CONSULTATION DRAFT
Best practices for business and human rights: Amazon and Alibaba

Note: This document is the third in a series of three documents that are being shared for consultation regarding RDR's addition of new companies and services to the RDR Corporate Accountability Index. The purpose is to obtain expert and stakeholder feedback on the concepts, principles, and standards for company best practice that will in turn inform the possible inclusion of these companies and services in future editions of the RDR Index. This document should be read last, after the *Rationale for expanding the RDR Index to include Amazon and Alibaba* and *Human rights risk scenarios: Amazon and Alibaba*. It builds on the *Risk Scenarios*—short narratives linking company practices to human rights harms—to propose concrete accountability and transparency standards that companies should apply to mitigate these harms.

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

What are "best practices"?

In the context of the RDR Index methodology development process, "best practices" are normative statements ("should" statements) about what companies should do (or refrain from doing) in order to prevent or mitigate the risks identified in the *Human Rights Risk Scenarios* document. They will form the basis for *indicators* and *elements*, which are the building blocks of the RDR Index methodology. Elements must describe practices that are technically possible for a company to implement, they must be measurable by examining the company's publicly disclosed information, and there must be a way to benchmark the disclosures of different companies against one another. Here, the best practices are organized by service type, and then into two categories: freedom of expression and information, and privacy.

Please note that this is a draft document that will be subject to an iterative process of consultation, feedback, and revision. Best practices are intended as provocations to elicit feedback from participants in the consultation. We may ultimately determine that some of the best practices listed here are out of scope for RDR or would be too difficult to evaluate using publicly available information.

Best Practices

The best practices presented below are grouped by service type (e-commerce platforms and personal digital assistants) and then within those two groups, by two categories: Freedom of Expression and Information, and Privacy. Please note that many of these best practices are already reflected in the RDR Corporate Accountability Index methodology, and in these cases, we have added the corresponding indicator number from our current methodology as a reference.

E-commerce platforms

Freedom of expression and information

- Companies should have clear, publicly accessible policies that explain the circumstances under which they may take down or restrict access to a third-party seller's store, or restrict specific items in that store, such as books or other content (F3).

- Companies should have clear, publicly accessible policies that explain the circumstances under which they may restrict a user's access to digital content that the user has already purchased (F3).

- Companies should disclose all the methods or processes they use to enforce their own rules or to curate, restrict, or prioritize product listings (F3).

- Companies should clearly disclose and regularly publish data about the volume and nature of the actions they take to curate, restrict, or otherwise exercise editorial judgment over product listings, store pages, or accounts for any reason (F4).

- Companies should clearly disclose their processes for responding to government requests (including judicial orders) and private requests to remove, filter, or restrict store pages, products, content or accounts (F5, F6).

- Companies should clearly disclose that when they restrict access to products, store pages, or content, or place restrictions on accounts and third-party stores, they notify whoever created or controls them (F8).

- Companies should provide users with a clear mechanism to appeal the removal of their content, store page, or account (G6).

Privacy

- Companies should clearly disclose how they handle user information, including what is collected, for what purpose, how, with whom this information is shared, how long it is retained, and how it is used (P3-P9).

- Companies should clearly disclose to users what options they have to control their collection, retention, and use of user information (P7).

- Companies should clearly disclose their process for responding to requests from governments and other third parties to hand over user information, and should disclose data about the nature and volume of requests they receive and comply with (P10, P11).

- Companies should notify users to the extent legally possible when their information has been requested by governments and other third parties (P12).

- Companies should disclose information about the processes and methods they have in place to ensure the security of their products and the user information they retain, including systems to limit and monitor employee access to user information, and conducting security audits (P13).

- Companies should publicly disclose information about their processes for responding to data breaches (P15).

Personal digital assistants

Freedom of expression

- Companies should disclose all the methods they use to curate, restrict, or otherwise moderate the information and content presented to users by personal digital assistants (F3).

- Companies should clearly disclose the circumstances under which their personal digital assistant may withhold information from a particular source, and whether users are notified of the rules and default settings the platform uses to provide information (F3).

- Companies should clearly explain all situations in which their device may prevent users from performing a search (F3).

- Companies should regularly disclose data about the volume and nature of actions they take to curate, restrict, or otherwise exercise editorial judgment over content presented by their personal digital assistants (F4).

- Companies should clearly disclose that they notify affected users and third-party app developers when they restrict or remove content, third-party apps, or accounts (F8).

- Companies should clearly disclose all circumstances in which they may reject third-party apps from being accessed through a personal digital assistant (F3).

- Companies should clearly disclose their processes for responding to government requests (including judicial orders) and private requests to remove, filter, or restrict content, accounts, or third-party applications accessed through a personal digital assistant (F5).

Privacy

- Companies should clearly disclose how they handle user information, including what is collected, for what purpose, how, with whom this information is shared, how long it is retained, and how it is used (P3-P9).

- Companies should clearly disclose to users what options they have to control their collection, retention, and use of user information (P7).

- Companies should clearly disclose their process for responding to requests from governments and other third parties to hand over user information, and should disclose data about the nature and volume of requests they receive and comply with (P10, P11).

- Companies should notify users to the extent legally possible when their information has been requested by governments and other third parties (P12).

- Companies should disclose information about the processes and methods they have in place to ensure the security of their products and the user information they retain, including systems to limit and monitor employee access to user information, and conducting security audits (P13).

- Companies should address security vulnerabilities when they are discovered (P14).

- Companies should publicly disclose information about their processes for responding to data breaches (P15).

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.