

U.S. DEPARTMENT OF STATE ISSUES GUIDANCE ON HUMAN RIGHTS DUE DILIGENCE FOR SURVEILLANCE-CAPABLE PRODUCTS AND SERVICES

05 November 2020 | New York
Legal Briefings

On September 30, 2020, the U.S. Department of State published [new guidance](#) on human rights due diligence for U.S. businesses involved in the sale of products or services with surveillance capabilities that could be used by foreign governments.

The voluntary guidance identifies eight steps that businesses should take to assess and minimize the risk that their product or service will be used to violate human rights and sets out a series of “red flags” that might indicate the potential for human rights abuse. It is another example of the global trend towards the recognition of human rights due diligence as a core standard for the responsible conduct of business.

The guidance – titled “Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities” (the “**Guidance**”) – is voluntary and does not impose obligations under U.S. law. However, the Department of State has “encouraged” U.S. businesses to conduct human rights due diligence to assess and mitigate the risk that their products or services will be used to violate human rights. It notes that the misuse of products or services:

can take many forms, including to stifle dissent; harass human rights defenders; intimidate minority communities; discourage whistle-blowers; chill free expression; target political opponents, journalists, and lawyers; or interfere arbitrarily or unlawfully with privacy.

The Guidance applies to a broader range of transactions than may initially be apparent. It covers not only products and services intended to be used for surveillance, but also those with “unintended surveillance capabilities.” This includes products and services that can be used to collect or analyze sensitive data, regardless of their intended purpose, and those which are a critical component of another product or service that can be used in such a way. The non-exhaustive list of potential examples includes biometric identification software, location tracking technology, recording devices, sensors, and data analytics software or services. The Guidance also applies not only to transactions directly with foreign governments, but also to transactions with private entities that may serve (even unintentionally) as intermediaries, such as distributors and resellers, and private entities with close links to a foreign government.

The Guidance is based on the framework set out in the UN Guiding Principles on Business and Human Rights (**UNGPs**), which provides that corporations should uphold their responsibility to respect human rights by conducting due diligence to avoid and mitigate adverse human rights impacts and remediating those that occur. But whereas the UNGPs are drafted broadly, for application to any sector or type of transaction, the Guidance applies that framework to the specific context of the sale of surveillance-related products and services, helping businesses to identify risks and considerations unique to that context.

To that end, the Guidance identifies eight steps that businesses should take to assess and minimize the risk that their product or service will be used to violate human rights:

1. Review the capabilities of the product or service to assess the potential for it to be used (or misused) to violate human rights. This should include consideration of whether the product or service can be used in unintended ways, alone or in combination with others.
2. Review the human rights record of the foreign government end-user. The Guidance recommends collecting information from publically available sources, stakeholders, and experts.
3. Assess whether the foreign government’s laws and policies are consistent with international human rights obligations, as set out in the Universal Declaration of Human Rights. The Guidance notes that this can involve both in-house and external counsel.
4. Review the stakeholders involved in the transaction. This includes identifying the entities that could obtain access to the product or service, whether authorized users or not.
5. To the extent possible and as appropriate, tailor the product or service to minimize the potential for it to be used to violate human rights when it is distributed to countries that have not demonstrated respect for human rights. Tailoring the product or service may involve either adding or removing features, limiting its distribution, and other potential safeguards depending on the circumstances.

6. Prior to sale, strive to minimize human rights risks through contractual and procedural safeguards, and strong grievance mechanisms. The business should use the resources at its disposal to minimize the risk of the product or service being abused to violate human rights. This can include incorporating human rights provisions into a contract, and retaining an ability to cut off access to, or support for, a product or service if the business determines it is being misused. The business should also strive to create effective grievance mechanisms so that it becomes aware of instances of misuse of the product or service and can take action.
7. Likewise, after the sale, strive to minimize human rights risks through contractual and procedural safeguards, and strong grievance mechanisms. In this respect, the Guidance recognizes that businesses' obligation to respect human rights does not end with the sale, but continues while the product or service is in use.
8. Publically report on sales practices, such as in annual reports or on the business's website.

At each of steps 1-4, the Guidance lists potential "red flags" that indicate a risk the product or service will be used to violate human rights. The presence of any of these red flags should cause the business to consider the extent to which the risk can be eliminated or minimized through the actions described in steps 5-7, and depending on the answer whether the business should proceed with the transaction at all.

Red flags include (among many others):

- past use of similar products or services to commit human rights abuses;
- that the transaction includes products or services can be used to create a system that has been identified as reasonably likely to be used to commit or facilitate human rights abuses (even in the absence of previous examples of such use);
- a foreign government's history of human rights abuses, or history of exporting products to other countries with a history of human rights abuses;
- laws that unduly restrict civic space or target particular groups in violation of international human rights law; and
- conversely, the absence of adequate legal protections for human rights, or absence of rule of law in the foreign state.

Publication of the Guidance comes at a time when the U.S. Government is paying attention to the human rights impacts of technology exports through export control regulations as well – such as a recent new rule (issued Oct. 6, 2020) clarifying that the U.S. Bureau of Industry and Security may consider potential human rights impacts when reviewing certain export license applications. The Guidance supplements binding export control regulations by encouraging U.S. businesses to conduct human rights due diligence even when export authorization is not required for the product or service in question. [As we noted in a prior post](#), the U.S. Government has also encouraged businesses to implement the due diligence processes described in the UNGPs as a means of detecting and avoiding potential violations of U.S. sanctions.

The Guidance also comes at a time when laws making it mandatory for businesses to conduct human rights due diligence are being enacted or considered in a number of jurisdictions, particularly [in Europe](#). The Guidance is nowhere near as sweeping as those pieces of legislation, with its focus on surveillance-capable products and foreign government end-users, and is not mandatory. But it does suggest further acceptance of human rights due diligence as an appropriate means to avoid human rights impacts associated with business activity, which will only increase expectations for businesses to conduct due diligence, even when it is not legally mandatory.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.



ANTONY CROCKETT
PARTNER, HONG
KONG
+852 21014111
Antony.Crockett@hsf.com



BENJAMIN GUTHRIE
ASSOCIATE, NEW
YORK
+1 917 542 7851
benjamin.guthrie@hsf.com



OLIVER ELGIE
SENIOR ASSOCIATE,
LONDON
+44 20 7466 6446
Oliver.Elgie@hsf.com

LEGAL NOTICE

The contents of this publication are for reference purposes only and may not be current as at the date of accessing this publication. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.

© Herbert Smith Freehills 2022

SUBSCRIBE TO STAY UP-TO-DATE WITH INSIGHTS, LEGAL UPDATES, EVENTS, AND MORE

Close