CONSULTATION DRAFT
Human rights risk scenarios: Amazon and Alibaba

Note: The purpose of this document is to obtain expert and stakeholder feedback on the concepts, principles, and standards for company best practices that will inform our addition of two new companies—Amazon and Alibaba—in future iterations of the Ranking Digital Rights (RDR) Corporate Accountability Index. This document should be read after the *Rationale for RDR's Corporate Accountability Index expansion to include Amazon and Alibaba*, as it builds on concepts summarized in that overview. This document in turn should be read before the list of *Best Practices for Business and Human Rights: Amazon and Alibaba*, which are based on the *Risk Scenarios* outlined below.

All documents can be downloaded from the RDR website at: https://rankingdigitalrights.org/methodology-development/2021-revisions/#new-company-types.

What are human rights risk scenarios?

This document presents a range of different human rights risk scenarios, which are short narratives linking company practices to violations of human rights enumerated in the Universal Declaration of Human Rights (UDHR). These scenarios are derived from news reports or published research. They illustrate possible risks to freedom of expression or privacy that may result from using various Amazon and Alibaba services: namely, e-commerce platforms and personal digital assistants (like Alexa).[1] Mapping these scenarios enables us to identify best practices for companies to either prevent or mitigate the risk and severity of these harms. Best practices are in turn used as the basis for developing or adapting indicators to evaluate company disclosures of relevant policies and practices.

What is the scope of human rights harms?

As two of the world's largest digital platforms, Amazon and Alibaba's absence from the RDR Index represents a key gap in RDR's current ranking. There have been growing concerns about both companies' privacy practices and respect for human rights in general. Amazon collects an

[1] We use the term "personal digital assistant (PDA)" to refer to the artificial intelligence interface that powers and controls smart speakers and Internet of Things (IoT) devices, and which allows users to access both native services and third-party applications using voice or other commands. Examples of PDAs include Alexa (Amazon), AliGenie (Alibaba), Siri (Apple), the Google Assistant (Google), and Cortana (Microsoft).

enormous amount of information about people, notably through its e-commerce platform and through its dominance in the personal digital assistant (PDA) market. Alibaba's (mis)handling of user data, including its practice of sharing user data with its credit-scoring service and other third-party services without consent, has also raised concerns.

The risks to freedom of expression and privacy posed by PDAs are similar to those posed by mobile ecosystems.[2] There are concerns about the vast amounts of user information these devices collect, share, and retain, how that information is secured, and whether the company has processes in place for responding to law enforcement or other government requests to hand over user information. PDAs also act as gatekeepers to information, allowing users to orally ask queries of a search engine, seek out news content, and connect to other applications (for example, a user's email inbox or calendar). How the company decides and enforces its rules for governing its platform, and whether and how it will respond to third-party demands to remove or restrict access to content, applications, or user accounts, has serious implications for people's ability to exercise their rights to freedom of expression and information.

For e-commerce platforms, while the risks these platforms might pose to user privacy are clear, the risks to users' freedom of expression are less straightforward. We recognize that e-commerce platforms do not operate as a "digital public square" in the same way as social media platforms, and that the human rights risks that might stem from restricting access to content on an e-commerce platform (or alternatively, promoting some content over others) is qualitatively different than restricting access to content on a social media platform. At the same time, it is possible that risks to freedom of expression could become more pronounced if companies do not take active steps now to anticipate and mitigate them. For example, if Amazon.com is the only place users in a particular country can access books or materials about their government's history of oppressing ethnic or religious groups, and the government demands that Amazon withhold access to all of those books within the country, complying with such a demand has a significant impact on freedom of expression and opinion.

The risk scenarios below summarize risks to freedom of expression and privacy posed by both e-commerce platforms and PDAs. RDR's goal is to use these risk scenarios during the stakeholder consultation period to fully assess the scope of risks for these types of services, in order to better understand what adaptations or expansions to the methodology would need to be made in order to add Amazon and Alibaba to the next iteration of the RDR Corporate Accountability Index.

[2] RDR defines mobile ecosystems as "the indivisible set of goods and services offered by a mobile device company, comprising the device hardware, operating system, app store and user account." Read more here: "What do we mean by mobile ecosystems?," *Ranking Digital Rights*, September 2016.

Risk scenarios

A. Freedom of expression

Scenario 1: Company A introduces a new feature to its personal digital assistant which provides users with news highlights. However, it is not clear how the company determines which news source it derives its highlights from, and it does not disclose this to the user when asked. As a result, users do not have a clear understanding of how information is being delivered to them.

References:

- Alexa talks politics, but avoids Republicans, Democrats, and Trump

Human rights risks: Freedom of expression and information (UDHR art. 19). The situation described in this scenario poses a potential risk to freedom of expression because the company prioritize users personal interest based on their behavior over the right to freedom of expression, including the right to seek and impart information without giving users options to decide if they would like the company to do so.

Type of service:

- Personal digital assistants

Scenario 2: An e-commerce platform removes a store that sells digital security devices (e.g. security keys, privacy phone cases that protect users from surveillance etc.) or makes it unavailable in Country X. The e-commerce platform notifies the store owner about the removal but gives only very general information about what rule they violated without explaining which product broke the rule or how. As a result, human rights defenders based in Country X are prevented from purchasing these security devices because the only available source was taken down by the e-commerce platform. The e-commerce platform company did not explain to its customers (other users trying to access the page) the exact reasons for taking down the store.

References:

- Amazon seller forum post by HighFiveBuys
- Discussion of Alibaba product takedowns (in Chinese)

Human rights risks: Freedom of expression and information (UDHR art. 19) and the right to life, liberty and security of person (UDHR art. 3). The situation described in this scenario poses a potential risk to freedom of expression because the company fails to clearly disclose when it has taken an action in response to a government request, and offers no transparency about its process for responding to government requests to remove products from its platform. Further, the company is operating in a country where human rights defenders have limited access to

security devices essential for their own safety and work. Hence, by shutting down the store the company ends up risking the security of human rights defenders in Country X, which suggests that the company mays not carry out due diligence on third-party requests before deciding how to respond.

Type of service:

- E-commerce platforms

Scenario 3: An e-commerce platform sells people digital copies of a book but retains some form of control over the files after they have been downloaded (for example, through digital rights management software). The platform remotely deletes purchased copies of materials from a customer's device without notification or explanation.

Reference(s):

- Amazon Erases Orwell Books From Kindle
- Amazon wipes customer's Kindle and deletes account with no explanation

Human rights risks: Freedom of expression and information (UDHR art. 19).
The situation described in this scenario poses a potential risk to freedom of expression and opinion, including the right to seek and impart information. When e-commerce platforms retain the ability to restrict users' access to content they already purchased (for example, books or other published materials), their actions could make it greatly impossible or significantly more difficult for users to access that content.

Type of service:

- E-commerce platforms

Scenario 4: Company A filters or restricts certain voice or text-based search results and/or queries in compliance with local regulations and/or its own rules. However, the company does not provide comprehensive information about its own rules and how those are enforced, nor does it disclose the legal basis under which it might restrict or filter results for certain searches. As a result, users do not have a clear understanding of how their search results might be restricted or curated.

References:

- New Scrutiny on Censorship Issues for U.S. Companies in China
- China firms to curb 'harmful internet data'
- Apple Comes Under Fire After Siri Refuses to Provide Abortion Content
- Alexa, You Are a Goddamn Prude

Human rights risk: Freedom of expression and information (UDHR art. 19). The situation described in this scenario poses a potential risk to freedom of expression because a) the company is not clear about the circumstances under which it may restrict content or user accounts, b) the company fails to clearly disclose its process for responding to government requests and private requests to remove, filter, or restrict content or accounts. Hence, by arbitrary content restriction and blocking, the company undermines the right to freedom of expression of its users.

Types of services:

- E-commerce platforms
- Personal digital assistants

B. Privacy

Scenario 1: A company collects sensitive user information, such as voice recordings, transaction histories, etc, and retains that information without the users' knowledge. This information is inadvertently leaked or shared with a third party, either due to an action by the company or an inadvertent action by the user. Since the user was unaware that the company was retaining this type of sensitive information, they were unable to take necessary precautions to secure their information or prevent its collection.

References:

- Is Alexa Listening? Amazon Echo Sent Out Recording of Couple's Conversation

Human rights risk: Privacy (UDHR art. 12). The situation described in this scenario poses a risk to the right to privacy, as it pertains to the collection, retention, and disclosure of user information to third parties without the user's knowledge or consent. This could be of particular concern when the user information is disclosed to malicious actors or governments that may abuse their access to the data to target vulnerable groups and individuals such as human rights defenders and political dissidents. In addition, it is particularly concerning when the data is highly sensitive, detailed, and personal, such as a recording of a conversation inside one's home.

Types of services:

- Personal digital assistants
- E-commerce platforms (purchase histories, for example)

Scenario 2: A company or a service retains user data such as purchased items, reviews or audio files, despite the user deleting that information. The company retains that information for an unspecified period of time.

Reference(s):

- Amazon confirms it holds on to Alexa data even if you delete audio files

Human rights risk: Privacy (UDHR art. 12). The situation described in this scenario poses a potential risk to the right to privacy. When a company retains user information it no longer needs for a long or an unspecified period of time, it exposes that data to potential risks, including requests from law enforcement, data breaches, or company misuse. In addition, if a company allows a user to delete information, the information should actually be deleted from the company's records.

Types of services:

- Personal digital assistants
- E-commerce platforms

Scenario 3: A company collects and retains a large amount of personal data about its users. However, it fails to monitor or limit its employees' access to user data. The employees in turn can misuse that data, such as by selling it or making it available to others, or misusing it to surveil and abuse users.

References

- Amazon Workers Are Listening to What You Tell Alexa

Human rights risk: Privacy (UDHR art. 12). This scenario poses a risk to privacy by exposing users' information to employees who should not have access to it and don't need access to it in order to perform their jobs. Companies should minimize the number of people who have access to users' information and should have clear processes in place to minimize misuse, including strong whistleblowing mechanisms.

Types of companies/services

- Personal digital assistants
- E-commerce platforms

Scenario 4: A company or a service may be required by law enforcement agencies to hand over user data (with or without a court order or other form of judicial oversight, depending on the jurisdiction). This access can enable government authorities that lack sufficient legal constraints, accountability and/or independent oversight to surveil not only suspected criminals, but also political activists, human rights defenders, journalists and marginalized groups.

References:

- China's Tech Giants Have a Second Job: Helping Beijing Spy on Its People

Human rights risk: Privacy (UDHR art. 12). Users may not be aware of the types of information a company collects and retains, or how that might be used by law enforcement. This can present risks to the privacy of all users but can have especially dire consequences for religious or ethnic minorities or LGBTQ users who live in places where they may be targeted by others (including law enforcement) because of their identity, identities which could be revealed by the types of information companies collect.

Types of services:

- Personal digital assistants
- E-commerce platforms

Scenario 5: A company's personal digital assistant retains voice data to improve its voice recognition technology. The company hires contractors to listen to anonymized user audio clips for the purposes of improving their respective voice assistant's capabilities. While the company states that it does not sell users' personal information to anyone, it also states that there are some circumstances where it shares information with third parties. These circumstances, though, are not described in the company's privacy policy as it does not cover device-specific questions. As a result, users do not have sufficient information to understand the privacy risks of using the personal digital assistant, since they are not aware that these voice recordings are shared with contractors for the purpose of analyzing and improving the service.

References

- Amazon and Google are listening to your voice recordings. Here's what we know about that
- Amazon confirms it holds on to Alexa data even if you delete audio files
- Amazon Alexa 'keeps recordings of your voice forever' – and shares them with other companies too

Human rights risk: Privacy (UDHR art. 12). This scenario poses a risk to privacy because users may not be aware of the types of information a company collects and retains, how long it retains, whether it is shared with third parties, and if so with whom.

Type of service:

- Personal digital assistants

Scenario 6: Security researchers discovered a security vulnerability allowing them to send secret commands that undetectable to the human ear to a company's personal digital assistant. These commands, which the researchers embedded into recordings of music and spoken text, allowed them to secretly perform tasks such as dialing phone numbers, taking pictures and opening malicious websites.

References

- Alexa and Siri Can Hear This Hidden Command. You Can't.

Human rights risk: Privacy (UDHR art. 12). This scenario poses a risk to privacy. In the hands of malicious actors, this vulnerability could be exploited by individuals seeking access users' sensitive data in order to commit fraud, blackmail, or otherwise conduct unlawful surveillance for private or government clients.

Types of companies/services:

- Personal digital assistants

Stakeholder consultation: We welcome feedback on these consultation documents. Feedback from a wide range of experts and stakeholders is essential to our methodology development process, as we work to identify clear accountability standards that will encourage these companies to meet their obligations to respect and protect human rights. After receiving feedback from experts, human rights advocates, and companies on these documents and conducting further case study research, the risk scenarios, and best practices will be used to adapt the current methodology and will be tested in a pilot study.

Please send all feedback by **September 13, 2019** to methodology@rankingdigitalrights.org.