

# **EU: European Parliament must vote to stop surveillance equipment going to rights-abusing governments**

**16 January 2018 - For Immediate Release**

European Parliament's (EP) vote tomorrow could stop the export of dangerous surveillance equipment to rights-abusing governments, according to a coalition of international NGOs. The vote, on European Union's (EU) export control regime for dual-use items, which have civilian and military uses, is an important step forward to protect journalists, dissidents and human rights defenders all over the world from human rights violations caused by surveillance technologies originating from EU countries.

"These new rules should eventually stop EU produced surveillance equipment from being exported to countries where there is a high risk it would be used to abuse journalists, activists and others who work to defend rights. They have learnt the hard way that they cannot rely upon EU governments to prioritise human rights over economic interests," said Nele Meyer, Senior Executive Officer at Amnesty International.

BAE Systems, the UK's largest arms manufacturer, was revealed in 2017 to have been exporting controlled internet surveillance systems capable of carrying out mass surveillance to countries where human rights abuses are common, including Saudi Arabia, UAE, Qatar, Oman, Morocco, and Algeria. If the EP's changes are agreed with the European Council, such exports would no longer be possible if they are likely to lead to serious human rights violations.

"The EU must take a firm stand in defence of the freedom to inform. Journalists must not be spied on or arrested with the help of these 'dual use' technologies, which also have a chilling effect on journalists and their sources, fuelling concern about the security of their communications and therefore discouraging an exchange of information," said Elodie Vialle, Head of Journalism and Technology desk at Reporters Without Borders (RSF).

The EP's proposal would require Member States to deny license applications if the export of a surveillance technology is likely to lead to serious human rights violations. Authorities will be required to consider the legal framework governing the use of any surveillance technology in the country that it is being exported to, and assess an exports' impact on the right to privacy, the right to data protection, freedom of speech, and freedom of assembly and association.

Crucially, improved transparency measures will also require Member States to record, and make publicly available, licensing data regarding approved and denied exports, allowing democratic oversight bodies, individuals, civil society and journalists to gain insight into the secretive global trade in surveillance technologies.

“The sale of surveillance equipment from EU Member States allowing authoritarian regimes to strengthen their oppressive arsenal is a routine. Transparency and a human rights based framework are needed to improve accountability and increase the public scrutiny over these practices,” said Maddalena Neglia, Director of Globalisation and Human Rights desk at FIDH.

Other measures include a new list of technologies requiring export authorisations - putting the EU’s list ahead of similar international export control bodies - and increased obligations on exporters to conduct human rights due diligence. Importantly, the proposal also recognises the imperative to protect IT security research from the scope of control, and recognises the importance of removing current export controls on cryptography. However, negotiations with Member State authorities will now determine how successfully these goals will be met.

Currently, although Member States may already take human rights considerations into account in the current system, evidence shows that they have prioritised other considerations and have approved the vast majority of exports. It is therefore crucial to ensure that the final human rights license assessment criteria are clear, binding, and applied consistently across the Union.

"The current system fails to adequately account for user’s rights to privacy and freedom of expression -- an unacceptable status quo which betrays human rights defenders and journalists around the globe,” said Lucie Krahlcova, Policy Analyst at Access Now.

“How can the EU strongly condemn intimidation and harassment against journalists, yet continue to provide the tools which facilitate that to repressive governments who undertake such repression? Now is the time to end mixed messages. In line with the EU Human Rights Guidelines on Freedom of Expression Online and Offline, the EU must take a lead on the world stage by taking all possible measures to protect these fundamental rights - and to communicate these standards clearly in all dialogues with all governments,” said Tom Gibson, CPJ’s EU Representative.

"Surveillance technologies sold by European companies endangers freedom of expression and the lives of activists, human rights defenders, journalists, and all citizens, with tragic consequences. We need transparency from Member States on these practices, and licensing data about exports to be publicly available," said Antonella Napolitano, Coordinator of the Civil Liberties in the Digital Age Programme at Coalizione Italiana Liberta e Diritti civili.

**Access Now**  
**Amnesty International**  
**Coalizione Italiana Liberta e Diritti civili (CILD)**  
**Committee to Protect Journalists**

**Fédération internationale des ligues des droits de l'Homme (FIDH)**  
**Privacy International**  
**Reporters without Borders**

**Examples and cases**

Reports in 2017 have showed that:

- UK authorities approved the export of telecommunications interception to the Ministry of Interior in Macedonia in 2012 as a security agency under its command was engaged in the unlawful surveillance of an alleged 20,000 people ([Computer Weekly](#)).
- Of over 330 export license applications for controlled surveillance technology made to 17 EU authorities since 2014, 317 have been granted and only 14 have been rejected; 11 member states, including France and Italy, refuse to make any licensing data available to public scrutiny, meaning that the actual amount of surveillance equipment being licensed for export is likely to be significantly more ([The Correspondent](#)).
- BAE Systems, the UK's largest arms manufacturer, has been exporting controlled internet surveillance systems capable of carrying out mass surveillance to countries where human rights abuses are common, including to Saudi Arabia, UAE, Qatar, Oman, Morocco, and Algeria ([BBC and Dagbladet Information](#)).
- Italy approved then subsequently revoked an export license for an internet surveillance system to Egypt ([lIFattoQuotidiano](#)).
- A French company has been exporting similar internet surveillance equipment to Egypt and has received nine other export licenses in 2016 ([Telerama](#)).
- Companies based in Italy were filmed admitting to be willing to skirt existing export regulations to sell surveillance technology to potential clients around the world, including to countries under EU restrictive measures ([Al Jazeera](#)).

**Background**

Information about the global trade in surveillance technology [came to public](#) attention during the Arab Spring, when numerous security agencies across the region were found to have been using surveillance systems exported from EU Member States.

In 2011, the Commission [released](#) a Green Paper recognising the need to update the Dual Use Regulation to reflect [advances](#) in technology and early in 2013 first [recognised](#) stakeholders' desire to bring the "use of ICT interception and monitoring items or 'cybertools'" into the scope of the Regulation.

The Commission concluded on the basis of a wide-ranging [Impact Assessment](#) and public consultation that "Cyber-surveillance technologies have legitimate and regulated law enforcement applications, but have also been used for internal repression by authoritarian

or repressive governments to infiltrate computer systems of dissidents and human rights activists, at times resulting in their imprisonment or even death.”

The Commission eventually [released](#) a subsequent proposal to modernise the EU export control infrastructure in September 2016. While the proposal offers some improvements on the current regime, it requires significant further changes to ensure it lives up to its potential of protecting human rights.

In November 2017, amendments to the proposal were agreed within the Committee on International Trade, the committee responsible for the report at the European Parliament. Proposed amendments will be discussed between the Commission, Parliament, and Member States in secretive “[trialogue](#)” meetings aimed at reaching a compromise position. Once the member states and Parliament agree to the amendments, they will become binding across the European Union.

In May 2017, a coalition of [NGOs published a short analysis on the Commission’s proposal](#).