
Human Rights Baseline Assessment for Small and Medium Sized Technology Companies

January 2020

Contents

Acknowledgements	01
Introduction	02
Using the tool	03
Understanding the landscape of human rights	04
Introductory questions	07
Assessing risks to privacy	14
Assessing risks to freedom of expression	20
Endnotes	28

Acknowledgements

We would like to thank Michaela Lee from Business for Social Responsibility and Evelyn Aswad from the University of Oklahoma College of Law for their support in reviewing and creating this human rights baseline assessment tool.

This tool was developed by New America's Open Technology Institute and Ranking Digital Rights as part of a consortium of organizations working on promoting business and human rights in the tech sector to advance internet freedom.

Introduction

Information and communication technologies, including the internet, have significantly changed how we communicate, coordinate and create, and share information. However, these technologies have also been found to pose significant risks to human rights, such as privacy and freedom of expression, as they often involve the vast collection of user data and can limit user speech.

When considering how to adequately safeguard human rights, it is particularly important to consider the role played by businesses. Although the private sector will understandably strive to innovate and further their bottom lines as they develop and dispatch new products and services, they also have a responsibility to respect and uphold human rights under the UN Guiding Principles on Business and Human Rights (UNGPs). There is also a strong business case for respecting human rights, as it fosters trust between businesses and their consumers and other stakeholders. The UNGPs are a set of guidelines, developed at the United Nations, for States and companies that aim to prevent, address, and remedy human rights abuses committed in the business sector.

According to the UNGPs, “the responsibility to respect human rights requires that business enterprises: (a) Avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur; (b) 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 this responsibility, businesses “should have in place policies and processes appropriate to their size and circumstances, including: (a) **A policy commitment** to meet their responsibility to respect human rights; (b) **A human rights due diligence process** to identify, prevent, mitigate, and account for how they address their impacts on human rights; (c) **Processes to enable the remediation of any adverse human rights impacts** they cause or to which they contribute” (emphasis added).

Businesses around the world can meet their responsibility to protect human rights by seeking to understand how their own products, services, and operations impact human rights. A human rights impact assessment is a process that can help facilitate this understanding.

Using the tool

This tool is designed to help small- and medium-sized technology companies (tech SMEs) assess the impact of their business operations on the rights to privacy and freedom of expression. This tool can help surface risks a company's operations may pose to the human rights of their users and other rights holders.

This "General Assessment" section of the assessment should take approximately three hours to complete and should include input from employees with expertise on various products or services, as well as with insight into corporate operations and policies. The answers you provide in this section will help inform whether and how you should respond to the questions in the subsequent "Privacy Assessment" and "Freedom of Expression Assessment" We welcome questions and are happy to offer support and guidance as you go through this process.

As your company, customers, and operational environments change, it is important to revisit this tool to ensure no lapse in your company's protection of human rights occurs. This tool has been designed to analyze impacts on privacy and freedom of expression, but it should not replace larger-scale or differently-focused impact assessments, which can provide a more comprehensive evaluation of how a company may affect the broader spectrum of human rights—such as with respect to supply chain issues, or which may address specific issues such as environmental or labor rights impacts. We recommend conducting such an impact assessment whenever there is a significant event that is likely to impact human rights. Such events might include when a new product, policy, or key business decision—such as entering a new market—is proposed, and when there are significant geopolitical or legislative changes in a country that a company is operating in (e.g. changes in domestic law or practices or regime changes). Impact assessment should be an ongoing practice that helps ensure that a company establishes and maintains its support and protections for human rights.

As mentioned, this impact assessment focuses primarily on privacy and freedom of expression. It should therefore serve as a starting point for tech SMEs to understand how they may interface with these two fundamental human rights that are most relevant to digital technologies.

Understanding the landscape of human rights

The first step in this assessment is to understand the range of human rights your company may impact through its products, services, and operations. Although this impact assessment will focus primarily on the right to privacy and the right to free expression, it is necessary to understand how those rights fit into the broader human rights landscape, as well as what the potential challenges associated with mitigating any human rights risks may be for your organization.

The [Universal Declaration of Human Rights](#), together with widely-adopted human rights treaties, sets out the key human rights that are globally accepted and should be contemplated. Take a look through these rights and think about what they may mean in relation to your business activities and the products or services that your company offers. You may want to pay special attention to cross-cutting rights such as the right to be free from discrimination and the right to equality before the law. Please also consider how your business activities, products, and services may impact the freedom of thought and religion, the right to education, and the right to participate in cultural life. Of particular concern, as elaborated further in this document and the other parts of this tool, are the rights to privacy and freedom of expression.

The right to privacy means that each individual has the right to not be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence. In addition, everyone has the right to the protection of the law against such interference or attacks. This right is enshrined in multiple international instruments and treaties. These include Article 12 of the United Nations Universal Declaration of Human Rights and Article 17 of the United Nations International Covenant on Civil and Political Rights.

Of particular importance for tech companies is the fact that the scope of the right to privacy includes personal information and data. Any collection, processing, or sharing of an individual's personal information or data will therefore have an impact on their right to privacy.

The right to freedom of expression means that every individual has the freedom to hold opinions without interference. In addition, each individual also has the right to seek, receive, and disseminate information and ideas using any media and format.

Any restrictions on speech must meet a rigorous three-part test: a restriction must be (1) provided by law—e.g. it must be easily available and must not be vague—and (2) necessary—e.g. the least restrictive means—to (3) achieve a legitimate public interest purpose—e.g. protection of the rights and reputations of others, public morals, public health, public order, or national security.

The right to freedom of expression is enshrined in multiple international instruments and treaties. These include Article 19 of the United Nations Universal Declaration of Human Rights and Article 19 of the United Nations International Covenant on Civil and Political Rights.

Of particular importance for tech companies is the fact that the right to freedom of expression includes online forms of expression, such as creating content on online platforms, and searching for/receiving information online. While providing opportunities for people to communicate and search for/receive information online can enhance their right to freedom of expression, restrictions can adversely impact this right.

Introductory questions

The following questions are designed to outline basic information about your company and its operations. They will also evaluate, at a high level, your engagement with human rights impact assessments thus far. You may be required to consult with other colleagues/teams in order to answer these questions:

1. What is the name of your company?

2. In what country or jurisdiction is your company headquartered?

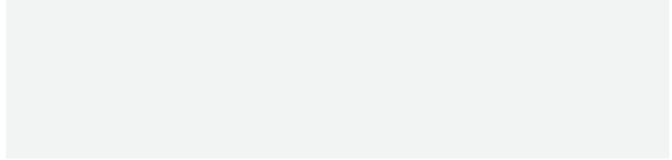
3. What other countries or jurisdictions does your company operate in? If your product or service is available globally, are there any countries that you affirmatively restrict access from?

4. Which of the following sectors does your company operate in? If any appropriate sector is not listed below, please select "other" and list your sector(s).

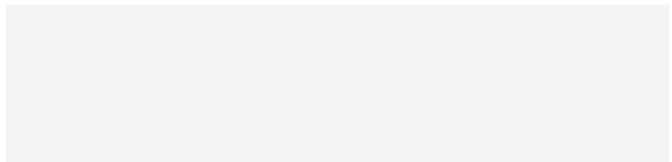
- Fintech
- Healthtech
- Edtech
- Consumer technology
- Social media
- News aggregation
- Other

- 5. Please set out a summary of the products and services, including subsidiaries, your company offers below:**

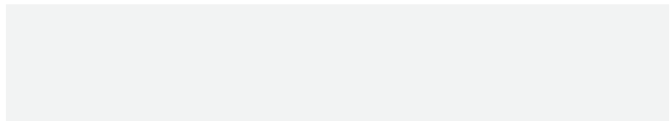
Products:



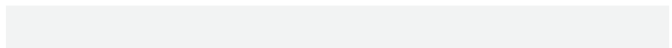
Services:



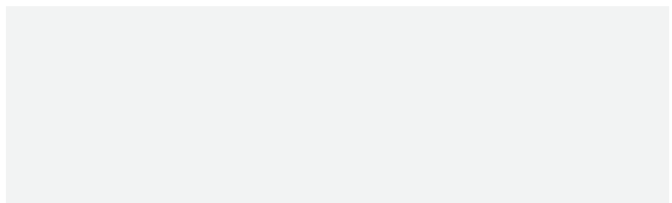
- 6. Has your company issued a public statement or policy that recognizes the need to respect human rights and commits to meet this responsibility? If yes, is it posted on your website? If not, where can it be found?**



- 7. Does your company have a designated employee or employee(s) responsible for human rights engagement?**



If yes, please list their name(s), a description of their role(s), and where they are situated in your organization/who they report to.



If no, please list any other individuals at your company who may have responsibilities relating to your company's potential impact on human rights (e.g. individuals working on public policy, external engagement, government affairs, legal compliance, labor/human resource issues, law enforcement liaison, data/consumer protection, etc.) and provide a description of their role(s) and where they are situated in your organization/who they report to.

- 8. Has your company conducted a human rights impact assessment or any type of rights-focused impact assessment before?**

- 9. If yes, which rights or principles did the assessment identify as potentially affected by your company's products, services, or operations? Describe the assessment and what actions were taken as a result.**

10. Are you aware of any limitations or challenging factors in the following categories that may hinder your ability to effectively meet the responsibility to respect human rights in any country in which you operate? If yes, please list these factors in the appropriate section below. If there are other limiting factors that are not covered by the suggested categories, please list them in the “other” category.

Domestic legislation in any country in which you operate:

Government, political pressure, or political conflict:

Conflict zones or violence:

Other:

- 11. Do you have any contacts with any external experts in any country in which you operate from any of the following categories that your company has consulted to help manage these challenges? If yes, please list these experts or organizations in the appropriate section below. If there are other experts or organizations that are not covered by the suggested categories, please list them in the “other” category.**

Domestic government:

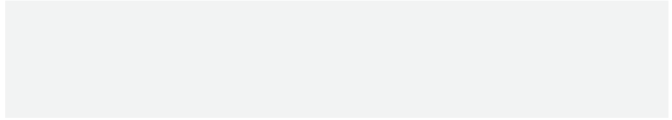
Foreign government:

Domestic civil society:

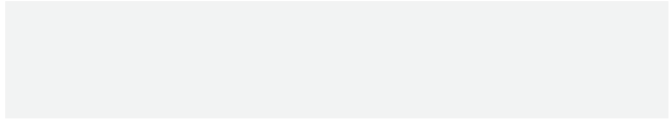
International civil society:

National human rights institutions:

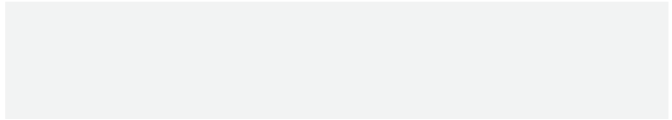
International human rights institutions:



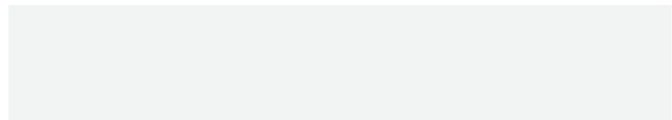
Multistakeholder initiatives:



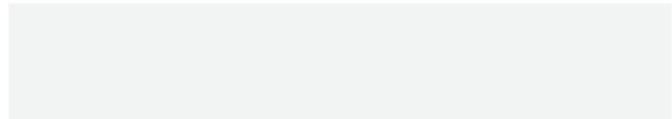
Academics:



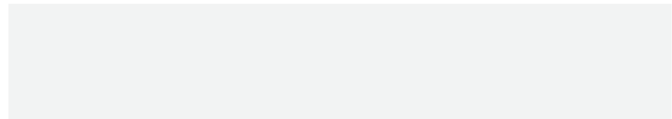
Consultants:



Business partners:



Other:



Assessing risks to privacy

The following questions are designed to help you assess at a high level whether your products, services, or operations engage with and potentially pose a risk to the right to privacy. You may be required to consult with a cross-functional set of teams in order to answer these questions.

Data Collection

1. **Does your company collect any information or data relating to, or generated by, your users?**

2. **If yes, please select the types of user data that your company collects:**

- Personal data (name, address, password, contact information, payment information)
- Communications content data (content of messages, emails, or other text-based communication; recordings of voice or video-based communications)
- Location data (GPS or other data identifying the location of a user)
- Biometric data (fingerprints, physical data like heart rate or other medical data)
- Network data
- Other data that users provide while using your product or service (search queries, metadata, subscriber information, data tracking usage, call/user logs, and others)

3. For what purposes do you collect this data?

4. Do you inform users about the types of data that are being collected and how the data will be used?

5. Are users required to opt in or do they have a meaningful opportunity to opt out of the collection of specific types of personal data?

Data Sharing

6. Do you share user data with any third parties?

a) Do you share data with government actors?

i) If yes, from which of the following parties do you receive these requests (select all that apply and list which particular entities). If there are parties that are not covered by the suggested categories, please list them in the "other" category.

- Government agencies (non-law enforcement)
- Law enforcement
- Individual government representatives
- Courts
- Other

b) Do you share data with non-government third parties?

If yes, for what purposes do you share this data?

Do third parties pay your company for the sharing of that user data?

7. Does your company have established policies or processes to guide when you share user data with third parties?

a) Please provide an outline of any relevant policies or processes.

b) Do you enter into any written agreements with third parties when engaging in such data sharing practices? If yes, do these written agreements contain safeguards for privacy?

c) Were these policies or processes created in consultation with legal counsel and/or external stakeholders?

d) Are these policies publicly available to your users? If yes, are these policies easily accessible to your users and are they written in user-friendly and easily comprehensible language?

8. Do you inform users more generally about what types of their data is shared and with whom?

9. Are users notified when their specific personal data is shared?

Data Security

10. Do you use any security best practices to protect user data?

a) Is the information you collect encrypted at rest and/or in transit?

b) Do you use any kind of authentication system to manage and limit employee access to that data?

c) Do you have structured notification mechanisms you would use to inform users if their data has been breached?

Assessing risks to freedom of expression

The following questions are designed to help you assess whether your products, services, or operations may impact and potentially infringe on the right to freedom of expression. You may be required to consult with other colleagues/teams in order to answer these questions.

General Risks to Free Expression

1. **Do your company's products or services permit users to create and share content or express themselves, either publicly or privately?**

2. **Do your company's products or services provide information or content without allowing for the production of user-generated content?**

3. **If you answered yes to questions 1 or 2, please select all of the following mechanisms in which your company facilitates the creation and sharing of content by users. If there are mechanisms that are not covered by the suggested categories, please list them in the "other" category.**

- The ability for users to publish videos, audio files, articles, or posts (please specify which)
- The ability for users to respond to existing content via comments or otherwise
- The ability for users to use online forums for discussion
- The ability for users to communicate with others, whether publicly or privately, in groups or one-on-one
- Other

4. **Have you ever used a methodology or rubric for evaluating the impact of your products, services, and practices on free expression? If so describe that methodology or rubric and explain what actions were taken as a result.**

5. **Does your company ever receive requests to delete, remove, or restrict any posting or other content or user expression?**

- a) If yes, from which of the following parties (select all that apply and list which particular entities). If there are parties that are not covered by the suggested categories, please list them in the “other” category.

- Law enforcement. *If yes, are these never, sometimes, or always accompanied with a court order?*

- Other (non-law enforcement) government agencies (please list the relevant countries these agencies are from as well). *If yes, are these never, sometimes, or always accompanied with a court order?*

- Individual government representatives. *If yes, are these never, sometimes, or always accompanied with a court order?*

- Directly from courts

- Internet Referral Units¹

- Users

- Trusted flaggers.² *If yes, please describe what your policy is on trusted flaggers.*

- Copyright holders

- Other

b) If yes, please indicate which of the following types of requests for content removal or restriction you have received. If there are types of requests that are not covered by the suggested categories, please list them in the “other” category.

- Legal requirements to remove or restrict content
- Government requests not based in domestic law to remove or restrict content
- Requests to remove or restrict content based on your company’s Terms of Service or Community Standards
- Requests to remove content based on copyright infringement claims
- Requests to remove content based on trademark infringement claims
- Requests to delist search results based on any “right to be forgotten”
- Requests to disrupt services
- Other

6. **Do you notify users whose content or accounts are subject to legal requests for content removal?**

Content Moderation

7. **If your company hosts or otherwise facilitates online content, does your company have established policies or rules in place that define unacceptable content or outline what types of content will be removed? *If yes, are these policies or rules publicly available?***

8. **Does your company use human moderators to review, remove, and restrict content (in addition to or instead of algorithmic or other automated processes)?**

9. **Does your company use automated tools to review, remove, restrict, and generally moderate content (in addition to or instead of human moderators)?**

Transparency Reporting

10. Does your company publish a transparency report detailing the scope and volume of content removals or account restrictions?

If yes,

Which of your products or services does this transparency report cover?

How often is this transparency report issued?

Please indicate which of the following types of requests for content removal or restriction are covered in the reports. If there are types of requests that are not covered by the suggested categories, please list them in the “other” category.

- Legal requests to remove or restrict content
- Requests to remove or restrict content based on your company’s Terms of Service or Community Standards
- Requests to remove content based on copyright infringement claims
- Requests to remove content based on trademark infringement claims
- Requests to delist search results based on a “right to be forgotten”
- Other

Providing Adequate Notice to Users

- 11. Has your company publicly committed to providing meaningful notice to users whose content has been removed or suspended, unless prohibited by law in very narrow or specific emergency situations, or if doing so would be ineffective?**

- 12. Does your company provide a notice to users who have had their content or accounts removed, restricted, or suspended?**

- 13. Does your company provide a notice to users who have flagged content or accounts for removal, restriction, or suspension?**

Appeals of Content Takedown Decisions

- 14. Does your company provide users with an appeals process to challenge decisions to moderate content?**

- 15. Do you offer users who have had their content or accounts removed, restricted, or suspended the opportunity to appeal these decisions?**

16. Do you offer users who have reported content or accounts for removal, restriction, or suspension the opportunity to appeal your decisions?

17. Are appeals reviewed by personnel who operate independently from those personnel who made the initial decision on removal? How does this process work?

18. How long does the appeals process take?

19. Do you have a public description of your appeals process and how users can invoke it?

Endnotes

1. Internet Referral Units are government-established agencies that flag content for removal to internet platforms based on the premise that they violate the company's Terms of Service/Community Standards.
2. Trusted Flaggers are individuals, NGOs, or government who have demonstrated particular effectiveness at flagging content for removal to internet platforms for violating their Terms of Service/Community Standards. Trusted Flaggers often have access to more robust content flagging tools such as bulk flagging.

Second Home
68 Hanbury St
London E1 5JL

+44 203 818 3258