AMNESTY INTERNATIONAL

Amnesty International Comments on the European Commission Dual-Use Export Proposal

(April 2017)

Introduction

The threat of surveillance

Digital surveillance poses a grave threat to the ability of human rights groups, journalists, lawyers, and activists of all types to do their work.

This threat may take the form of unlawful mass surveillance programs, or attempts to subject people to unlawful targeted surveillance, such as surveillance undertaken because of the protected exercise of their human rights. This unlawful surveillance not only violates the right to privacy and chills expression and peaceful assembly, but can lead to arbitrary arrest, torture or even death.

In many contexts, the technology and tools that facilitate this unlawful surveillance are sold by foreign companies, including those within the EU. The Hacking Team scandal of 2015 – wherein invasive monitoring software sold by an Italian firm was revealed to have apparently been sold to governments such as Saudi Arabia, Uzbekistan, Ethiopia and other governments with poor human rights records – demonstrates the potentially vast harm to human rights that could result from this trade if it is not properly regulated to ensure that companies and states comply with international human rights law and standards.

The Respective Human Rights Obligations of States and Companies

Nation states have binding obligations under international human rights law to protect human rights from abuse by third parties. This includes the obligation to regulate the conduct of non-state actors who are under their control in order to prevent them from causing or contributing to human rights, even if they occur in other countries.

As laid out in the UN Guiding Principles on Business and Human Rights (UNGPs), companies also have a responsibility to respect human rights wherever they operate in the world. The UNGPs require that companies take pro-active steps to ensure that they do not cause or contribute to human rights abuses within their global operations, and to respond to any human rights abuses when they do occur. In order to meet that responsibility, companies must carry out human rights due diligence to "identify, prevent, mitigate and account for how they address

their human rights impacts." The corporate responsibility to respect human rights exists independently of a state's ability or willingness to fulfil its own human rights obligations and over and above compliance with national laws and regulations protecting human rights. For example, the interpretative guidance on the UNGPs specifically notes that a company may contribute to a human rights violation if it provides "data about Internet service users to a Government that uses the data to trace and prosecute political dissidents contrary to human rights".[1]

Moreover, it is possible that a company that sells surveillance equipment could be complicit in any subsequent violation of human rights in which the equipment is used. An International Commission of Jurists (ICJ) Panel of Experts has examined the question of corporate complicity in human rights violations in some depth and clarified how legal liability, both civil and criminal, could arise for such complicity. The ICJ panel considered that there could be a sufficiently close link in law if the company's conduct enabled, exacerbated or facilitated the abuse, and the company knew, or ought reasonably to have known, that the abuse would occur. A company could enable, exacerbate or facilitate abuse through, among other things, the provision of goods or services.

Updating the Regulation

The EU regulates the trade in dual-use items – goods, software and technology that can be used for both civilian and military applications – through Regulation (EC) No. 428/3009. Under this regulation, exports of dual-use items listed in the regulation's annexes must be authorized. Additionally, states may impose additional requirements for authorization on dual-use items that are not listed, subject to the regulation's catch-all clause.

At present, the dual-use list includes some surveillance items, including items related to IP-monitoring or intrusion software, as well as mobile phone interception and jamming equipment, such as IMSI catchers.

Following a lengthy review of the existing regulation, the European Commission produced an impact assessment report, and has now introduced a new proposal (hereinafter "the proposal") to update the existing regulation and dual-use list.

The proposal contains several innovations, which will be discussed below – some positive, some that are cause for concern. As the proposal is reviewed by the

[1] United Nations Office of the High Commissioner for Human Rights, "The Corporate Responsibility to Respect Human Rights: An Interpretive Guide," p. 17, available at: http://www.ohchr.org/Documents/Publications/HR.PUB.12.2_En.pdf

Council and the Parliament, it will be important for civil society to make its voice heard to ensure the proposal becomes a regulation capable of helping enforce the existing human rights obligations of states and responsibilities of companies involved in the surveillance trade.

- **What is Positive?**
    - The proposal extends the definition of dual-use items, adding surveillance technology that can be used for committing serious human rights violations
    - The proposal explicitly requires the consideration of human rights when authorising an export license
    - There is a new cyber surveillance clause in the dual-use list, adding additional surveillance technology
- **What is of concern?**
    - The requirements that states and companies consider human rights do not go far enough
    - The proposal must require that companies and states scrutinize all surveillance exports for risks to human rights
    - More transparency is needed
    - Greater protection is needed for legitimate security research

Specific Concerns

1. Content of Human Rights Considerations

What is the concern?

The inclusion of human rights in the definition of dual use and as a criterion in assessment of export authorizations in the proposal is very welcome. Many questions remain, however, as to how this will be given effect.

As written, the references to human rights in the proposal are vague. It is not clear how the human rights implications of dual-use exports should be analysed and it is not clear in which situations a human rights risk would be considered severe enough that an export license should be denied. The proposal should be strengthened to indicate:

1. The scope of what is considered "dual use" when it comes to human rights violations,
2. The scope of human rights considerations that must be considered, and
3. When human rights concerns oblige states to deny export licenses

What sections of the proposal are implicated?

Article 2(1)(b) expands the definition of dual-use items to include surveillance technology "which can be used for the commission of serious violations of human rights or international humanitarian law." **Article 4(1)(d)** creates the possibility for states to impose authorisation requirements on non-listed dual-use items that may be intended, in whole or in part "for use by persons complicit in or responsible for directing or committing serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression in the country of final destination, as identified by relevant public international institutions, or European or national competent authorities, and where there is evidence of the use of this or similar items for directing or implementing such serious violations by the proposed end-user."

However, this deals only with human rights abuses that are "serious", by specific end-users, and in situations of armed conflict or internal repression. Additionally, the imposition of an authorization requirement on these grounds is optional.

The limitation to "serious" human rights violations is potentially problematic in the surveillance context if it is interpreted to limit consideration to a small set of human rights (such as torture or slavery) that are considered serious in nature. The proposal must make clear that "serious" will be interpreted to relate rather to the scale or pervasiveness of violations, including those most commonly violated

by unlawful surveillance, such as privacy, expression and association.

Similarly, restrictions on the interpretation of human rights in Article 4(1)(d) that limit this consideration to specific end users with documented histories of past human rights violations, or to specific situations should be removed. Human rights can be violated by unlawful surveillance outside the context of armed conflict or officially recognized situations if internal repression.

Article 14(1)(b) requires only that the competent authorities in Member States – when considering authorizations –"take into account… respect for human rights in the country of final destination as well as respect by that country of international humanitarian law," while **Article 14(1)(c)** mandates consideration of the internal situation in that country, such as the existence of armed conflict.

This is problematic because Article 14 neither specifies how human rights must be taken into account in licensing decisions, nor mandates a denial of licenses in cases where the consideration of the above criteria reveal human rights concerns.

This omission threatens to undermine the purpose of human rights protections since it theoretically allows for licenses to be granted even if exports are found to pose a serious risk to human rights.

The proposal does not specify how these criteria will be applied. Instead, it states, in **Paragraph 5 of the recital** that the Commission and the Council will, at a later date, make available guidance and/or recommendations on implementation.

Recommendations

The content of the human rights provisions in the proposal relating to what technology is considered dual-use, which dual-use items require licensing and in which situations licenses should be granted or denied, should be strengthened.

In doing this, the proposal should draw on international and regional human rights standards, as well as relevant jurisprudence of the CJEU and ECtHR, such as *Zakharov v. Russia*, which have developed numerous tests specific to the potential human rights harms of surveillance technology. The EU should ensure that the same human rights standards apply abroad as do inside the EU.

- Limitations to "serious" human rights violations in articles 2 and 4 should be either removed, or specifically defined to encompass those human rights (such as privacy, expression and association) which are most commonly violated by unlawful surveillance, in manners described in relevant international and regional law and standards, such judgments of the European Court of Human Rights.

- Limitations in article 4 related to the proposed end user of exports, or to specific situations of armed conflict or internal repression should be removed. Authorizations should be required for exports as soon as states or companies are aware of a substantial risk the items could cause or facilitate human rights violations.

The proposal must also *require a denial* of authorization where:

- There is a substantial risk the items transferred could be used to violate human rights.
    - As specifically pertains to surveillance technology, the proposal should make clear that licenses must be denied where exports could violate the right to privacy through the arbitrary interception of communications, or to use unlawful surveillance for serious human rights violations such as to unlawfully restrict freedom of expression, to repress political dissidents or target individuals for arbitrary arrest, torture or execution, or
    - The legal framework or technical arrangements in the destination country fails to provide adequate safeguards against serious human rights abuse. This should include legal safeguards as defined by international and European law and standards (including, for example, whether authorities have direct access to communications or associated data, whether surveillance requires an individualized warrant based on reasonable suspicion of wrongdoing, and whether surveillance is overseen by an independent judicial authority);
- An exporting company has failed to provide proof that a robust human rights risk assessment has been carried out, including the need for any mitigating measures as relates to any of the above risks.

2. Companies and States Must Scrutinize All Exports of Surveillance Technology for Human Rights Risks

What is the concern?

The proposal explicitly includes some new categories of surveillance technology in the dual-use list, making these technologies automatically subject to a licensing requirement. The list thus now includes: equipment for mobile phone interception or jamming, certain types of internet monitoring software, "intrusion software," and newly-added items such as monitoring centres and retention systems.

Some of the included items may be problematic. For instance, the dual-use list applies to some encryption technology. Some security researchers have voiced concerns that language around "intrusion software" in the dual-use list could apply to tools for their work, though language in the preamble specifies that this should not be the case (see Section 4, below).

Because technology evolves quickly, it is not possible to include all surveillance technologies in the list. The proposal includes "catch-all" provisions which may be used to subject other types of technology exports to authorization requirements, even if they are not specifically listed as dual-use items.

As written, the catch-all provisions appear weak and easily circumvented. They should be redrafted to make clear the human rights obligations of states and the responsibilities of exporting companies.

What sections of the proposal are implicated?

Under **Article 8(1)**, a state may – but is not required to – prohibit the export or impose authorization requirements for the export of technologies not listed in the list of dual-use items, for reasons including "human rights considerations" – which are not defined. **Article 4(1)** and **4(1)(d)** state that licenses are required for non-listed items where an exporter has been informed by the state authority that the items in question "are or maybe intended, in their entirety or in part…for use by persons complicit in or responsible for directing or committing serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression."

The obligation on states, therefore, to assess the human rights risks of non-listed exports, as currently determined by Art. 8(1) and 4(1), is problematic because:

1. It is discretionary,
2. The human rights clause in article 4(1)(d) contains unduly restrictive limitations (see section 1, above)

Under **Article 4(2)**, an exporter who, under their "obligation to exercise due diligence," becomes aware that, *inter alia,* a dual-use item intended for export is intended for an illegitimate use, as listed in Art. 4 I, must notify authorities of the intention, who will, in turn, "decide whether or not it is expedient to make the export concerned subject to authorisation."[2]

This is problematic because:

1. It does not specify the content of the "due diligence" duty to which it refers, or make clear that companies have existing duties under international human rights law and standards that include, *inter alia*, the obligation to conduct human rights due diligence, including by conducting risk assessment, considering measures to mitigate identified risks, and in case of harms, to provide remediation, and
2. There is no obligation on state authorities – as part of their decision on whether to require licensing of an export or whether to approve or deny a license - to verify the adequacy of risk assessments or other human rights due diligence measures undertaken by corporate actors

Recommendations

The proposal should be strengthened through an explicit reference to the pre-existing international human rights responsibilities of exporting companies to carry out human rights due diligence, including through identifying, preventing, mitigating and accounting for any human rights risks associated with their exports, whether intentional or otherwise.

The proposal should also clarify states' obligations to ensure that all relevant exports are scrutinized to ensure that they do not contribute to serious human rights abuses, whether intentional or otherwise. As part of their legal obligation to protect human rights, states should offer guidance to companies on how to respect human rights in their operations.

The proposal should be strengthened to ensure that it provides an effective catch-all by which these human rights principles can be meaningfully realized in practice.

This could be accomplished by, for example:

- Specifying steps required from exporters when undertaking human rights due diligence, and requiring exporters to submit to state authorities their

[2] Article 4.2

human rights risk assessments, and any envisioned measures for prevention or mitigation of human rights risks.

- Requiring states to verify the adequacy of human rights risks assessments carried out by companies, and to independently conduct an assessment of the risk that specific potential transfers of non-listed items could be used for serious human rights violations.
- Requiring that the above assessments by states and companies be made public.
- Explicitly clarifying that "due diligence" means the process by which businesses may meet their responsibility to respect human rights, as laid out in the UN Guiding Principles on Business and Human Rights, by identifying, preventing, mitigating and accounting for human rights impacts of their operations (and business relationships).

3. Transparency Lacking

What is the concern?

The lack of transparency regarding which companies are granted export licenses, for which products and which end users and end use, as well as about how decisions to grant or deny authorizations are made, are a key impediment to avoiding serious human rights abuses linked to dual-use exports. The proposal does not go far enough in demanding transparency around these issues.

What sections of the proposal are implicated?

Article 8 requires states to notify the Commission if they impose authorisation requirements on non-listed dual-use items and requires the Commission to publish these notices in the *Official Journal of the European Union*.

Article 29 proposes the publications of a public annual report by the Commission, to be submitted to the Parliament. However, neither of these appear to include detailed information about specific exports.

Recommendations

- The proposal should be amended to require that member states publicly disclose, in a timely and easily-accessible manner, meaningful information on the volume, value, nature of equipment, and destination of their trade in dual-use items, as well as information regarding approved or denied exports, so as to enable appropriate oversight by elected representatives, independent bodies and the public.
- Human rights risk assessments undertaken by states and companies regarding authorized or denied export licenses should also be made publicly available.
- These documents should be required to be readily accessible to the public, such as by posting on the website of the national export license authority, or a dedicated EU-level website.

4. Greater Protection is Needed for Legitimate Security Research

What is the concern?

The proposal states, in **Recital 5** of the preamble, that export controls should "not prevent the export of information and communication technology used for legitimate purposes, including law enforcement and internet security research." However, there may be a need for stronger operative language, or changes to definitions to ensure against unwarranted interferences or chilling effects on security research, which supports the human rights of internet users through the discovery, disclosure and patching of vulnerabilities. Such research often relies upon the sharing of data across borders.

What sections of the proposal are implicated?

Article 2(1)(21)(b) includes "intrusion software" in the definition of "cyber-surveillance technology." Further definitions are provided in the **Annex**.

Recommendations

The proposal should further clarify that definitions of terms such as "intrusion software," "technical assistance" and "intangible technology transfers" shall not be construed to cover uses such as private exploitation research, and legitimate security items such as anti-virus products, fuzzers, defensive pentesting, exploit generation software and jailbreak software. Alternately, definitions of these terms should be amended to prevent these sorts of overbreadth.

Useful References

- Case of Roman Zakharov v. Russia, European Court of Human Rights (Grand Chamber), Application No. 47143/06 (2015)

- Case of Szabó and Vissy v. Hungary, European Court of Human Rights, Application 37138/14 (2016)

- United Nations Guiding Principles on Business and Human Rights

- United Nations Human Rights Council Resolution on the Right to Privacy in the Digital Age (adopted March 23, 2017)

- United Nations High Commissioner for Human Rights, Report on the Right to Privacy in the Digital Age (30 June 2014)

- Report of the Special Rapporteur on the Right to Privacy, A/HRC/34/60, 24 February 2017

- Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/34/61, 21 February 2017 and A/69/397, 23 September 2014

- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38 (11 May 2016) and A/HRC/23/40 (17 April 2013)

Amnesty International Publications on Surveillance and Human Rights

- "We Will Find You, Anywhere": The Global Shadow of Uzbekistani Surveillance (March 31, 2017)

- False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan (March 10, 2017)

- "It's Enough for People to Feel it Exists": Civil Society, Secrecy and Surveillance in Belarus (7 July 2016)

- Dangerous to Dissent: Human Rights Defenders Under Threat in Gambia (2 June 2016), pp. 37-39.