarian law applies online as offline, stating that "efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments." The same Resolution also calls on States to "encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs."

The London Process Seoul Framework document also noted that it "is important to maintain an open environment that supports the free flow of information, research, innovation, entrepreneurship and business transformation, to ensure the protection of personal information in the online environment and to empower consumers and users in online transactions and exchanges." The Chair's statement from the (London Process) GCCS meeting in The Hague also urged stakeholders "to ensure that cyber security policies are, from their inception, rights-respecting and consistent with international law and international human rights instruments."

The Freedom Online Coalition members at the annual meeting in Tallinn in 2014 committed, in their own activities, "to respect our human rights obligations, as well as the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight, and transparency" and well as to "promote transparency and independent, effective domestic oversight related to electronic surveillance, use of content take-down notices, limitations or restrictions on online content or user access and other similar measures."[6]

On the need for the engagement of all stakeholders

The Working Group notes that calls for the engagement of stakeholders in cybersecurity matters are growing. UNGA resolution 57/239 on the *Creation of global culture of cybersecurity* and in particular the Annex on *Elements for creating a global culture of cybersecurity****[7]*** notes the importance of stakeholders working together. The 2013 report of the UN Governmental Group of Experts by the

Group of Governmental Experts in Developments in the Field of Information and Telecommunications in the Context of International Security A/68/98 suggests that effective responses to cyber security challenges "would benefit from the appropriate participation of the private sector and civil society."[8]

The London Process (meetings in 2011 in London, 2012 in Budapest, 2013 in Seoul and 2015 in The Hague) has also highlighted the need for multistakeholder engagement and cooperative approaches to cybersecurity challenges. The Seoul Framework states that it is "necessary to continue to work together towards ensuring a trusted, secure and sustainable environment in partnership with multiple stakeholders, including international organizations and the private sector."[9] The Chair's statement at the 2015 GCCS meeting in The Hague urged governments "to ensure that cyber policy at national, regional and international level is developed through multistakeholder approaches, including civil society, the technical community, businesses and governments across the globe."[10] The 2014 NETMundial Multistakeholder Statement[11] noted, inter alia, that "initiatives to improve cybersecurity and address digital security threats should involve appropriate collaboration among governments, private sector, civil society, academia and technical community."

END NOTES

[1] https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/
[2] https://www.freedomonlinecoalition.com/wp-content/uploads/2014/08/FOC-Working-Groups_TOR.pdf
[3] http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/20/L.13&Lang=E
[4] http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/26/L.24
[5] http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167
[6] https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf
[7] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf
[8] http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98
[9] http://www.mofat.go.kr/english/visa/images/res/SeoulFramework.pdf
[10]https://www.gccs2015.com/sites/default/files/documents/Chairs%20Statement%20GCCS2015%20-%2017%20April.pdf
[11] http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

21 September 2015