epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER to

EUROPEAN COMMISSION

on

Guidelines on the export of cyber-surveillance items under

Article 5 of Regulation (EU) No. 2021/821

June 9, 2023

By notices published March 31, 2023, the European Commission (Commission) has solicited input to inform the Commission's efforts to strengthen export controls on certain cyber-surveillance items "that may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law." EPIC applauds the EU Commission's efforts and submits these comments to aid the Commission in further strengthening cyber-surveillance due diligence.

Since its founding in 1994, EPIC has fought to secure the fundamental right to privacy for all. EPIC continually evaluates new surveillance technologies and engages in advocacy and coalition building to halt or slow the deployment of systems that threaten individual rights or lack adequate oversight. EPIC urges the European Commission to ensure that due diligence obligations include review of stakeholders' export or use of other surveillance items, not just cyber-surveillance items.

As the Commission has noted, the significant growth in past years of spyware and other cyber-surveillance items poses grave danger to privacy and human rights. Spyware and other cyber-

surveillance items pose a particularly acute danger of abuse given their capacity to gain secret and unconstrained access to electronic device data. Indeed, repressive regimes have relied on spyware and cyber-surveillance items to target politicians, journalist, human rights defenders, and others, with dire consequences.

EPIC applauds the progress that has been made by bodies in the European Union as well as the United States, but there is still much work to be done. Many of these obligations are unnecessarily narrow and do not address the full scope of cyber-surveillance-enabled repression and privacy violations. Therefore, while EPIC commends the Commission for its efforts to ensure proper due diligence by industry stakeholders, EPIC reiterates the need for a moratorium on at least the most intrusive forms of cyber-surveillance, such as spyware.

Comments on Proposed Guidelines

Under the Commission's proposed guidance, exporters should review stakeholders involved in the transaction. According to Section IV.3 of these guidelines, red flags include instances in which "[t]he end-user has in the past exported ***cyber-surveillance items*** to countries where the use of such items has given rise to internal repression measures and/or serious violations of human rights and international humanitarian law."

The scope of this red flag is unnecessarily narrow and risks missing how cyber-surveillance tools fit into the broader surveillance ecosystem. For example, Section III.2.1 of the Commission's guidelines state that while facial and emotion recognition technology may fall within the scope of cyber-surveillance tools, this is not always the case. Further, according to Section III.2.3 of the guidelines, "[v]ideo-surveillance systems and cameras - incl. high-resolution cameras - used for the filming of people in public spaces are not covered by the definition of cyber-surveillance items, as they do not monitor or collect data from information and telecommunication systems." Certainly, larger entities may offer cyber-surveillance tools as one part of a broader suite of surveillance tools,

all of which can be used for internal repression. However, under the proposed guidelines, a red flag would only trigger if an end-user had previously exported *cyber-surveillance items* that were used for repression. Although the guidelines' context-based scope for tools like facial recognition technology help address the ways in which surveillance tools can be layered on top of one another, the narrow obligation to review prior cyber-surveillance items misses an opportunity to address surveillance-enabled repression before bad actors move from traditional surveillance tools to cyber-surveillance.

Broadening this red flag to include all surveillance items is not an unduly burdensome requirement because industry must already undertake a preliminary assessment of surveillance items to assess whether an individual item falls within the scope of these guidelines. Therefore, EPIC urges the Commission to expand due diligence obligations to include the abuse of any surveillance items, not just those that fit the definition of cyber-surveillance.

Conclusion

EPIC applauds the Commission for its continued efforts to regulate cyber-surveillance items and protect privacy. EPIC looks forward to engaging further with the Commission to support its work in this vital area. For any questions, please contact info@epic.org.

Respectfully Submitted,

Alan Butler
Alan Butler
EPIC Executive Director

Chris Baumohl
Chris Baumohl
EPIC Law Fellow