November 29, 2023

US Department of Commerce
Regulations Branch
Bureau of Industry and Security
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

RE: Notice of Inquiry – Advanced Surveillance Systems and Other Items of Human Rights Concern in Docket 200710-0186 (RIN 0694-XC063)

Freedom House appreciates the opportunity to provide comments to the Bureau of Industry and Security (BIS) in response to its Notice of Inquiry on Advanced Surveillance Systems and Other Items of Human Rights Concern. We view export controls as critical tools in protecting and advancing rights and democracy around the world and protecting human rights defenders.

Freedom House is the oldest human rights and democracy organization in the United States, founded in 1941 by Eleanor Roosevelt and Wendell Wilkie. The organization works to expand and defend freedom in the United States and around the world through a unique combination of research, programming, and advocacy.

The problem: Governments’ malign use of technology that threatens human rights

Freedom on the Net, originally launched in 2009, is Freedom House’s annual report that analyzes the ways in which human rights are protected or undermined in 70 countries around the world.¹ Over a decade of conducting this research has allowed Freedom House to monitor and analyze the changing nature of digital repression. Through this project, Freedom House works directly with activists, human rights defenders, and other civil society actors to elevate concerns about the ways they are being targeted online and, often, the types of technologies that are used against them.

What Freedom House and other civil society organizations have found, again and again, is that governments are deploying technology imported from abroad for repression.

Censorship and surveillance technologies have become more and more affordable, and a shadowy market of private companies selling these technologies has emerged in recent years. A growing market for these tools, mixed with their affordability, has lowered the barrier of entry for digital repression. Now, it is possible for governments, security officials, and local police forces to simply buy this advanced technology irrespective of their internal technical capacity and ability to produce it in-house. This includes artificial intelligence technologies, such as biometric tools like facial recognition, that will allow states to scale, deploy, and refine their capacities more quickly.

Furthermore, the global market for sophisticated spyware is booming. Spyware technologies allow any government agency to covertly and remotely access people’s personal devices. The Freedom on the Net report documented spyware being used against activists and journalists in countries around the world, including Rwanda, Uganda, India, Mexico, and Armenia.² Freedom

House also found that at least 49 of the 70 countries studied in the 2023 report were suspected of having access to sophisticated spyware or data extraction technologies. And Amnesty International and the European Investigative Collaborations media network revealed that surveillance products produced by the Intellexa alliance were deployed in at least 25 countries across Africa, the Middle East, Asia, and Europe to the detriment of human rights defenders.

In addition to facilitating human rights abuses at home, governments are also deploying spyware and other technologies to track and target people who live beyond their borders, known as transnational repression. Freedom House released its first major report on the phenomenon in early 2021 and has been devoting increased attention to the topic since.

Unsurprisingly, technology has played an enormous role in the transformation and expansion of transnational repression. This is because digital platforms and services have increased the reach of states beyond their borders, allowing them to surveil, track, harass, and target individuals through social media platforms and personal devices. Examples of the use of spyware in the commission of transnational repression include the case of Jamal Khashoggi, whose colleagues and family had their devices infected with spyware in the period leading up to his murder; as well as spyware used against Ethiopian dissidents and journalists; and malware used against Kazakh dissidents and journalists. Most recently, Galina Timchenko of the Russian independent media organization Meduza was targeted with spyware technology in Germany. And Freedom House found that spyware was used in transnational repression seventeen times in the year 2021.

The Chinese government carries out the most sophisticated and comprehensive campaign of transnational repression in the world, using a wide array of digital tactics to attempt to silence those it views as threats to the regime. As BIS is well aware, there is also widespread surveillance inside China, especially in the Uyghur region. This includes phone tapping, video surveillance, location tracking, online activity monitoring, biometric collection, and the use of artificial intelligence and associated big data tools. In fact, China is a leader in manufacturing surveillance and other digital tools that are used inside its borders and are exported to other governments, like Iran, who then use them to violate human rights. These tools may rely on equipment and chips imported from the United States. For instance, researchers found that the Iranian government deployed surveillance tools like facial recognition technology provided by a Chinese company that uses chips and equipment from a US provider.

---

3 Freedom on the Net: The Repressive Power of Artificial Intelligence, Freedom House, 4 October 2023, freedomhouse.org/report/freedom-net. Please visit the country reports within Freedom House’s Freedom on the Net, to find more information on spyware in each country: freedomhouse.org/countries/freedom-net/scores. A data sheet with sourcing by country can also be provided by Freedom House on request.
8 This huge Chinese company is selling video surveillance systems to Iran, MIT Technology Review, 15 December 2021, technologyreview.com/2021/12/15/1042142/chinese-company-tiandy-video-surveillance-iran.
While the Commerce Department, other agencies, and Congress have already given considerable attention to addressing the way Xi Jinping’s government is intensifying repression at home, and exporting that repression abroad, there is more that can be done, and BIS should seek to limit harmful impacts of US products headed to the PRC.

**The solution: Recommendations on how to protect human rights through strengthened export controls**

Freedom House commends BIS for its efforts to better protect human rights through updated export control regulations and licensing policies. We understand and acknowledge the complexity of this issue. Authoritarians and repressive actors are endlessly creative in ways to use dual-use products for repression.

Against this backdrop, Freedom House has developed three top-line recommendations on how to better protect human rights through strengthened export controls to achieve greatest impact.

1. **Establish process for routinely engaging with civil society, including NGOs, media, academia, and human rights defenders**

   Engaging civil society actors – including non-governmental organizations (NGOs), human rights defenders, media, and academia – is critical to more effectively understand the potential risks of exports and, thereby, better protect human rights through strengthened export controls. NGOs often have access to human rights defenders, vulnerable groups, and other members of civil society who may be targeted for repression. These individuals are uniquely placed to identify and report on the evolving use of technologies in repression. Indeed, thanks to civil society efforts that exposed the harm of spyware technologies, the Commerce Department and other members of the End User Review Committee were well-equipped to add rights-violating vendors like NSO Group and Intellexa to the Entity List. This action sent an important signal to the world that there will be a steep price to pay for companies found to be aiding and abetting repression.

   Specifically, BIS should involve civil society in the information gathering and assessment of due diligence guidance and other advisories. NGOs, journalists, independent researchers, and other civil society actors are regularly developing initiatives focused on non-state actor policies and procedures that could help enable implementation of due diligence strategies. This is especially pertinent given that the Export Controls and Human Rights Initiative (ECHRI) Code of Conduct, to which the United States is committed to following as a member of the ECHRI, calls for the “[promotion] of non-state actors’ implementation of human rights due diligence policies and procedures in line with the UN Guiding Principles on Business and Human Rights or other complementing international instruments.”

   In addition, Freedom House strongly urges BIS to create a clear process for routine engagement with civil society organizations and human rights defenders who may have informative expertise. To this end, the ECHRI Code of Conduct explicitly calls for governments to engage with “members of civil society, including those from vulnerable groups . . . concerning effective implementation of export control measures.” The Department of State and Department of Treasury have created this type of mechanism for engagement on Global Magnitsky and other targeted sanctions, and it has proven effective for both government and civil society with regards to two-way information exchange aimed at strengthening both the efficacy and precision of these targeted sanctions programs.

2. **Address human rights concerns through export control regulation**

   [Continued]
Freedom House also encourages BIS to address human rights concerns in new export control regulation. These regulatory changes could include the creation of a list of EAR-99 items that can be misused by repressive governments but are not subject to item-based controls, which exporters could use as a point of reference when performing transaction and counterparty diligence to identify potential red flags. BIS could regularly update this list with the NGO and other civil society input we describe above. BIS could include in the descriptions it provides for the listed items whether any end use or end user controls might apply to transactions involving the items.

In addition, for items that are already subject to item-based controls, BIS should consider reflecting “benign” and “malign” use cases for items in Export Control Classification Number headings and using subparagraph designation and/or technical notes to describe performance features or problematic uses of certain technologies. For example, there is likely a difference in outcome when governments deploy fingerprint testing technologies for government employees to enter their office building (more likely “benign” but may still raise concerns over data collection and storage) relative to the deployment of facial and gait recognition technologies used in “real-time” remote biometric identification systems in publicly accessible spaces (much more likely “malign”). Additional “malign” government uses may include pseudoscientific emotion recognition systems, especially in border management and law enforcement, and biometric categorization systems that use protected characteristics (such as gender, race, ethnicity, and sexual orientation) to classify people. Technology used in predictive policing would also pose a high risk of “malign” use in many countries.

Importantly, when considering both the listing of EAR-99 items and the amendment of ECCN descriptions to help exporters distinguish between “benign” and “malign” uses, exporters could be reminded that even technologies that have been developed to collect information to support commercial applications are not categorically “benign”; exporters need to consider how data that companies collect for commercial use can wind up in the hands of government actors to undermine human rights. For example, Position, Navigation and Timing data, which is often collected for marketing research and to generate commercial sales opportunities, can also be leveraged for surveillance if the technology is deployed by a government actor seeking to control and monitor a person of interest or for another repressive end. In other words, even commercial products that are not controlled for dual-use, and which are therefore classified only as EAR-99, can be used for nefarious purposes. BIS should add a statement along these lines in its current Crime Control and Detection policy description in Section 742.7.

For both the newly listed EAR-99 and described item-based controlled items, BIS could consider tying these items to human rights-related end use and end user licensing requirements, and creating a license exception that authorizes “white lists” of “benign” uses or “benign” end users and which would not be available for exports to “malign” end uses and end users.

In addition, and given the broader reach of export controls to transactions that involve items that are subject to EAR controls but may not involve US persons, BIS should add to its Entity List any individual or entity that the Department of the Treasury adds to its Specially Designated Nationals and Blocked Persons List (SDN) for their role in committing or enabling human rights abuses. And BIS could consider adding a new End Use/End User control that is tied to Department of Treasury designations under its Magnitsky authorities. Moreover, BIS and Treasury’s Office of Foreign Asset Control (OFAC) should coordinate on an ongoing basis on human rights-based sanctions or Entity List designations to consider whether individuals or entities should appear under both lists.
3. **Address human rights concerns through export control licensing**

BIS should also address human rights concerns through export control licensing. While governments across the democratic spectrum can and do use technology in a way that undermines human rights, the risk is higher and occurs more frequently in countries with weak rule of law and poor protections for basic freedoms. To help assess risk, licensing officers should be provided with watch lists of countries where governments or non-state actors are more likely to use exported items as tools of repression. Licensing officers should scrutinize transactions with countries that are rated as Partly Free or Not Free by any of Freedom House’s publications, as these categorizations reflect weak or vulnerable rights and rule of law. Furthermore, BIS should consult with civil society organizations with regards to adding persons and entities to any agency non-public lists that are used by licensing officers to evaluate export control licensing applications based on non-public information.

Relatedly, given the quickly evolving methods of regimes seeking to target individuals and populations for repression with technologies, BIS should have a mechanism for sharing use case studies with licensing officers to help them issue spot in their licensing reviews. And, finally, licensing officers should have access to a watch list of commodities, software, and technology that are not yet controlled for Crime Control or Section 1758 reasons but are being used by government and non-state actors in the facilitation of human rights violations.

Thank you again for the opportunity to submit comments to the Notice of Inquiry on Advanced Surveillance Systems and Other Items of Human Rights Concern. Freedom House is grateful for the invitation to contribute and looks forward to further collaboration on the topic.

Sincerely,

Annie Boyajian
Vice President of Policy and Advocacy, Freedom House