Sections of the text that you support being included in the final outcome document

Access (https://www.accessnow.org/) defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

Throughout the document we cite the paragraph number (e.g., ¶ 4) to indicate proposed changes, retention, or deletion of text. All text noted below in the following paragraphs in Question 1 should certainly be included.

(¶¶ 4, 36-43) – Access commends the strong recognition in the draft outcome document of the need to protect fundamental human rights, including freedom of expression and the right to privacy, online as well as offline (¶ 4). We recommend that all paragraphs reinforcing the importance of human rights (¶¶ 4, 36-43) should be included in the final outcome document.

(¶ 11) – Access also approves the recognition of the 'privacy by design' and the economic and security impacts of such an approach. Privacy should be designed into all layers of the technology stack and all elements of the ecosystem — and by doing so, protecting the users and the systems they depend upon.

(¶ 35) – In particular, Access supports the acknowledgement that human rights and security are complementary to each other. The right to privacy is a primary driver for increased security, and a user-centric approach to cybersecurity would protect users' human rights, while recognizing that the protection of critical infrastructure is one element of a larger security model.

(¶¶ 36, 37) – As the text notes, the right to privacy is integral to the realization of other human rights, including freedoms of expression, opinion, and assembly and the International Covenant on Civil and Political Rights (ICCPR) provides the robust framework.

(¶ 39) – Additionally, in furtherance of the recognition of the importance of a free and open internet, Access commends the welcoming of the newly-established UN Special Rapporteur on the right to privacy.

Areas of the text which could be strengthened

Overall, the statement should begin with a clear definition of the problem sought to be addressed. The statement should also emphasize the need to transparently establish goals for cybersecurity, to protect user's human rights and avoid any overheated rhetoric ripe for abuse or fraught with vague and overbroad application.

(¶ 6) – Access will provide additional feedback on the Global Forum on Cyber Expertise (GFCE) once details of the organization are revealed. We would like to see further information regarding the GFCE and be assured that any Forum includes adequate representation of civil society from all regions of the world.

(¶ 14, 17) – Governments, as well as consumers and supplies, play a critical role in improving the security of online products and services. The statement does not generally provide sufficient focus on the role of governments, in ensuring a free, open, and secure cyberspace. Instead, at times it pushes responsibilities to non-state actors, hackers, and to some extent, the corporate sector. It is Access' experience that governments frequently use national security to justify a number of detrimental practices, from surveillance to politically-motivated network disruptions or shutdowns, and weakened security standards (*See, e.g., a recent example in the Democratic Republic of Congo* http://www.pcworld.com/article/2877392/congo-restores-internet-to-banks-govt-agencies-but-public-block-remains.html).

The statement should indicate in (¶¶ 14, 17 at minimum) the importance of governments refraining from acting to undermine the security of communications technology. Governments should never undermine encryption standards or mandate lesser encryption protocols to facilitate surveillance capabilities. These "back doors" put all users at risk and make it easier for criminals and other bad actors to gain access to sensitive user data.

(¶ 19) – The statement rightly considers the need for more mature Computer Security Incident Response Teams (CSIRTs), however, the language should also specify that such organizations have a heightened responsibility to protect the privacy of the users dependent on CSIRTs assistance.

(¶ 20) – The statement should embrace a move toward a user-centric approach to cybersecurity. Namely, it should clarify that cybersecurity is about protecting the entire security ecosystem, starting at the user, and not only about critical infrastructure or national security. Laws and practices should not be antithetical to meaningful data security (*See* https://www.accessnow.org/blog/2014/12/08/the-dangers-of-a-militarized-internet). All users are entitled to due process and protections under the rule of law before personal data is accessed. The statement should recognize that a user has rights in his or her data and a level of control over its storage, use, and deletion.

(¶¶ 22-23) – States should consider means of increasing mutual assistance, but should do so in such a way as to protect the rights of individuals whose information may be transferred. For instance, states should abide by clear processes for the exchange of information and should respect protections developed by other states as many mutual legal assistance treaties (MLATs) require. Similarly, (¶32(d)-(e)) should emphasize the need for formal channels that operate openly and transparently to facilitate cooperation across governments. Governments should never be able to use one another to conduct end-runs around limitations in their own laws.

(¶¶ 23, 35, 37) – There are a number of places where the statement would be complemented by references to the International Principles on the Application of Human Rights to Communications Surveillance (Necessary and Proportionate Principles -

https://en.necessaryandproportionate.org), which have been signed by over 400 civil society organizations.

The Necessary and Proportionate Principles provide a framework for safeguarding human rights in the exchange of information across borders (¶ 23). The statement should also cite to the Principles in discussing the need to confront legitimate threats (¶ 35) to ensure users are protected against the potential of government overreach in its security efforts, endangering privacy or actually worsening security. While the statement's inclusion of the ICCPR (¶ 37) is commendable, civil society and human rights scholars developed the Principles to specifically articulate the application of ICCPR and other relevant sources of human rights law to communications technology.

(¶ 25) – The text of the statement should clarify that governments must not only assist in the development of norms of good behavior but they must act on those norms in good faith. International norm development should not be a means of advancing individual state goals or undermining collective security. The creation of "new" norms should not undermine the application of human rights or other existing laws and regulations.

(¶ 50) – In the same way that the introduction includes a paragraph on the primacy of human rights, the closing of the document should also include a paragraph if not a reference to human rights. For instance, paragraph 50 could be amended so the second paragraph reads, "We are all affected by ICTs on a daily basis and we increasingly utilize ICTs to exercise our fundamental human rights. Those rights should be protected unequivocally, both online as they are offline."

Areas of the text that raise concerns

(¶ 17) – The statement emphasizes State sovereignty, however self-determination cannot be used as a guise to enact programs that fragment the internet, such as data localization laws now at risk of enactment and implementation in countries (*See* https://www.accessnow.org/blog/2014/06/04/the-impact-of-forced-data-localisation-on-fundamental-rights)

(¶ 21) – Cooperation between government agencies and the private sector is critical. However, there should not be laws granting government agents expansive powers to control the internet or to require the private sector to take burdensome actions in attempting to counter crimes committed online. Cooperation between government and the private sector should neither be used to enable surveillance nor bypass user protections. The text should be modified to specify that information shared between the private sector and government must be narrow enough in scope to protect the right to privacy of those whose information is shared.

While not clear in the text (¶ 21), crimes should not incur additional penalties merely because they were committed using a computer. Yet this continues to be the paradigmatic method for states to "update" their existing criminal laws for the digital realm. Additionally, the statement

should emphasize that all legislation should be technology neutral in order to prevent laws from needing to be frequently updated as technology changes.

Areas of the text where there are inconsistencies or that lack clarity

(¶¶ 21-22) – This is inconsistent with statement (4), which highlights the need to protect fundamental rights online as they are protected offline. Unique considerations of criminal activity on the internet may warrant discussion. However, governments and corporations should use established mechanisms with recognized human rights protections for investigating crimes committed online rather than creating new or enhanced authorities that will have a disproportionate impact on online users.

For further information on this question or any of those above, please contact Amie Stepanovich, amie@accessnow.org or Drew Mitnick drew@accessnow.org.