The global proliferation of commercial surveillance technologies, including spyware, poses a grave threat to human rights and national security. These tools are often wielded by malicious government authorities to surveil journalists and human rights defenders in ways that violate international human rights law and undermine democracy.

Export controls can be a key tool to combat the spread and malign use of these technologies. These controls include prohibitions on specific exports and licensing requirements. The Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware and the Export Controls and Human Rights Initiative, among other international efforts, demonstrate growing attention from governments around the world to ensuring technologies exported from their countries are not used to facilitate human rights abuses.

Recognizing the importance of export controls, Freedom House submitted comments to the US Commerce Department’s Bureau of Industry and Security in response to its Notice of Inquiry on Advanced Surveillance Systems and Other Items of Human Rights Concern. This fact sheet outlines high-level takeaways from Freedom House’s submission.

**The Problem: Governments’ Malign Use of Technology Threatens Human Rights**

Surveillance technologies have become increasingly affordable, and numerous private companies selling these technologies have emerged in recent years. A growing market for these tools, mixed with their affordability, has lowered the barrier of entry for digital repression. 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.

Specifically, the global market for sophisticated spyware is booming. Spyware technologies allow any government agency to covertly and remotely access people’s personal devices. Freedom on the Net, Freedom House’s flagship report on internet freedom in 70 countries, documented that in at least 49 countries across the democratic spectrum, governments were suspected of having access to sophisticated spyware or data extraction technologies. This included Rwanda, Uganda, Saudi Arabia, the United Arab Emirates, India, Mexico, and Armenia. Activists, journalists, and human rights defenders are particularly at risk of being targeted by these tools.

**The Solution: Protect Human Rights by Strengthening Export Controls**

Establish a process to routinely engage civil society, including NGOs, media, academia, and human rights defenders

The Bureau of Industry and Security (BIS) and similar government bodies around the world, should create a clear process for routine engagement with civil society organizations and human rights defenders who have specialized expertise.
Nongovernmental organizations (NGOs) often work with human rights defenders, vulnerable groups, and other members of society who may be targeted for repression. These individuals are uniquely placed to identify and report on the evolving use of technologies in repression.

The US Departments of State and Treasury have created this type of process for engagement on Global Magnitsky and other targeted sanctions, and it has proven to be an effective way for government and civil society to exchange information and strengthen the efficacy and precision of these targeted sanctions programs.

_Incorporate human rights protections in export control regulation_

Improved export control regulation includes:
- Creating a list of EAR-99 items that can be misused by repressive governments but are not subject to item-based controls;
- Noting “benign” and “malign” use cases for items already subject to item-based controls in Export Control Classification Number headings;
- Teaching exporters that technologies that have been developed to collect information to support commercial applications are not categorically “benign”;
- Adding to the BIS Entity List any individual or entity that the Department of the Treasury adds to its Specially Designated Nationals and Blocked Persons List for their role in committing or enabling human rights abuses; and
- Adding a new End Use/End User control that is tied to Department of Treasury human rights-related targeted sanctions designations made by the Department of the Treasury or Department of State.

_Incorporate human rights protections through export control licensing_

Improved export control licensing includes:
- Providing licensing officers with watch lists of countries where governments or non-state actors are more likely to use exported items as tools of repression, leveraging resources such as Freedom House publications;
- Creating ways to share use case studies with licensing officers to help them issue spot in their licensing reviews; and
- Providing licensing officers with access to a watch list of commodities, software, and technology that are not yet controlled for Crime Control or Section 1758 reasons but are used by government and non-state actors in the facilitation of human rights violations.

For more information, read the full comments [here](#) and read more about Freedom House’s research on technology and democracy [here](#).