October 23, 2020

U.S. State Department Issues Human Rights Compliance Guidance for Products and Services With Surveillance Capabilities

Attorneys
Michael R. Littenberg
Anne-Marie L. Beliveau
Nellie V. Binder

On September 30, the U.S. State Department published Guidance on implementing the UN Guiding Principles on Business and Human Rights in connection with transactions linked to foreign government end-users involving products and services with surveillance capabilities. The Guidance, which is the culmination of a two-year process, is intended to provide a framework for helping U.S. companies that work with or design and manufacture products or services that have surveillance capabilities to identify the risk of the end-user misusing the product or service to carry out human rights violations or abuses. The Guidance will be particularly helpful for businesses undertaking a human rights review where U.S. government authorization for export is not required. The Guidance is described in further detail in this Alert.

Scope, Context and Purpose of the Guidance

The Guidance applies to products and services with intended or unintended surveillance capabilities that are furnished to foreign persons by U.S. businesses. For purposes of the Guidance, products with intended or unintended surveillance capabilities are products or services marketed for or that can be used (with or without the authorization of the business) to detect, monitor, intercept, collect, exploit, preserve, protect, transmit and/or retain sensitive data, identifying information or communications concerning individuals or groups. Examples of relevant product or service types include sensors, biometric identification, data analytics, internet surveillance tools, non-cooperative location tracking and recording devices. Relevant products and services come within the scope of the Guidance if they are furnished to either foreign government end-users or foreign private end-users with a close relationship with a foreign government.

As indicated in the Guidance, products or services with intended or unintended surveillance capabilities have the potential to provide positive contributions to a country's economic, defense and societal well being. For example, these products or services can be used to strengthen government end-user network security in a rights-protecting manner, such as protecting election systems from interference. When used appropriately, the products or services can help resolve urgent challenges facing society.

However, as also indicated in the Guidance, these products and services can be misused to violate or abuse human rights when exported to foreign government end-users or private end-users that have close relationships with governments that do not demonstrate respect for human rights and rule of law. According to the Guidance, in some cases, foreign governments have misused these products or services to subject entire populations to arbitrary or unlawful surveillance, violating or abusing the right to be free from arbitrary or unlawful interference with privacy as set out in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. In other cases, governments employ these products or services as part of a broader state apparatus of oppression that violates and abuses human rights and fundamental freedoms enumerated in the Universal Declaration of Human Rights, including freedoms of expression, religion or belief, association and peaceful assembly. Some of the forms misuse can take include stifling dissent, harassing human rights defenders, intimidating minority communities, discouraging whistle-blowers, chilling free expression, targeting political opponents, journalists and lawyers and interfering arbitrarily or unlawfully with privacy.

The Guidance provides a framework for U.S. businesses to consider the human rights risks associated with products and services with surveillance capabilities in accordance with the UN Guiding Principles on Business and Human Rights and the Organisation for Economic Co-operation and Development's Guidelines for Multinational Enterprises, both of which

are further described below. The Guidance also is intended to provide U.S. businesses with a greater understanding of the human rights concerns the U.S. government may have with certain transactions.

The UN Guiding Principles and the MNE Guidelines – A Brief Overview

The UN Guiding Principles on Business and Human Rights, which were adopted in 2011, implement the United Nation's "Protect, Respect and Remedy" framework. The human rights encompassed by the UN Guiding Principles include internationally recognized human rights, which, at a minimum, include those expressed in the International Bill of Human Rights and the principles concerning fundamental rights set out in the International Labour Organization's Declaration on Fundamental Principles and Rights at Work.

As part of the foundational principles of the corporate responsibility to respect human rights, business enterprises should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved. More specifically, the responsibility to respect human rights requires business enterprises to (1) avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur, and (2) seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.

In order to meet their responsibility to respect human rights, the UN Guiding Principles indicates that business enterprises should have in place policies and processes appropriate to their size and circumstances, including (1) a policy commitment to meet their responsibility to respect human rights, (2) a human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights and (3) processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute.

The OECD Guidelines for Multinational Enterprises are recommended principles and standards for responsible business conduct in a global context. The MNE Guidelines are aligned with the UN Guiding Principles.

The recommendations in the MNE Guidelines are broken out into ten topic areas:

- General policies
- Disclosure
- Human rights
- Employment and industrial relations
- Environment
- Combating bribery, bribe solicitation and extortion
- Consumer interests
- Science and technology
- Competition
- Taxation

Integrating Human Rights Due Diligence into Compliance Programs

The Guidance encourages businesses to integrate human rights due diligence into compliance programs, including export compliance programs. As used in the Guidance, "due diligence" is defined as the process by which a business works to identify, anticipate, prevent, mitigate and account for how it addresses actual or potential adverse impacts on the human rights of individuals. Consistent with the UN Guiding Principles, this includes impacts that the business may cause or contribute to, or to which it is otherwise directly linked.

As noted in the Guidance, characteristics of due diligence in line with the UN Guiding Principles include, but are not limited to, (1) assessing and addressing risk, (2) ongoing assessment of monitoring and evaluation to verify whether

adverse impacts are being effectively addressed and new potential impacts identified, (3) stakeholder engagement, (4) public communication, (5) establishing secure, accessible and responsive communication channels for internal and external reporting of grievances and (6) alignment with human rights instruments.

According to the Guidance, integration of human rights due diligence should include (1) support from the highest levels within the organization, (2) training on relevant human rights considerations for employees, (3) development of appropriate policies, systems and processes and (4) documentation and communication of both commitments and steps taken to mitigate the risk of human rights abuses and violations.

Human Rights Due Diligence and Risk Mitigation Recommendations

The Guidance contains eight broad due diligence and risk mitigation considerations and safeguards, as further described below.

The Guidance notes that not all of the recommendations will be appropriate in all contexts and circumstances. In addition, recommendations may warrant different weight depending on the level of risk associated with the product or service, destination country and end-user. The Guidance also notes that, in accordance with the UN Guiding Principles, the factors that should be considered in addressing risks where impacts are directly linked include the business's leverage over the entity concerned, how crucial the relationship is to the business, the severity of the abuse and whether terminating the relationship with the entity would have adverse human rights consequences.

The Guidance also contains related red flags that may warrant follow-up. The red flags contained in the Guidance are not intended to be exhaustive. In addition, the weight carried by a red flag depends on the context and surrounding circumstances. The mere existence of a red flag does not mean that a transaction should be terminated, but rather that it should be evaluated in the context of other red flags and context-specific factors.

Review Product or Service Capabilities for Potential Misuse to Commit Human Rights Violations or Abuses

- Review the product or service and conduct assessments to determine if it could be misused to violate or abuse human rights, including the rights to freedom of expression, peaceful assembly, freedom of association, freedom of religion or belief and the right to be free from arbitrary or unlawful interference with privacy. According to the Guidance, factors to consider when evaluating the human rights impact of a potential transaction include, but are not limited to, whether:
    - The primary purpose or an inherent capability of the product or service is to collect sensitive data that can reasonably be linked to an individual.
    - The primary purpose or an inherent capability of the product or service is to analyze datasets in order to capture or derive sensitive insights about identified or identifiable individuals.
    - The product or service can be used without modification for the purposes described in the preceding sub-bullets items, irrespective of its design or intended use.
    - The product or service is widely available from other suppliers or provides a unique or custom capability.
    - The product or service is a critical component or part of an end-product or service described in the first three sub-bullets above.

Red Flags

- Information (such as reports, articles and publications) that indicates a similar product or service has been misused to commit human rights violations or abuses.

- The transaction includes products or services that could be used to build, customize or configure a system that is known to be misused to commit or facilitate human rights violations or abuses, or it is assessed by a reasonable person to be likely that it will be used for that purpose.

Review the Human Rights Record of the Foreign Government Agency End-User

- Review credible reports of the human rights record of the recipient government agency end-user, including the State Department's annual Country Reports on Human Rights Practices, news reports and information from non-governmental and/or local sources. Reviews should focus on the specific entity within the government, as appropriate.

- Consider reaching out to the State Department (including U.S. embassies) and NGOs at the international level and in the country where the transaction is to occur concerning the human rights record of the recipient government agency end-user.

- Consider whether the foreign government agency end-user has targeted individuals (such as journalists or members of minority groups), including through use of technology, in retaliation for the exercise of their human rights or on discriminatory grounds prohibited by international law.

- Consider the nature of the relationship between the receiving foreign government agency end-user and the part of the foreign government that provides security services.

- If the foreign government agency end-user is a provider of security services, consider whether there are instances where similar products or services have been misused for something other than a legitimate law enforcement or intelligence purpose. The Guidance describes a legitimate law enforcement or intelligence purpose as official use by government law enforcement or intelligence agencies, including government security services, in a manner consistent with government commitments under the Universal Declaration of Human Rights.

Red Flags

- Information, such as reports or articles, regarding the foreign government agency end-user's misuse of products or services with similar capabilities to commit human rights violations or abuses.

- Laws, regulations or foreign government policies that unduly restrict civic space and/or target individuals or members of a group solely on the basis of race, sex, language, religion, political opinion, national origin or any other grounds inconsistent with international human rights law.

- Ongoing conflict in the region where the transaction involving the product or service occurs.

- Ongoing abuse or arbitrary detention of members of minority groups, civil society members or journalists, such as for exercising freedom of expression.

- Lack of independent judicial or other appropriate oversight/rule of law.

- The foreign government agency end-user provides security services and has misused the product or service or similar products or services for something other than a legitimate law enforcement purpose.

- The foreign government agency end-user has a close relationship with the part of the foreign government that provides security services and has misused the product or service or similar products or services to commit or facilitate human rights violations or abuses.

- The foreign government end-user has a record of human rights violations or abuses, including where the foreign government end-user's record on human rights is so poor that it raises credible concerns that the product or service would be misused to commit or facilitate governmental human rights violations or abuses.

- The foreign government end-user has a history of exporting products or services to other countries with a history of committing human rights violations or abuses.

Review, Including Through In-House or Outside Counsel, Whether the Foreign Government End-User's Laws, Regulations and Policies that Implicate Products and Services with Surveillance Capabilities Are Consistent with the Universal Declaration of Human Rights

- Review laws, regulations or policies that may unduly hinder freedom of expression, and/or unlawfully or arbitrarily interfere with privacy, as appropriate.

- Review laws, regulations or policies concerning government interception of private communications and government access to stored private communications, as appropriate.

- Review the extent to which the foreign government has laws on surveillance and the oversight mechanisms in place, and the extent to which it implements such laws, as appropriate.

- Review the IT infrastructure of the destination country to determine level of government access and/or control, as appropriate.

Red Flags

- Laws (pending or otherwise) or policies that provide for government access to information and communications technology company data without reasonable safeguards and appropriate oversight.

- Laws, regulations or policies (including those relating to counterterrorism or national security) that appear to unduly restrict freedom of expression or unlawfully or arbitrarily interfere with privacy.

- Absence of written laws dealing with government access to communications, laws that are not publicly accessible or laws that are vague and ambiguous in terms of government powers.

- Foreign government engagement in malicious cyber-activities or arbitrary or unlawful data collection against individuals or dissident groups.

- Lack of independent judicial or other appropriate oversight/rule of law over data collection or data sharing.

- Laws, regulations or policies that require data sharing with foreign governments with poor human rights records.

- Data localization requirements.

- Total or significant government control or ownership (e.g., a partially state-owned enterprise) of information technology infrastructure and/or Internet Service Providers or telecommunication networks beyond that used for government systems and communications. The Guidance includes an illustrative list of the types of laws that may raise these concerns.

Review Stakeholders Involved in the Transaction, Including End-user and Intermediaries Such as Distributors and Resellers

- Before and during any transaction, review how the intermediaries and/or end-users intend to use the product or service.
- Review or seek to ascertain whether the end-user is intending to or likely to contract the work involving the product or service in question to non-governmental entities or individuals inside or outside the destination country and consider the available past human rights performance of such entities or individuals.
- If the end-user is not the government, review the level of control the government has over the entity in question, to the extent possible.
- Review risks that the product or service will be diverted to a different unauthorized end-user.
- Review, to the extent possible, the end-user government's history of use of the types of products or services involved in the transaction.

Red Flags

- The end-user is not a foreign government, but has a close relationship with a foreign government that has a reputation for committing human rights abuses or violations, including the kinds of human rights violations or abuses the transaction could help facilitate.
- The stated end-user in the transaction is likely not the only end-user.

To the Extent Possible and as Appropriate, Tailor the Product or Service Distributed to Countries that Do Not Demonstrate Respect for Human Rights and the Rule of Law to Minimize the Likelihood that It Will Be Misused to Commit or Facilitate Human Rights Violations or Abuses

- Integrate safety, privacy by design and security by design features appropriate to the risks and technical capabilities of the covered product or service, such as:
    - Mechanisms for individuals to report misuse of the product or service.
    - Stripping certain capabilities from the product or service prior to sale.
    - Preventing interconnected products from being misused.
    - Limiting use to the authorized purpose.
    - Limiting upgrades, software updates and direct support that enhance or provide new surveillance features.

- Providing for data minimization.

- Place conditions on intellectual property associated with use of the products or services to be consistent with international human rights standards.

Prior to Sale, Strive to Mitigate Human Rights Risks through Contractual and Procedural Safeguards and Strong Grievance Mechanisms

- Include human rights safeguards language in contracts. The language should be specific to human rights risks identified and/or associated with the product or service.

- For sales where the ultimate end use may not be known, but the product or service presents a human rights risk, require end-user license agreements with human rights safeguards language, and require resellers to conduct their own human rights due diligence in cases of resale.

- Include protections for the seller and human rights protections in the contract. For example, as applicable to the technical capabilities of the product or service, include (1) end-use limitations, (2) clauses requiring end-users to agree to comply with applicable U.S. export control laws and regulations and (3) limitations on how the product or service can or cannot be used. In addition, restrict how and by whom collected data is to be analyzed, stored, protected and shared. Also reserve the seller's right to terminate access to technology, deny software updates, training and other services and/or unilaterally terminate the contract if the seller uncovers, in its sole discretion, evidence that the technology is being misused.

- Adopt access and distribution mechanisms and contractual provisions that authorize the seller to maintain full control and custody of the product and terminate access if necessary to minimize risk of diversion, where practicable (such as through cloud-based access rather than on-premises installations and license keys requiring periodic renewal rather than permanent activation).

- Establish a preventative framework to revoke usage rights when necessary (e.g., the seller may stop providing support, updates and training or cut off the user's access to any cloud-based portion of the service based on substantiated instances of misuse).

- Provide routine human rights due diligence training to all employees involved in the transaction.

- Grievance mechanisms:

    - Develop secure, accessible and responsive communications channels for both internal and external persons to report possible misuse of products or services, such as a reporting mechanism through the company website and allowing for anonymous reporting.

    - Develop secure and confidential reporting procedures to protect those reporting misuse.

    - Develop a formal follow-up mechanism for non-anonymous reports, including an investigation and response to the person reporting misuse. As part of the foregoing, consider whether it is possible to communicate a response securely to the person reporting misuse to avoid risking their safety.

    - Regularly review and update the communication channel to make sure it is effective.

After Sale, Strive to Mitigate Human Rights Risks Through Contractual and Procedural Safeguards and Strong Grievance Mechanisms

- As appropriate and applicable to the technical capabilities of the product or service, invoke contractual protections that permit the seller to immediately stop providing upgrades, direct support and other assistance in the event of breaches of contractual terms and conditions.

- Reassess human rights due diligence considerations prior to (1) license renewal, (2) new activities, provision of services to or relationships with the customer, (3) major changes in the business relationships and (4) social and political changes that could result in misuse of products or services in the country where the customer resides.

- Stay aware of news developments and shifts in a customer's home country in order to stay abreast of how the product or service could be used by the government to restrict civic space and/or target journalists, vulnerable groups or minority groups, such as by reaching out to non-governmental organizations and civil society groups in the export destination country and carrying out ongoing due diligence after sale)

- Grievance mechanisms:

    - Thoroughly investigate all complaints of misuse. In addition, remotely disable the product or service and/or limit upgrades and customer support when a credible and significant complaint of misuse is received until the investigation is complete. Given the level of complexity of investigations involving foreign governments, the Guidance notes that the U.S. seller could consider engaging in formal or informal multi-stakeholder efforts.

    - Where misuse is found, follow up with the person filing the report through a secure communications channel (if it is possible to communicate securely to avoid risking their safety) to provide remedy where possible.

Publicly Report on Sale Practices

- At least annually, publicly report on human rights due diligence.

- At least annually, publicly report on credible complaints, incidents and resolutions, while minimizing security risks to persons filing complaints (such as by providing a high-level summary).

- Publish a human rights policy.

- Publicly report on a website, in a public annual report or an otherwise accessible location.

Relationship to Existing Export Requirements

The Guidance does not modify existing law. As noted in the Guidance, it should not be conflated with the regulatory requirements for exporters under the International Traffic in Arms Regulations, Export Administration Regulations or any other U.S. government export control regime. Exporters are responsible for obtaining appropriate licenses and/or authorizations for the export of controlled dual-use items, defense articles and defense services.

Additional Materials

The Guidance also includes two appendices.

Appendix 1 lists selected human rights tools, reports and guidance. These materials include (1) U.S. government information and tools, (2) non-U.S. government tools, reports, initiatives and guidance and (3) selected international treaties, principles and guidance.

Appendix 2 includes examples of government laws, regulations and policies that could raise concerns. These are broken out into four categories: (1) freedom of expression; (2) privacy; (3) restricting civic space/targeting individuals or members of groups on the basis of their race, sex, language, religion, political opinion, national origin or other grounds; and (4) total or significant control over internet service providers or telecommunications networks.

About Our Practice

Ropes & Gray has a leading ESG, CSR, business and human rights and supply chain compliance practice. We offer clients a comprehensive approach in these subject areas through a global team with members in the United States, Europe and Asia. In addition, senior members of the practice have advised on these matters for more than 30 years, enabling us to provide a long-term perspective that few firms can match.

For further information on the practice, click here.

Please click here to visit our CSR and Supply Chain Compliance website.