**Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries (2014/2232(INI))**

## Introduction

Thank you for circulating this report and inviting comments from a wide group of stakeholders – and now we bid you good luck in sorting through everyone's comments! Here are a few general comments on the report, following the structure of the draft.

Firstly, Access is a global organisation dedicated to defending and extending the digital rights of users at risk around the world. Access provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. Access wields an action-focused global community of nearly half a million users from more than 185 countries, and also operates a 24/7 digital security helpline that provides real-time direct technical assistance to users around the world. Access is non-partisan and not affiliated with any country, corporation, or religion.

As Rapporteur for the AFET report on Human rights and technology, we welcome your work underlining many fundamental points that should be addressed in the EU relations with third countries regarding technology and human rights, and we hope that, eventually, the resulting report will reflect these preliminary considerations.

In particular, we would like to acknowledge that the following are crucial points that we are pleased you addressed in this report:

- the inclusion of conditionality clauses referring to online rights in all agreements (point 7.);
- the admissibility as evidence in court proceedings of digital material (point 9.);
- the exclusion of companies providing potentially harmful ICTs products and services (point 19.).

## Private actors and applicable norms

*E. “whereas in the digital domain, private actors play an increasingly significant role;”*

It could be useful to mention more precisely both the situations where private actors play such a significant role, and the nature of these private actors themselves. For instance, firms which export technology to third countries, or private contractors performing critical activities in the domain of surveillance and/or (cyber-)security outside the EU. As you pointed out rightly during the last DROI meeting, overcoming the difficulties raised by dual-use technology can often be done by assessing appropriately the context and the actors involved.

In relation to this, it could also be useful to stress the need to clarify the norms applicable to these private actors, in adding a point on this particular issue. It could be valuable to underline, in particular, that while these actors are becoming more important, safeguards providing clear dispositions on their role and responsibilities are still lacking.

**Nature and role of technologies**

3. “*Stresses that the role of technologies should be mainstreamed in all EU policies and programmes to advance human rights protection;”*

This point could be improved in detailing more clearly which kind of technologies and what role should be mainstreamed by EU policies. This could be developed by modifying the sentence as follows:

*“Stresses that **the impact of technologies on human rights** should be mainstreamed in all EU policies and programmes to advance human rights protection;”*

**Complementarity between technical and policy instruments**

*4. “Calls for the active development and dissemination of technologies that help protect human rights and facilitate people´s digital freedoms and security;”*

While we understand that this report is focused on the impact of technological advances on human rights, it nevertheless remains important in this context to consider the complementarity between technical and policy instruments in the fight against human right abuses. For this reason, we suggest to modify this point as follows:

*“Calls for the active development and dissemination of technologies that help protect human rights and facilitate people´s digital freedoms and security, **along with promoting best practices and an appropriate legislative frameworks**;”*

**Conceptual differences and implications**

*16. "Calls on the Commission to submit proposals to review how EU standards on ICTs could be used to prevent the potentially harmful impacts of the export of such technologies or other services to third countries where concepts such as 'lawful interception' have different implications, or where the rule of law does not exist;"*

We suggesting adding the following to point 16: "Furthermore, we reaffirm that EU standards, particularly the EU Charter of Fundamental Rights, should prevail when assessing incidents where dual-use technologies are employed in a way that may restrict human rights"

**Involvement of European companies**

*18. "Deplores the active involvement of certain European companies and international companies operating in the EU and in countries violating human rights;"*

To further clarify this point, it could be instructive to explicitly state in which capacity certain European companies are presumed actively involved. For instance by adding :

*"Deplores the active involvement of certain European companies and international companies**, which trade dual-use technologies with potential detrimental effects of human rights,** operating in the EU and in countries violating human rights;"*

**Net neutrality**

*20. "Calls on the Commission and Council to actively defend the open internet, multi-stakeholder decision making procedures, and digital freedoms in internet governance fora;"*

Here, an explicit reference to net neutrality would be a strong message, as it can insure the openness and safeness of the internet. For this reason, we suggest adding to this sentence *"[…] the open **and neutral** internet"*, or alternatively

*"Calls on the Commission and Council to actively defend the open internet, multi-stakeholder decision making procedures, **net neutrality**, and digital freedoms in internet governance fora;"*

In addition with this, the term "*multi-stakeholder*" may not reflect appropriately the variety of actors that should be included nor the process in which such inclusive decision making can take place, and can be subject to undesirable interpretations. For this reason, we suggest to define the term with the following: "By multi-stakeholder decision making we mean a process ensuring meaningful, inclusive and accountable participation of all stakeholders, governments, civil society, technical and academic communities, private sector, and users".

**Additional points**

It should be stressed that in order to *"support, train and empower human rights"* (as described in 5.), the European Parliament should establish a dedicated budget.

In accordance with the calls for active development of technologies to help protect human rights (as stated in 3. and 4.), it seems essential to explicitly call for promoting tools enabling the anonymous and/or pseudonymous use of the internet. This seems especially critical with regards to the fact that such tools are easily considered, by default, as allowing criminal activities, rather than empowering human rights activists beyond and within the EU (Cf. the interpretation made recently by a Spanish judge that using secure communication technologies, in that case RiseUp email, is inherently suspicious) [1]. Additionally, an explicit call for promoting the use of open source software (notably by public institutions) should be added.

Importantly, there is strong evidence demonstrating that not only private companies, but also EU member states' government services are using tools in a way that contradict the spirit of EU human rights (for instance, the recent disclosures on GCHQ's hacking into Gemalto servers). For this reason, we suggest to add a point calling on the Parliament to remind member states that their actions must reflect their commitment to EU fundamental rights, as otherwise there is a real risk to deeply undermine the trust between them, which would undoubtedly be catastrophic for inter EU cooperation.

On a more general note, we suggest addressing the point that regulation of technologies at the EU level should not be framed or discussed in opposing individual and/or civil liberties to national security prerogatives, but rather, in the perspective that, in your own words, *"digital security and digital freedom are [both] essential and […] should reinforce one another"*.

*For more information, please contact*
*Raegan MacDonald, European Policy Manager at raegan@accessnow.org.*

---

[1] https://www.eff.org/deeplinks/2015/01/security-not-crime-unless-youre-anarchist