

Human rights organizations call to strengthen the European Commission position on dual-use recast

June 2020



Commissioner Phil Hogan
cab-hogan-contact@ec.europa.eu

RE: Human rights organizations call to strengthen the European Commission position on dual-use recast

Dear Commissioner Hogan,

We write to you today on behalf of the undersigned organisations to call on the European Commission to strengthen its compromise position regarding the EU dual-use recast, and bring them in line with the original Commission proposal from September 2016.¹

The Commission's position should enable the European Union to enact a legislation that "prevent[s] human rights violations associated with certain cyber-surveillance technologies" by adopting appropriate human rights standards, mandatory human rights impact assessment in due diligence processes, a functional mechanism for catch-all and the EU control list, and mandatory transparency and disclosure criteria for export licensing by Member States.²

Following the ongoing stream of evidence that digital surveillance technology continues to be exported from the Union to repressive regimes around the world, we have repeatedly urged the EU institutions and member states to fulfil their human rights obligations by prioritizing the long overdue reforms to the EU export controls regime.^{3,4}

Since our first calls for the export controls reform in 2011, we have observed alarming trends indicating exponential and unconstrained growth in the market of digital surveillance technology. Intrusion and interception spyware tools are weaponized by repressive regimes raising the stakes and dire need for the protection of human rights.⁵ We also observe the

¹ Reported by and published on Politico (May 2020)

<https://www.politico.eu/wp-content/uploads/2020/05/POLITICO-export-controls-EC-non-paper-on-catch-all-cla-use-May-2020.pdf>

² "Commission proposal for improved export controls would modernise and simplify the system to respond to new risks" (28 September 2016) <http://trade.ec.europa.eu/doclib/press/index.cfm?id=1548>

³ "The Global Surveillance Industry" (Privacy International, July 2016),

https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf; Likhita Banerji, "A Dangerous Alliance: Governments Collaborate with Surveillance Companies to Shrink the Space for Human Rights Work" (Amnesty International, 16 August 2019) <https://www.amnesty.org/en/latest/research/2019/08/a-dangerous-alliance-governments-collaborate-with-surveillance-companies-to-shrink-the-space-for-human-rights-work/>.

"140 Characters" (Human Rights Watch, November 2016)

https://features.hrw.org/features/HRW_2016_reports/140_Characters/index.html

⁴ "Open NGO Letter to EU Member States and Institutions Regarding the Export of Surveillance Equipment" (Access Now, July 2017),

<https://www.accessnow.org/cms/assets/uploads/2017/07/NGOlettertoEUmemberstatesonsurveillanceexports.pdf>

"A Critical Opportunity: Bringing Surveillance Technologies Within the EU-Dual Use Regulation" (Coalition Against the Unlawful Use of Surveillance Exports: June 2015)

https://www.privacyinternational.org/sites/default/files/2018-02/CAUSE_8.pdf

⁵ "Ending the targeted digital surveillance of those who defend our rights: A summary of the impact of the digital surveillance industry on human rights defenders" (Amnesty International, December 2019)

<https://www.amnesty.org/download/Documents/ACT3013852019ENGLISH.PDF>

emergence of intrusive biometric surveillance and its increased use for unlawful surveillance and repression. The use of these technologies have enabled violations of the rights to privacy, non-discrimination, peaceful assembly and association, freedom of expression, and more.⁶ This trend must be stopped and a regulatory framework for the export of digital surveillance that poses high risks to human rights is a stepping stone in ensuring accountability and respect for human rights.

In 2016, the European Commission proposed ambitious and necessary reforms to the current system. We are particularly encouraged by the commitment to delist vital security tools and enable the free spread and use of encryption technologies which serve to protect all users at risk, human rights advocates, journalists, and the population at large. We deeply regret that some member states are staunchly opposed to more stringent legislation, putting interests ahead of values. We would urge the Commission to maintain its strong opening position and work with the remaining institutions to ensure that states throughout the European Union prevent surveillance exports that pose risks to human rights.

To that end, we welcome your remarks from 19 May 2020 to the OECD Global Forum on Responsible Business Conduct where you emphasized the need for a strong EU position on due diligence for companies and supply chains; as well as the need for such initiatives to strengthen and support human rights.⁷ We also welcome the proposal for the new Action Plan for Human Rights and Democracy, which will identify the priorities along the line of action for harnessing opportunities and addressing challenges of new technologies.⁸ In order to help the Commission achieve its objectives in this space, we urge you to reconsider the compromise position as was disclosed earlier this May. In line with its own ambitions, the Commission should support the text and provisions adopted by the European Parliament.⁹ We urge the Commission to consider the following:

Strengthen human rights standards

In the draft amendments the Commission seems to revert to the old, existing wording of “serious violations” of human rights as a standard for judgement. We are concerned that this threshold lacks legal clarity, ambition, and will continue to allow harmful technologies to be exported.

⁶ “United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age” (Human Rights Council 27/37, 30 June 2014)

https://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye “Surveillance and human rights” (Human Rights Council 41/35, May 2019)

https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/41/35

⁷ “Introductory Remarks by Commissioner Phil Hogan at OECD Global Forum on Responsible Business Conduct” (European Commission, 19 May 2020)

https://ec.europa.eu/commission/commissioners/2019-2024/hogan/announcements/introductory-remarks-commissioner-phil-hogan-oecd-global-forum-responsible-business-conduct_en

⁸ “Joint Communication to the European Parliament and the Council, EU Action Plan on Human Rights and Democracy 2020-2024” (JOIN 2020/05/final, March 25, 2020)

<https://ec.europa.eu/transparency/regdoc/rep/10101/2020/EN/JOIN-2020-5-F1-EN-MAIN-PART-1.PDF>

⁹ “Draft Parliament resolution on setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast)” (December 2017)

https://www.europarl.europa.eu/doceo/document/A-8-2017-0390_EN.html

Provisions in the recast should be strengthened to guard against all risks to human rights and to recognize that serious human rights violations may occur outside situations of armed conflict or recognized situations of internal repression. In doing so, the Commission should require the consideration of relevant European human rights protections, such as the EU Charter of Fundamental Rights as well as those developed by the Court of Justice of the European Union, and the European Court of Human Rights, such as the opinion in *Zakharov v. Russia*, which offers guidance on the specific safeguards needed to ensure that secret surveillance complies with human rights law (limits on the duration of such measures, the procedures for authorising interception as well as for storing and destroying the intercepted data and the supervision of the interception).¹⁰ The Commission should ensure that the same human rights standards apply abroad as do inside the EU.

Set up meaningful due diligence

In the amendments disclosed to Politico in May, the Commission's phrasing imposes no obligations on companies to identify, prevent, mitigate and account for how they address their actual and potential impacts on human rights, associated with their operations, services and products.

We welcome the recent pledge of EU Justice Commissioner Didier Reynders to impose mandatory due diligence as well as the Commission's study on due diligence requirements, which concluded that voluntary approaches are insufficient and recommends mandatory rules for companies.¹¹ We expect to see such requirements established and meaningfully enforced in the export controls regime. Given the human rights risks associated with the use of digital surveillance technology, the export control regime should oblige exporting companies to identify, prevent, mitigate and account for risks of how their activities impact human rights as an integral part of business decision-making and risk management.

Ensure a functional catch-all and EU control list

We have previously urged the institutions to make clear in this recast that states are required to deny export licenses where there is a substantial risk that those exports may be used to violate human rights or where the legal framework for its use falls short of international human rights law or standards.

A mechanism to update the EU control list should be agreed, which will decide on updates to the EU control list in a transparent and consultative manner, taking into account the expertise of all stakeholders, including civil society, and international human rights law. The procedure to include a new category or item to the EU control list should not lay with the companies, but with the member state authorities as was present in earlier drafts. Furthermore, the Commission should publish all the decisions made through the catch-all, whether they were added to the Annex through the member state decision or whether the member states 'voted' against a technology class being added. The stand alone EU control list is incredibly valuable in achieving uniform understanding across the Union and

¹⁰ *Zakharov v Russia*: "Mass Surveillance and the European Court of Human Rights" (December 2015) <http://eulawanalysis.blogspot.com/2015/12/zakharov-v-russia-mass-surveillance-and.html>

¹¹ "Study on due diligence requirements through the supply chain" (February 2020) <https://op.europa.eu/en/publication-detail/-/publication/8ba0a8fd-4c83-11ea-b8b7-01aa75ed71a1/language-en>

preventing ‘forum shopping’ where companies deliberately pick jurisdictions with weaker implementation of export controls to process their requests.¹²

Enable meaningful transparency and reporting

Transparency regarding export licenses granted, and denied, including information regarding the type of equipment concerned, the product category, description, value, destination country and end use/end user is crucial in enabling parliaments, civil society, industry, and the broader public – both in the EU and in recipient countries – to meaningfully scrutinize the human rights impact of the trade in dual-use items.

The Commission should require that member states publicly disclose such information as well as the reasons for the approval or denial of licenses under the EU control list and catch all. While some reporting is done at the member state level, it varies greatly in scope and detail, making meaningful scrutiny nearly impossible.

We welcomed the proposal that the Commission put forth in 2016 and we are determined in assisting you in delivering a strong and ambitious set of rules for dual-use technologies that reflect the EU’s commitment to protecting human rights and enforce international law in a unified manner across the Union.

Thank you for your consideration.

Access Now

Amnesty International

Brot für die Welt

Committee to Protect Journalists

FIDH (International Federation For Human rights)

Human Rights Watch

Privacy International

Reporters Without Borders (RSF)

¹² As documented in Access Now reporting “Is NSO Group’s infamous Pegasus spyware being traded through the EU” (15 September 2019)
<https://www.accessnow.org/is-nso-groups-infamous-pegasus-spyware-being-traded-through-the-eu/>