U.S. DEPARTMENT OF STATE

Guidance on Implementing the *UN Guiding Principles* for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities

TABLE OF CONTENTS

PURPOSE

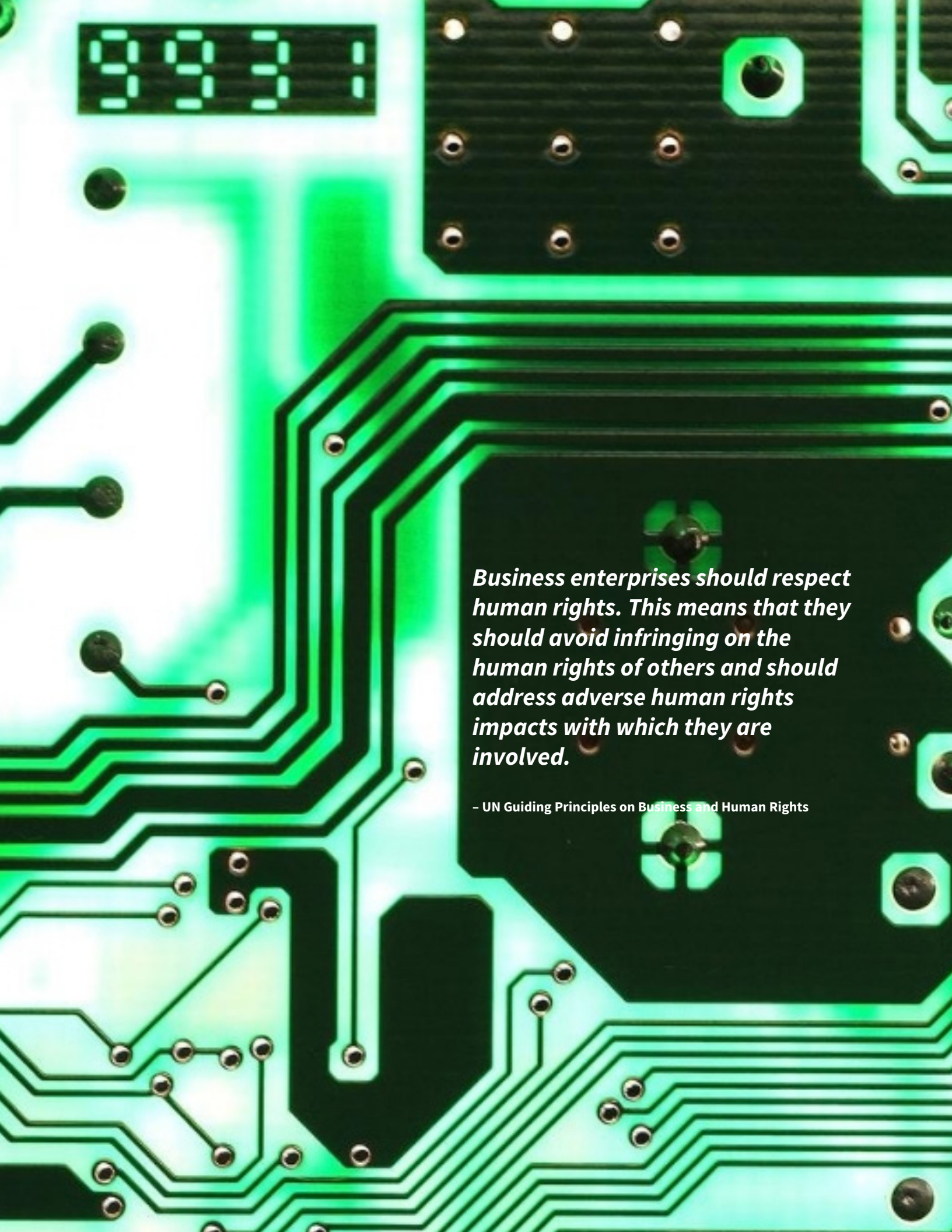
The U.S. Department of State is committed to the promotion and protection of human rights. In that spirit, U.S. businesses should carefully review this voluntary guidance and consider whether to participate in, or continue to participate in, transactions if they identify a risk that the end-user will likely misuse the product or service to carry out human rights violations or abuses. The responsibility of U.S. businesses to respect human rights does not depend on the size, sector, operational context, ownership, or structure of the business. Nevertheless, the scale and complexity of the means through which businesses meet this responsibility may vary according to these factors and will be influenced by the severity of risk of the business's adverse human rights impacts. Not every recommendation in this document is appropriate in all contexts and circumstances, but businesses can employ the recommendations to identify past patterns of abuse and risks of future misuse. Each recommendation may also warrant different weight depending on the level of risk associated with the product or service, destination country, and end-user. This guidance provides a framework for U.S. businesses to consider the potential and foreseeable consequences that a product or service can be misused to violate or abuse human rights.

This guidance is not intended to, nor should it be interpreted as, imposing requirements under U.S. law or regulations. The language contained in this document should not be conflated with the regulatory requirements for exporters under the International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), or any other U.S. government export control regime. The Department of Commerce's Bureau of Industry and Security (BIS) and the Department of State's Directorate of Defense Trade Controls (DDTC) are responsible for regulating the export of EAR-controlled dual-use items and ITAR-controlled defense articles and defense services, respectively. BIS maintains a set of Red Flag Indicators and "Know Your Customer Guidance" for exporters to follow when exporting items subject to the EAR. Exporters are responsible for obtaining appropriate licenses and/or authorizations for the export of controlled dual-use items, defense articles, and defense services.

The guidance seeks to assist U.S. businesses that work with or design and manufacture products or services that have surveillance capabilities with implementation of the UN Guiding Principles on Business and Human Rights (UN Guiding Principles) as well as the Organization for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises (OECD Guidelines). The guidance provides U.S. businesses with a way of identifying products or services that can be misused to violate or abuse human rights, and considerations to weigh prior to engaging in transactions linked to foreign government end-users or private end-users that have a close relationship with governments. This guidance will be particularly helpful for U.S. businesses that want to undertake a human rights review where the U.S. government does not require an authorization for export.

U.S. businesses are encouraged to integrate human rights due diligence into compliance programs, including export compliance programs. Such integration should include support from the highest levels within a business' organization; training on relevant human rights considerations for employees; development of appropriate policies, systems, and processes; and documentation and communication of both commitments and steps taken to mitigate the risk of human rights abuses and violations.

The guidance also offers U.S. businesses greater understanding of the human rights concerns the U.S. government may have with certain transactions. Appendix 1 provides a list of recommended resources that U.S. businesses may find helpful to consult when conducting due diligence on transactions involving products or services with intended and unintended surveillance capabilities. For global context, Appendix 2 provides a list of general issues of human rights concern that have arisen related to such products or services, including examples of relevant government laws, regulations, and policies.



Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.

– UN Guiding Principles on Business and Human Rights

BACKGROUND

Products or services with intended and unintended surveillance capabilities have the potential to provide positive contributions to a country's economic, defense, and societal well being. For example, such 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, such products or services can help resolve urgent challenges facing society.

At the same time, these products or 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. In some cases, foreign governments have misused such 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 (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).[1] In other cases, governments employ such products or services as part of a broader State apparatus of oppression that violates and abuses human rights and fundamental freedoms enumerated in the UDHR, including freedoms of expression, religion or belief, association, and peaceful assembly.

Misuse 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. Arbitrary or unlawful interference with individual privacy is a particular concern since such interference may also impede the enjoyment of other human rights, including the rights to freedom of expression, hold opinions without interference, freedom of association and peaceful assembly, and religion or belief. These and other rights are among the foundations of any society and underpin a rules-based international order.

[1] *Throughout this document we will use the UDHR given that it applies universally.*

DEFINITIONS

Human Rights Due Diligence (hereinafter "due diligence"): For the purpose of this document, "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. This includes impacts that it may cause or contribute to, or to which it is otherwise directly linked. In accordance with the UN Guiding Principles, among the factors that should be considered 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.

Due diligence is an integral part of business decision-making and risk management systems.

Characteristics of due diligence in line with the UN Guiding Principles include but are not limited to:

- **Assess and Address Risk:** The amount and depth of due diligence should be commensurate with the severity and likelihood of an adverse impact, where more significant risks are prioritized (e.g., due to the type of product or service involved and/or the end-user's operating context.)
- **Ongoing Assessment of Monitoring and Evaluation:** Iterative, responsive, and adaptable process that includes monitoring, evaluation, and feedback loops to verify whether adverse impacts are being effectively addressed and new potential impacts identified.
- **Stakeholder Engagement:** Ongoing communication with those whose human rights could be affected by the business's activities. The non-governmental organizations whose reports are referenced at Appendix 1 "Non-U.S. Government Tools, Reports, Initiatives, and Guidance" are recommended groups for stakeholder engagement.
- **Public Communication:** Communication, at least annually, of the business's commitment to a rigorous internal and external review of human rights risks and to adequate measures to address these risks.
- **Grievance Mechanism:** Establish secure, accessible, and responsive communication channels for internal and external reporting of possible misuse of a product or service. As outlined in the UN Guiding Principles, the mechanism should be legitimate, accessible, predictable, equitable, rights compatible, and developed in consultation with those whose use it is intended for.
- **Alignment with Human Rights Instruments:** Review process should be based on the UDHR, ICCPR, OECD Guidelines, and the UN Guiding Principles.

Legitimate Law Enforcement or Intelligence Purpose: For the purpose of this document, "legitimate law enforcement or intelligence purpose" means official use by government law enforcement or intelligence agencies, including government security services, in a manner consistent with government commitments under the UDHR.

Product or Service with Intended or Unintended Surveillance Capabilities: For the purpose of this document, "product or service with intended or unintended surveillance capabilities" [also referred to as "product(s) or service(s)" in this document] is defined as a product or service 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.

Factors to consider when evaluating the human rights impact of a potential transaction include but are not limited to:

a. 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.
b. 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.
c. Whether the product or service can be used without modification for such purposes described in (a) or (b) regardless of its design or intended use.
d. Whether the product or service is widely available from other suppliers or provides a unique or custom capability.
e. Whether the product or service is a critical component or part of an end-product or service described in (a), (b), and (c).

Different steps of this guidance will be more or less relevant, depending on the industry sector and type of product or service (e.g., critical component or end-product). Examples of the types of relevant products or services include but are not limited to:

- Sensors (e.g., specialized computer vision chips, thermal imaging systems, electronic emissions detection systems, products designed to clandestinely intercept live communications)
- Biometric identification (e.g., facial recognition software, automated biometric systems, rapid DNA testing, gait analysis software)
- Data analytics (e.g., social media analytics software, predictive policing systems)
- Internet surveillance tools (e.g., "spyware," products with certain deep packet inspection functions, penetration-testing tools, products designed to defeat cryptographic mechanisms in order to derive confidential variables or sensitive data including clear text, passwords, or cryptographic keys)
- Non-cooperative location tracking (e.g., products that can be used for ongoing tracking of individuals' locations without their knowledge and consent, cell site simulators, automatic license plate readers)
- Recording devices (e.g., body-worn or drone-based, network protocol surveillance systems, devices that record audio and video and can remotely transmit or can be remotely accessed)

Red Flag: For the purpose of this document, a "red flag" is any information that arises through any source where follow-up, assessment, and/or further due diligence is warranted. Not all red flags carry equal weight – rather, it 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. For example, red flags relating to the past commission of human rights abuses or violations by a government end-user involving similar products or services requires more significant follow-up. This document does not provide an exhaustive list of red flags that should be considered.

HUMAN RIGHTS DUE DILIGENCE AND RISK MITIGATION CONSIDERATIONS

1. **Review the capabilities of the product or service in question to determine potential for misuse to commit human rights violations or abuses by foreign government end-users or private end-users that have close relationships with a foreign government.**

   Due Diligence Considerations:

   - Review product or service and conduct assessments to determine if the product or service 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. See the definition of "product or service with intended or unintended surveillance capabilities" for some factors to consider in evaluating the human rights impact of a product or service.

   Red Flags:

   - Information (e.g., reports, articles, 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.

2. **Review the human rights record of the foreign government agency end-user of the country intended to receive the product or service.**

   Due Diligence Considerations:

   - Review credible reports of the human rights record of the recipient government agency end user, including the U.S. Department of State'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. See Appendix 1 for additional recommended sources and Appendix 2 for general examples of laws, regulations, and policies that have raised human rights concerns.
   - Consider reaching out to the U.S. Department of State, including U.S. embassies, and non-governmental organizations at the international level and in the country where the transaction is to occur to access first-hand knowledge of the human rights record of the recipient government agency end-user. Appendix 1 includes a list of some non-governmental organizations to engage.
   - Consider whether the foreign government agency end-user has targeted individuals, including through use of technology, in retaliation for the exercise of their human rights or on discriminatory grounds prohibited by international law (e.g. journalists or members of minority groups).
   - 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.
   - In cases where 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.

Red Flags:

- Information regarding the foreign government agency end-user's misuse of products or services with similar capabilities to commit human rights violations or abuses (e.g., reports, articles).
- 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 (e.g., for exercising freedom of expression).
- Lack of independent judicial or other appropriate oversight/rule of law.
- 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.
- 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.
- 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.
- 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.

3. **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 UDHR. See Appendices 1 and 2.**

Due Diligence Considerations:

- 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 counterterrorism or national security-related laws, regulations, or policies 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 of IT infrastructure and/or Internet Service Providers or telecommunication networks beyond that used for government systems and communications (e.g., partially state-owned enterprise). See Appendix 2 for examples.

4. Review stakeholders involved in the transaction (including end-user and intermediaries such as distributors and resellers). Refer to BIS Know Your Customer Guidance.

Due Diligence Considerations:

- 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.

5. 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.

- » Strip certain capabilities from the product or service prior to sale.
- » Prevent interconnected products from being misused.
- » Limit use to the authorized purpose.
- » Limit upgrades, software updates, and direct support that enhance or provide new surveillance features.
- » Provide for data minimization.

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

6. Prior to sale, strive to mitigate human rights risks through contractual and procedural safeguards and strong grievance mechanisms.

Contractual and Procedural Safeguards:

- 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.
- In sales where the ultimate end use may not be known but the product or service in question presents a human rights risk, require end-user license agreement with human rights safeguards language, and require re-sellers 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 end-use limitations; clauses requiring end-users to agree to comply with applicable U.S. export control laws and regulations; and limitations on how the product or service can/cannot be used. Restrict how and by whom collected data is to be analyzed, stored, protected, and shared; and 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 (e.g., cloud-based access rather than on-premises installations; 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 actors to report possible misuse of products or services (e.g., reporting mechanism through company website; allow 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 actor reporting misuse. Consider whether it is possible to communicate a response securely to the actor reporting misuse to avoid risking the actor's safety.
- Regularly review and update the communication channel to make sure it is effective.

7. **After sale, strive to mitigate human rights risks through contractual and procedural safeguards and strong grievance mechanisms.**

   Contractual and Procedural Safeguards:

   - 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 license renewal; new activities, provision of services to, or relationships with the customer; major changes in the business relationships; and 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 (e.g., reach out to non-governmental organizations and civil society groups in the export destination country; carry out ongoing due diligence after sale).

   Grievance Mechanisms:

   - Thoroughly investigate all complaints of misuse. Remotely disable the product or service and/or limit upgrades and customer support when a credible and significant complaint of misuse is received until investigation is complete (given the level of complexity of investigations involving foreign governments, the U.S. seller could consider engagement in formal or informal multi-stakeholder efforts).
   - Where misuse is found, follow-up with actor filing report through secure communications channel (if it is possible to communicate securely to avoid risking the actor's safety) to provide remedy where possible. Examples of possible remedies can be found in the UN Guiding Principles.

8. **Publicly report on sale practices (e.g., in annual reports or on websites).**

   - At least annually, publicly report on human rights due diligence (e.g., rigorous internal and external review of human rights risks; adequate measures taken to address these risks; data requests). See Appendix 1, Ranking Digital Rights Corporate Indicators which may be relevant to public reporting.
   - At least annually, publicly report on credible complaints, incidents, and resolutions, while minimizing security risks to actors filing the complaint (e.g., high-level summary).
   - Publish a human rights policy.
   - Publicly report on a website, in a public annual report, or an otherwise accessible location.

Misuse of products and 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.

APPENDIX 1 – HUMAN RIGHTS TOOLS, REPORTS, & GUIDANCE

Information Source or Tool	Description	Frequency of Updates
U.S. Government Information and Tools		
U.S. Department of State Country Reports on Human Rights Practices	Covers internationally recognized individual, civil, political, and worker rights, as set forth in the Universal Declaration of Human Rights and other international documents. The reports can include specific information on foreign government agencies.	Annually
U.S. Department of State Investment Climate Report	Provides information on the business climates of more than 170 economies around the world. They analyze a variety of economies that are or could be markets for U.S. businesses. Topics include Openness to Investment, Legal and Regulatory Systems, Dispute Resolution, Intellectual Property Rights, Transparency, Performance Requirements, State-Owned Enterprises, Responsible Business Conduct, and Corruption.	Annually
Non-U.S. Government Tools, Reports, Initiatives, and Guidance[2]		
Access Now	Supports civil society efforts to track and mitigate threats posed by new technologies. Reports are labeled by content type and region.	Frequently
Africa – State of Internet Freedom in Africa Report	Maps trends in government Internet controls over the last 20 years.	Annually
Africa – Digital Rights in Africa Report	Reports on digital rights in Africa relevant to surveillance technologies.	Annually
Amnesty International	Reports documented patterns of human rights abuse on various issues including surveillance. Reports are issue- and country-specific.	Frequently
The Citizen Lab	Website includes research on investigating digital espionage against civil society; documenting Internet filtering and other technologies and practices that impact freedom of expression online; analyzing privacy, security and information controls of popular applications; and examining transparency and accountability mechanisms relevant to the relationship between corporations and government agencies regarding personal data and other surveillance activities.	Frequently

[2] *This list of tools and guidance is a resource for consideration by U.S. businesses. It shouldn't be taken as comprehensive and does not signify an endorsement of these tools and guidance by the U.S. government.*

Information Source or Tool	Description	Frequency of Updates
Civicus	Maintains an interactive world map providing access to up-to-date information on civic space trends. Website also includes more in-depth reporting.	Frequently
Committee to Protect Journalists	Country reports document attacks on the press and obstructions to free press.	Annually
CYRILLA	Online database that facilitates sharing, comparison, and visualization of legal information on digital rights.	Monthly
Freedom in the World Report	Assesses the condition of political rights and civil liberties around the world. The report includes numerical ratings and descriptive text for 195 countries and 14 territories.	Annually
Freedom on the Net Report	Includes ranked country-by-country assessment of online freedom, a global overview of latest developments, and in-depth country reports. The report includes a color-coded map of countries reviewed showing whether they rank as free, partly free, or not free.	Annually
Global Network Initative (GNI) and Country Legal Framework Resource	The GNI Principles on Freedom of Expression and Privacy, together with its related Implementation Guidelines, provide guidance to the Internet and communications technology industry and its stakeholders in protecting and advancing the enjoyment of human rights globally. The Country Legal Framework Resource explores the legal environment affecting freedom of expression and privacy around the world.	Country Legal Framework – periodically, updates announced on the website
Global Surveillance Index	Compiles empirical data on AI surveillance use in 176 countries.	Issued September 2019
Human Rights Watch Country Reports	Reports and investigations on human rights abuses around the world.	Annually
Latin America - CELE	Analysis of legislation focused on freedom of expression and access to information in Latin America.	Frequently

Information Source or Tool	Description	Frequency of Updates
Ranking Digital Rights Corporate Indicators	Provides guidance to providers of digital platforms, services, and devices on public reporting regarding human rights, especially privacy and freedom of expression.	Annually
World Justice Project Rule of Law Index	Measures how the rule of law is experienced and perceived by the general public in 126 countries and jurisdictions worldwide.	Annually
Selected International Treaties, Principles, and Guidance		
International Covenant on Civil and Political Rights (ICCPR)	The ICCPR is an international human rights treaty adopted by the United Nations in 1966. The U.S. government ratified the treaty in 1992, obligating the U.S. government to protect and preserve human rights identified in the treaty, including the right to be free from arbitrary or unlawful interference with privacy and the right to freedom of expression.	Not applicable
OECD Guidelines for Multinational Enterprises	The OECD Guidelines for Multinational Enterprises are recommendations addressed by governments to multinational enterprises operating in or from adhering countries. They provide non-binding principles and standards for responsible business conduct in a global context consistent with applicable laws and internationally recognized standards. The Guidelines are the only multilaterally agreed and comprehensive code of responsible business conduct that governments have committed to promoting. The OECD Guidelines draw upon and are aligned with the UN Guiding Principles on Business and Human Rights. The U.S. government National Contact Point offers a dispute resolution and mediation mechanism when issues arise related to the OECD Guidelines.	Not applicable
OECD Due Diligence Guidance on Responsible Business Conduct	Building on the OECD Guidelines, in May 2018 the OECD released new Due Diligence Guidance for Responsible Business Conduct ("Guidance"). The Guidance elaborates on the due diligence responsibilities of businesses under the OECD Guidelines. It is intended to be used in all sectors of the economy and by all companies, regardless of size, geographical location, or value chain position. Its main objective is to help companies understand and implement due diligence responsibilities. The Guidance explicitly refers to risks and impacts, highlighting the need for companies to identify and address these risks and impacts and providing recommendations on how they can do this.	Not applicable

Information Source or Tool	Description	Frequency of Updates
UN Guiding Principles on Business and Human Rights	Endorsed by consensus by the UN Human Rights Council in 2011, the Guiding Principles are a set of global guidelines for States and business to prevent, address, and remedy human rights impacts that involve business enterprises.	Not applicable
UN Universal Periodic Review	The Universal Periodic Review (UPR) involves a review of the human rights records of all UN Member States. The UPR is a State-driven process under the auspices of the UN Human Rights Council, and provides the opportunity for each State to declare what actions they have taken to improve the human rights situations in their countries and to fulfill their human rights obligations.	Not applicable

APPENDIX 2 – EXAMPLES OF GOVERNMENT LAWS, REGULATIONS, & POLICIES THAT COULD RAISE CONCERNS

The below list is illustrative of the kinds of laws, regulations, and government policies that could place the product or service at a higher risk of misuse by governments that do not respect human rights and rule of law. The form of misuse will vary based on the kind of product or service involved in the transaction. Examples of risks include arbitrarily or unlawfully tracking movements, behaviors, and relationships among vulnerable groups, minority groups, activists, and journalists.

Concern	Example of Laws, Regulations, and Government Policies
Freedom of Expression	Criminal punishment for speech online on the basis that it is blasphemy/ apostasy, political/anti-government, defamation, anti-national, or toxic content.
	Blocking of content published online found objectionable for political reasons, without effective means to request review.
	No or severely restricted independent press, including targeting, harassment, threats, or physical attacks of journalists for their work.
Privacy	Allows governments to access domestic computer data and networks, copy information, and/or seize computers or any devices without appropriate safeguards (e.g., subject to review by an impartial and independent judiciary) against unreasonable or abusive government searches and seizures.
	Deploys domestically, city-wide, or nationwide surveillance or data collection technology without appropriate safeguards (e.g., subject to review by an impartial and independent judiciary) against unreasonable or abusive government searches and seizures.
	Allows governments to arbitrarily or unlawfully intercept and collect personal information of platform users on broad grounds such as terrorism and "extremism."
	Requires all cyber/Internet cafes to install software that tracks and stores information about their clients' online activities.
	Requires mandatory SIM card registration.
	Prohibits anonymous profiles on online messenger applications, social media accounts, and other technology driven platforms.
	Implements national or regional facial recognition programs to arbitrarily or unlawfully target individuals for exercising their human rights and fundamental freedoms, including freedom of expression.
	Requires Internet users to install software that enables government officials to arbitrarily or unlawfully monitor communications of all Internet users and block individual webpages.

Concern	Example of Laws, Regulations, and Government Policies
Restricting Civic Space/ Targeting Individuals or Members of Groups on the Basis of their Race, Sex, Language, Religion, Political Opinion, National Origin, or Any Other Grounds	Unduly burdensome procedures or requirements for nongovernmental organizations (NGO) to register with the government and/or no reasonable alternative to mandatory government registration for legal personhood.
	Requires NGOs to notify local and national governments about and/or obtain approval for all activities, and gain permission to travel between cities or host fundraisers, celebrations/commemorations, and demonstrations/protests.
	Imposes restrictions, limits, or bans on foreign funding of NGOs.
	Requires all domestic and international donor funding to NGOs to be funneled through a government office before reaching the NGO recipient.
	Uses spyware to monitor, censor, or block websites, apps, and other digital platforms that cater to a specific minority to target dissidents.
	Prosecutes civil society activists and journalists for exercising their human rights and for advocating on certain issues, under the guise of counterterrorism, national security, political stability, public or social order, national identity, or morality.
	Targeted, government-sponsored harassment, discrimination, or imprisonment of individuals or groups on the basis of identity or beliefs.
Total or Significant Control over Internet Service Providers or Telecommunications Networks	Requires companies to provide access to customers' data and Internet activities without appropriate safeguards against unreasonable or abusive government searches and seizures.
	Requires data to be stored on servers within the country without appropriate safeguards against unreasonable or abusive government searches and seizures.
	Requires all telecommunications operators to install surveillance equipment or comply with laws that allow government access to all transmitted information and other related data, without judicial or other appropriate oversight.
	Requires provider to modify service or product to facilitate government access to data without appropriate safeguards against unreasonable or abusive government searches and seizures.

Designed and Printed by A/GIS/GPS