URGENT CALL TO THE COUNCIL OF THE EU: HUMAN RIGHTS MUST COME FIRST IN DUAL USE FINAL DRAFT

November 2020

---

accessnow

AMNESTY INTERNATIONAL

HUMAN RIGHTS WATCH

RSF REPORTERS WITHOUT BORDERS

fidh

Brot für die Welt

Christina Decker
Director of Foreign Trade and Payments Controls/Law
German Ministry for Economic Affairs and Energy
christina.decker@bmwi.bund.de

Adrian Toschev
Chair of the Working Party on Dual Use Goods
German Ministry for Economic Affairs and Energy
adrian.toschev@bmwi.bund.de

Re: Urgent call to the Council of the EU: human rights must come first in Dual Use final draft

Dear Ms. Decker and Mr. Toschev,

We, the undersigned organisations, write to ask you to reconsider the final draft of the EU dual use recast as it currently fails to meet basic human rights standards. More work must be done in trilogue to protect human rights in Europe's export regulation framework.

Since our first call for export regulation reform almost 10 years ago, the market of digital surveillance technology has grown exponentially and unconstrained. In addition to the widely-acknowledged intrusion and interception spyware tools that are being weaponized by repressive regimes, we have observed the use of intrusive biometric and filtering technologies in unlawful surveillance and repression. These technologies have enabled violations of the rights to privacy, non-discrimination, peaceful assembly and association, freedom of expression, and more. A large number of these technologies originate from the European Union, making it all the more pressing that the EU fulfills its human rights duties by regulating the export of such items. The common commercial policy must be conducted in the context of the principles and objectives of the Union's external action (Art. 207 TFEU) which include the respect and promotion of human rights (Art. 21 TEU).

Despite our continuous and loud calls for the EU to act to regulate the cyber-surveillance industry and install human rights safeguards for the export of digital surveillance items that pose significant risks to human rights, the EU has yet to take any meaningful action to address this. We find it alarming that the latest proposal discussed in trilogue falls short of human rights safeguards in the following ways:

1. NEUTRAL DEFINITION OF CYBER SURVEILLANCE TECHNOLOGY

OUR RECOMMENDATION	RELEVANT DRAFT PROVISIONS	DID IT MEET OUR RECOMMENDATION?	COMMENTS
Items should include hardware, software, and services.	2(1) & 2(21) & Annex "Technology" N.B. 1	YES 	The text includes hardware, software, and services.
Definition and scope should encompass all human rights violations, and not be limited to serious violations.	2(21) & 4a(1)	NO 	All provisions on cyber-surveillance only apply to "serious human rights violations."
Any information systems linked to human rights risks should be included and not only technology that uses a specific collection method, such as deep packet inspection or intrusion.	2(21) & 4a(1)	NO 	Definition only covers systems "specially designed" for surveillance by monitoring, extracting, collecting, or analysing data from information and telecommunication systems. Data extraction with generally designed systems with similar results falls outside the scope.
"Covert" and "non-covert" surveillance should be included.	2(21) & 4a(1)	NO 	Only covert surveillance is included.

2. EU CONTROL LIST

OUR RECOMMENDATION	RELEVANT DRAFT PROVISIONS	DID IT MEET OUR RECOMMENDATION?	COMMENTS
There should be a strong autonomous list procedure.	4a(4)-(7)	NO 	There is a weak and ineffective procedure for an autonomous list in the text in the form of a "soft law" procedure.
Besides Member States, EU institutions should be able to start the process of nomination based on intelligence from various sources.	4a(4)	NO 	Only Member States can initiate the procedure, EU institutions cannot.
Companies should have no influence on the start and outcome of the procedure.	4a(3) & 21(3)	NO 	Companies are the gatekeepers to start the "soft law" procedure; an exporter must have grounds to suspect that items are or may be intended for serious human rights violations. This makes the inclusion of the company a prerequisite for this process. Industry also influences the outcome of the procedure as they are a privileged group for consultation by the Commission.
The procedure should be fast and effective.	4a(6-7)	NO 	A marginal group of Member States can block the procedure because it requires unanimity.
Biometric surveillance technology should be added to the EU control list.	Recital 5a	PARTIALLY 	Biometrics are directly regulated in the text and could be added to the soft law autonomous list. However, this is unlikely due to the companies being the gatekeepers and the unanimity requirement.

3. EMERGENCY BRAKE PROCEDURE/CATCH-ALL CLAUSE

OUR RECOMMENDATION	RELEVANT DRAFT PROVISIONS	DID IT MEET OUR RECOMMENDATION?	COMMENTS
Member states must be able to hit the emergency brake for exports of non-listed cyber surveillance items with significant human rights risks.	4a(1)	PARTIALLY	Member States can only hit the emergency brake in relation to serious human rights violations, not when there is a significant risk of human rights violations.
Licensing authorities should be able to use various sources of information in this process, including information from civil society groups.	4a(1)	NO	It is unclear what sources will be accepted and what the burden of proof is.
Companies must notify the authorities when there is significant human rights risk for export of a non-listed item. Licensing authorities can stop this export.	4a(2)	PARTIALLY	Companies must only notify in relation to serious human rights violations. The licensing authority can stop that export.
Licensing authorities should exchange information about exports with each other.	4a(4)	PARTIALLY	Member States must share information on emergency brake procedures by default, but a Member State can also decide to withhold information.
Member States should ensure harmonization of the emergency brake procedure across the EU.	22	PARTIALLY	Member states are encouraged to exchange enforcement practices, but this does not explicitly extend to the emergency brake procedure.

4. HUMAN RIGHTS DUE DILIGENCE

OUR RECOMMENDATION	RELEVANT DRAFT PROVISIONS	DID IT MEET OUR RECOMMENDATION?	COMMENTS
Companies must be obligated to do human rights due diligence.	4(2)	NO	There is no explicit obligation to implement human rights due diligence procedures, even though "due diligence findings" are mentioned in the text.
Companies must actively and continuously seek information to become aware of their human rights impact.	4(2)	NO	The text does not require the company to proactively "become aware" of their human rights impact.
Every company must conduct due diligence, whether they are big or small.	Recital 5 &14(2) &4(2)	PARTIALLY	The text applies to all companies equally. But suggestions for Internal Compliance Procedures are size-dependent.
Companies should, where possible, conduct transparent reporting of performed due diligence.	4(2)	NO	There is no obligation for transparency reporting.
Victims of human rights abuses should have access to judicial remedy, followed by adequate sanctions.	4(2)	NO	There is no provision for access to remedies or redress.

5. HUMAN RIGHTS CONSIDERATION IN THE AUTHORIZATION DECISION

OUR RECOMMENDATION	RELEVANT DRAFT PROVISIONS	DID IT MEET OUR RECOMMENDATION?	COMMENTS
Human rights considerations should be included in all licensing decisions and have a decisive role in the decision process.	14(1)	NO ☹	Human Rights considerations are not explicitly made a criterion in the text and do not apply to all export decisions of cyber-surveillance items.

6. TRANSPARENCY

OUR RECOMMENDATION	RELEVANT DRAFT PROVISIONS	DID IT MEET OUR RECOMMENDATION?	COMMENTS
Licensing authorities should publicly and frequently disclose: exports volume, nature, value, and destination of the intended export of listed digital surveillance items for which an authorisation has been requested, as well as of decisions regarding non-listed items under the catch-all clause.	24(2) & 24(3)	PARTIALLY 😳	Data will not be provided by the licensing authorities directly, but by the European Commission once a year. The data will be aggregated and limited. Member States can refuse to provide data on the basis of multiple and overly broad exceptions.

We call on the Council to urgently reconsider its final position taking into account our recommendations. We acknowledge the significant amount of work that was put in discussing this legislative proposal and we believe that a favorable solution can be reached in trilogue when all negotiating parties work to secure a final text that upholds human rights safeguards.

Thank you for your consideration.

Signatories

Access Now
Amnesty International
Brot für die Welt
FIDH (International Federation For Human rights)
Human Rights Watch
Reporters Without Borders (RSF)