Proposed revisions to the 2017 Corporate Accountability Index research methodology (consultation draft)

July 2016

Acknowledgements

While the entire Ranking Digital Rights team provided input and conducted consultations with stakeholders, the following team members carried out the bulk of the work in researching and implementing revisions for the new draft methodology:

- Priya Kumar, Research Analyst
- Nathalie Maréchal, Open Technology Fund Information Controls Fellow
- Revati Prasad, Annenberg COMPASS Fellow

Work by the Ranking Digital Rights team to revise the indicators and research methodology described in this document was supported by the following organizations:

- John D. and Catherine T. MacArthur Foundation
- Ford Foundation
- Open Society Foundations
- Open Technology Fund Information Controls Fellowship Program
- Annenberg COMPASS Fellowship Program

For a full list of project funders and partners, please see https://rankingdigitalrights.org/who/partners/.

About Ranking Digital Rights

Ranking Digital Rights (RDR) is a non-profit research initiative housed at New America's Open Technology Institute that works with an international network of partners to set global standards for how companies in the information and communications technology (ICT) sector should respect freedom of expression and privacy.

For more about RDR and its Corporate Accountability Index, please visit www.rankingdigitalrights.org.

For more about New America, please visit https://www.newamerica.org/.

For more about the Open Technology Institute, please visit https://www.newamerica.org/oti/.

Table of Contents

About the revised methodology

Ranking Digital Rights has developed the Index as an annual ranking, and we plan to publish new editions in 2017 and 2018. For 2017, RDR will expand the Index to cover companies that produce software and devices. Subsequent iterations may include companies that produce networking equipment. As a result, we have added new indicators and elements to account for the potential threats to users' freedom of expression and privacy that can arise from use of networked devices and software. The RDR team also further refined the methodology based on a detailed review of the raw data from the 2015 Index as well as consultations with stakeholders from civil society, academia, the investor community, and the companies themselves.

This redline document shows where we propose to make substantive revisions to the Index methodology. Three additional documents provide further detail on these revisions; they are available for download here: https://rankingdigitalrights.org/2016/07/05/new-draft-methodology/.

- A summary of the proposed revisions to the RDR research methodology
- A table comparing the 2015 indicators and the draft 2017 indicators
- A clean version of the draft revised RDR methodology research guidance, and glossary

The revised methodology is a draft, and we invite feedback on the proposed revisions. **The deadline to submit comments is Friday, August 5, 2016.** Comments should be sent via email to feedback@rankingdigitalrights.org.

G: Governance

The company demonstrates that it has governance processes in place to ensure that it respects the human rights to freedom of expression and privacy. Both rights are part of the Universal Declaration of Human Rights and are enshrined in the International Covenant on Civil and Political Rights. They apply online as well as offline. In order for a company to perform well in this section, the company's disclosure should at least follow, and ideally surpass, the UN Guiding Principles on Business and Human Rights and other industry-specific human rights standards focused on freedom of expression and privacy such as the Global Network Initiative.

G1. Policy Commitment

The company should publicly commit to respect users' human rights to freedom of expression and privacy.

1. Does the company make an explicit, clearly articulated **policy commitment**[1] to human rights, including freedom of expression and privacy?

Guidance: This indicator seeks evidence that the company has made public commitments about the importance of freedom of expression and privacy.

By policy commitment, we mean that the company's commitment should be part of a human rights policy document. This represents a formal statement that has gone through an evaluation process and has received approval at the highest levels of the company. General commitments or statements made in non-policy documents (e.g., CSR reports, webpages, blog posts, press releases) do not count.

Evaluation: We expect to see company commitments that explicitly and specifically address both freedom of expression and privacy. Companies whose policies mention only one will receive partial credit.

Potential sources:

- Company human rights policy
- Company annual report, sustainability report, etc.
- Company blog posts (with author clearly listed)

G2. Governance and management oversight

The company's senior leadership should exercise **oversight** of how its policies and practices affect freedom of expression and privacy.

Checklist elements (select all that apply):

1. Does the board of directors exercise formal oversight over how company practices affect freedom of expression and privacy?

[1] Definitions of terms in bold can be found in the glossary at the end of this document.

2. Does an **executive-level** committee, **team, program** or **officer** oversee how company practices affect freedom of expression and privacy?

3. Does a **management-level** committee, **team, program** or **officer** oversee how company practices affect freedom of expression and privacy?

Guidance: This indicator seeks company disclosure that the company's governance and internal management structures include consideration of freedom of expression and privacy. The decisions made by executives and managers of ICT companies significantly affect people's ability to experience freedom of expression and privacy. We expect these decision-making processes, and the chain of responsibility within the company, to explicitly consider these human rights.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist. At the board level, this oversight could include a board committee or another public explanation of how the board exercises oversight of freedom of expression and privacy. Below board-level, it can include a company unit or individual that reports to the executive or managerial level. The committee, program, team, officer, etc. should specifically identify freedom of expression and privacy in its description of responsibilities.

Potential sources:
- List of board of directors committees
- Company governance documents
- Company CSR/sustainability report
- Company organizational chart
- Company human rights policy

G3. Internal implementation

The company should have mechanisms in place to implement its commitments to freedom of expression and privacy within the company.

Checklist elements (select all that apply):

1. Does the company provide employee training on freedom of expression and privacy issues?

2. Does the company maintain an employee **whistleblower program** through which employees can report concerns related to how the company treats its users' freedom of expression and privacy rights?

Guidance: Indicator C2 focuses on company leaders and decision-makers. This indicator seeks company disclosure about how the company also helps the rest of its employees understand the importance of freedom of expression and privacy. When staffers write code for a new product, review a request for user data, or answer customer questions about how to use a service, they act in ways that can directly affect people's freedom of expression and privacy. We

expect companies to disclose information about whether they provide training that informs employees of their role in respecting human rights and that provides employees with an outlet to voice concerns they have regarding human rights.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist. Disclosure should specify that employee training and whistleblower programs covers freedom of expression and privacy.

Potential sources:

- Company code of conduct
- Employee handbook
- Company organizational chart
- Company CSR/sustainability report
- Company blog posts

G4. Impact assessment

The company should conduct regular, comprehensive, and credible due diligence, such as **human rights impact assessments**, to identify how all aspects of its business impact freedom of expression and privacy.

Checklist elements (select all that apply):

1. As part of its decision-making, does the company consider how laws affect freedom of expression and privacy in jurisdictions where it operates?

2. Does the company regularly assess free expression and privacy risks associated with existing products and services?

3. Does the company assess free expression and privacy risks associated with a new activity, including the launch and/or acquisition of new products or services or entry into new markets?

4. Does the company assess free expression and privacy risks associated with the processes and mechanisms used to enforce its Terms of Service?

5. Does the company conduct in-depth due diligence wherever the company's risk assessments identify concerns?

6. Do **senior executives** and/or members of the company's board of directors review and consider the results of assessments and due diligence in decision-making for the company?

7. Does the company conduct assessments on a regular schedule?

8. Are the company's assessment assured by an external third party?

9. Is the external third party that assures the assessment accredited to a relevant and reputable human rights standard by a credible organization?

Guidance: This indicator examines whether companies disclose the existence of any human rights impact assessment (HRIA) process including freedom of expression and privacy (See definition and references in Appendix 1.)

Note that this indicator does not expect companies to publish detailed results of their human rights impact assessments, since a thorough assessment includes sensitive information. Rather, it expects that companies should disclose that they conduct HRIAs and provide information on what their HRIA process encompasses.

While this indicator uses the language of human rights impact assessments, companies may use different names for this review process. What companies call their process is less important than what the process encompasses and accomplishes. This indicator will include a review of Privacy Impact Assessments (PIAs) and other assessment processes that contain characteristics or components listed in this indicator but are not necessarily called "human rights impact assessments."

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if they demonstrate that their assessment process addresses all elements in the checklist. If a company conducts HRIAs, but there is no public disclosure of the fact that it does so, the company will not receive credit.

Potential sources:

- Company CSR/sustainability reports
- Company human rights policy
- Regulatory documents (e.g., U.S. Federal Trade Commission)
- Reports from third-party assessors or accreditors
- Global Network Initiative assessment reports

G5. Stakeholder engagement

The company should **engage** with a range of **stakeholders** on freedom of expression and privacy issues.

Checklist elements (select all that apply):

1. Does the company initiate or participate in meetings with stakeholders that represent, advocate on behalf of, or are people directly and adversely impacted by the company's business?

2. Is the company a member of an industry organization that engages with non-industry and non-governmental stakeholders on freedom of expression and privacy?

3. Is the company a member of a **multi-stakeholder initiative** whose focus includes a commitment to upholding of freedom of expression and privacy based on international human rights principles.

Guidance: This indicator seeks evidence that company engages with its stakeholders, particularly those who face clear human rights risks in connection with their online activities. Engaging with stakeholders, particularly those who operate in high-risk environments, can be sensitive. A company may not feel comfortable publicly disclosing specific details about which stakeholders it consults, where or when they meet, and what they discuss. While we encourage companies to provide details about non-sensitive stakeholder engagement, we seek, at minimum, public disclosure that a company engages with stakeholders who are or represent users whose rights to freedom of expression and privacy are at risk. One way the public knows a company participates in this type of engagement is through its involvement in a multi-stakeholder initiative that brings the company in touch with representatives from various stakeholder groups including human rights organizations and others who advocate for the rights of at-risk groups.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if they demonstrate that their engagement efforts address all elements in the checklist.

Potential sources:

- Company CSR/sustainability report
- Company annual report
- Company blog
- Membership lists on the Global Network Initiative and Industry Dialogue websites
- Company FAQ or Help Center

G6. Remedy

The company should have **grievance** and **remedy** mechanisms to address users' freedom of expression and privacy concerns.

Checklist elements (select all that apply):

1. Does the company disclose its processes for receiving complaints?
2. Does the company make clear that its process includes complaints related to freedom of expression and privacy?
3. Does the company articulate its process for responding to complaints?
4. Does the company report on the number of complaints received?
5. Does the company provide evidence that it is responding to complaints, including examples of outcomes?

Guidance: This indicator examines whether companies provide remedy mechanisms and whether they have a publicly disclosed process for responding to complaints or grievance reports from individuals who believe that the company has violated or directly facilitated violation of their freedom of expression or privacy rights.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential sources:

- Company terms of service or equivalent user agreements
- Company content policies
- Company privacy policies, privacy guidelines, or privacy resource site
- Company CSR/sustainability report
- Company help center or user guide
- Company transparency report (for the number of complaints received)

F: Freedom of Expression

In its disclosed policies and practices, the company demonstrates concrete ways in which it respects the right to freedom of expression of users, as articulated in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and other international human rights instruments. The company's disclosed policies and practices demonstrate how it works to avoid contributing to actions that may interfere with this right, except where such actions are lawful, proportionate and for a justifiable purpose. Companies that perform well on this indicator demonstrate a strong public commitment to transparency not only in terms of how they respond to government and others' demands, but also how they determine, communicate, and enforce private rules and commercial practices that affect users' freedom of expression.

F1. Access to terms of service

The company should provide **terms of service** (ToS) that are easy to find and easy to understand.

Checklist elements (select all that apply):

1. Are the company's terms of service (ToS) easy to find?

2. Are the ToS available in the language(s) most commonly spoken by the company's users?

3. Are the ToS are presented in an understandable manner?

Guidance: The terms of service outline the relationship between the user and the company, and companies can take action against users based on the conditions described in the terms. Given this, we expect companies to ensure that users can easily locate the terms and to make an effort to help users understand what they mean.

A document that is "easy to find," should be located on the home page of the company or service, or at most, on a page that is one click away from the home page.

In addition, we expect a company to steps to help users understand the information presented in their documents. This includes, but is not limited to, providing summaries, tips, or guidance that explain what the terms mean, using section headers, readable font size, or other graphic features to help users understand the document, or writing the terms using readable syntax.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist. This indicator includes a review of other documents such as "community guidelines" or service-specific rules that further explain to users what the terms mean. Privacy policies are NOT included in this indicator since they are covered in separate indicators in the "Privacy" section.

Potential sources:

- Company terms of service, terms of use, terms and conditions, etc.
- Company acceptable use policy, community guidelines, rules, etc.

F2. Changes to terms of service

The company should provide meaningful **notice** and **documentation** to users when it changes its **terms of service**.

Checklist elements (select all that apply):

1. Does the company commit to notify users about changes to its terms of service?
2. Does the company disclose how it will directly notify users of changes?
3. Does the company disclose the timeframe within which it provides notification prior to changes coming into effect?
4. Does the company maintain a **public archive** or **change log**?

Guidance: It is common for companies to change their terms of service as their business evolves. We expect companies to commit to notify users when they change these terms and to provide users with information to understand what these changes mean. This indicator seeks company disclosure on the method and timeframe within which companies commit to notify users about changes in the terms of service. It also seeks evidence that a company provides publicly available records of previous terms so that people can understand how the company's terms have evolved over time. Regarding element 2, the method of direct notification may differ based on the type of service. For services that contain user accounts, direct notification may involve sending an email or an SMS. For services that do not require a user account, direct notification may involve posting a prominent notice on the main page where users access the service.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential sources:

- Company terms of service

F3. Content and account restriction

The company should explain the circumstances in which it may restrict **content** or **user accounts**.

Checklist elements (select all that apply):

1. Does the company explain what types of content or activities it does not permit?
2. Does the company explain why it may **restrict a user's account**?
3. Does the company disclose the mechanisms it uses to identify content or accounts that violate the company's rules?

4. Does the company disclose whether any non-government and non-judicial entities receive priority consideration when identifying content to be restricted for violating the company's rules, and if so, how that priority status is conferred?

5. Does the company explain its process for enforcing its rules?

6. Does the company provide examples to help the user understand what the rules are and how they are enforced?

Guidance: Companies often set boundaries for what content users can post on a service as well as what activities users can engage in on the service. Companies can also restrict a user's account, meaning that the user is unable to access the service. For **mobile ecosystems**, this can include an end-user's account or a **developer's** account. We expect companies to disclose what these rules are and how companies enforce them. This includes information about how companies learn of material or activities that violate their terms. For example, companies may employ staff to review content and/or user activity or they may rely on community flagging mechanisms through which other users flag content and/or activity for company review. We also expect companies to disclose the extent to which they have established relationships with private entities to notify them of such content or activities. For mobile ecosystems, we expect companies to disclose the types of apps they would restrict. In this disclosure, the company should also provide examples to help users understand what these rules mean.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential sources:

- Company Terms of Service, user contract, acceptable use policy, community standards, content guidelines, abusive behavior policy, or similar document that explains the rules users have to follow.
- Company support, help center, or FAQ (e.g., questions around why is content removed, why is an account suspended, etc.)

F4. User notification about content and account restriction

The company should **notify users** when it restricts **content** or **accounts**.

Checklist elements (select all that apply):

1. If the company hosts user-generated content, does the company commit to notify users who generated the content when it is restricted?

2. Does the company commit to notify users who attempt to access content that has been restricted?

3. In its notification, does the company include an explanation of the basis for the content restriction (legal or otherwise)?

4. Does the company commits to notify users when it restricts access to their account?

Guidance: Indicator F3 examines company disclosure of restrictions on what users can post or do on a service. This indicator, F4, focuses on whether companies disclose that they notify users when they take these types of actions. We expect companies to disclose a commitment to notify users when they have removed content, restricted a user's account, or otherwise restricted users' abilities to access a service. This disclosure should be part of companies' explanations of content and access restriction practices. **Mobile ecosystems** have two types of **users**: end-users and **third-party developers**. For mobile ecosystems, element 1 applies to third-party developers; element 2 applies to end-users, and elements 3 and 4 apply to both types of users.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential sources:

- Company Terms of Service, acceptable use policy, community standards, content guidelines, abusive behavior policy, or similar document that explains the rules users have to follow.
- Company support page, help center, or FAQ (e.g., questions around why is content removed, why is an account suspended, etc.)
- Company guidelines for developers
- Company human rights policy

F5. Data about terms of service enforcement

The company should regularly publish information about the volume and nature of actions taken to restrict **content** or **accounts** that violate the company's rules.

Checklist elements (select all that apply):

1. Does the company have a public reporting and disclosure framework that provides data about the volume and nature of content and accounts being restricted as part of terms of service enforcement?

2. Does the company reports this data at least once a year?

3. Does the data reported by the company can be exported as a **structured data** file?

Guidance: This indicator seeks company reporting on the number of instances a company has removed content or restricted users' access due to violations of the company's terms of service. Publicizing this data will provide the public with a more accurate view of the content removal ecosystem as well as companies' own role in content removal. We expect companies to regularly publish data about their own decisions to remove content.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential sources:

- Company transparency report

F6. Process for responding to government requests

The company should publish information about its process for responding to **government requests** (including judicial orders) to remove, filter, or restrict **content** or **accounts**.

Checklist elements (select all that apply):

1. Does the company explain its process for responding to **non-judicial government requests**?
2. Does the company explain its process for responding to **court orders**?
3. Does the company explain its process for responding to requests from foreign jurisdictions?
4. Do the company's explanations include the legal basis under which it may comply?
5. Does the company commit to carry out due diligence on requests before deciding how to respond?
6. Does the company commit to push back on unlawful government requests?
7. Does the company provide guidance or examples of implementation of its process?

Guidance: Companies increasingly receive requests to remove, filter, or restrict access to content. These requests can come from government agencies or courts–domestic and foreign. We expect companies to publicly disclose their process explaining how they respond to requests from governments and courts.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential sources:

- Company transparency report
- Company law enforcement guidelines
- Company terms of service
- Company help or support center
- Company blog posts

F7. Data about government requests

The company should regularly publish data about **government requests** (including judicial orders) to remove, filter, or restrict **content** or **accounts**.

Checklist elements (select all that apply):

1. Does the company break out the number of requests it receives by country?
2. Does the company list the number of accounts affected?
3. Does the company list the number of pieces of content or URLs affected?
4. Does the company list the types of subject matter associated with the requests it receives?
5. Does the company list the number of requests that come from different legal authorities?
6. Does the company list the number of requests it receives from governments to restrict content or accounts through unofficial processes?
7. Does the company list the number of requests it complied with?
8. Does the company publish the original requests or provide copies to a public third-party archive?
9. Does the company reports this data at least once a year?
10. Can the data be exported as a **structured data** file?

Guidance: This indicator examines company disclosure of data on the requests it receives from governments and courts to remove content. This includes requests related to content or activities that may violate local laws. Companies may receive these requests through official processes (e.g., a court order), or informal channels (e.g., a flagging system originally intended for private individuals to report content that violates the terms of service). If a company knows that a request is coming from a government entity or court, the company should disclose it as part of its government requests reporting. Publishing this data helps the public gain a greater understanding of how freedom of expression operates online, and it helps the public hold companies and governments accountable for their respective roles to respect and protect freedom of expression.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all the elements in the checklist.

In some cases, the law might prevent a company from disclosing information referenced in this indicator's elements. For example, we expect companies to publish exact numbers rather than ranges of numbers. We acknowledge that laws sometimes prevent companies from doing so, and researchers will document situations where this is the case. But a company will lose points if it fails to meet all elements. This represents a situation where the law causes companies to be uncompetitive, and we encourage companies to advocate for laws that enable them to fully respect users' rights to freedom of expression and privacy.

Potential sources:

- Company transparency report

F8. Process for responding to private requests

The company should publish information about its process for responding to **requests from private parties** to remove, filter, or restrict access to **content** or **accounts**.

Checklist elements (select all that apply):

1. Does the company explain its process for responding to requests made by private parties?

2. Do the company's explanations include the basis for complying with private requests?

3. Does the company commit to carry out due diligence on requests before deciding how to respond?

4. Does the company commit to push back on inappropriate private requests?

5. Does the company provide guidance or examples of implementation of its process?

Guidance: Companies increasingly receive requests to remove, filter, or restrict access to content. Previous indicators evaluate company disclosure on the requests they receive from governments. However, companies can also receive these requests from private entities, that is, non-governmental and non-judicial entities. This indicator focuses on private requests that come through some sort of defined or organized process. This can be a process established by law, (e.g., requests made under the U.S. Digital Millennium Copyright Act, the European Right to be Forgotten ruling, etc.) or a self-regulatory arrangement (e.g., company agreements to block certain types of images). This indicator does not examine company processes to review notices made under terms of service enforcement mechanisms; that is evaluated in indicator F3.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential sources:

- Company transparency report
- Company law enforcement guidelines
- Company terms of service
- Company policy on copyright or intellectual property
- Company help or support center
- Company blog posts

F9. Data about private requests

The company should regularly publish data about **private requests** to remove, filter, or restrict access to **content** or **accounts**.

Checklist elements (select all that apply):

1. Does the company break out the number of requests it receives by country?

2. Does the company list the number of accounts affected?
3. Does the company list the number of pieces of content or URLs affected?
4. Does the company list the reasons for removal associated with the requests it receives?
5. Does the company describe the types of parties from which it receives requests?
6. Does the company list the number of requests it complied with?
7. Does the company publish the original requests or provide copies to a public third-party archive?
8. Does the company reports this data at least once a year?
9. Can the data be exported as a **structured data** file?

Guidance: This indicator examines company disclosure of data on the requests it receives from private (non-governmental and non-judicial) parties to restrict content or accounts. This indicator focuses on private requests that come through some sort of defined or organized process. This can be a process established by law, (e.g., requests made under the U.S. Digital Millennium Copyright Act, the European Right to be Forgotten ruling, etc.) or a self-regulatory arrangement (e.g., company agreements to block certain types of images). This indicator does not examine company reporting on content or accounts restricted under terms of service enforcement mechanisms; that is evaluated in indicator F5.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential sources:

- Company transparency report

F10. Network management (telecommunications companies)

The company should commit not to **prioritize**, block, or delay certain types of traffic, **applications**, **protocols**, or **content** for any other reason beyond assuring quality of service and reliability of the network.

Checklist elements (select all that apply):

1. Does the company disclose that it does not prioritize, block, or delay certain types of traffic, applications, protocols, or content for reasons beyond assuring quality of service and reliability of the network?
2. If the company does engage in these practices, does it disclose its purpose for doing so?

Guidance: This indicator is only applicable to telecommunications companies. It seeks disclosure about whether companies engage in practices that affect the flow of content through their networks, such as **throttling** or **traffic shaping**. We expect companies to commit to avoid prioritization or degradation of content. If companies do engage in these actions, we expect them to publicly disclose this and to explain their purpose for doing so. Note that this indicator does not address blocking of content; that is addressed in indicator F3. This indicator does include company disclosure related to blocking of services, apps, or devices, which are considered a type of prioritization.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist. If a company explicitly discloses that it does not engage in the practices referenced in element 1, it will receive an N/A for element 2.

Potential Sources:

- Company explanation of network management or traffic management practices

F11. Network shutdown (telecommunications companies)

The company should explain the circumstances under which it may **shut down or restrict access to the network** or to specific **protocols**, services, or **applications** on the network.

Checklist elements (select all that apply):

1. Does the company explain the reason(s) why it may shut down service to a particular area or group of users (where applicable)?

2. Does the company explain why it may shut down or restrict access to specific applications or protocols (e.g., VoIP, messaging) in a particular area or to a specific group of users?

3. Does the company explain its process for responding to requests to shut down a network or restrict access to a service?

4. Does the company commit to push back on requests to shut down a network or restrict access to a service?

5. Does the company commit to notify users directly when it shuts down the network or restricts access to a service?

6. Does the company report on the number of network shutdown requests it receives?

7. Does the company provide specific examples of situations that may trigger shutdowns or restriction of service by the company?

Guidance: This indicator is only applicable to telecommunications companies. This indicator looks at company disclosure of restrictions on a user's ability to access a communications network or a service on the network. Telecommunications companies can shut down a network, or block specific services on it. We expect companies to explain to their users the

circumstances under which they might take such action and to report on the requests they receive to take such actions.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential Sources:

- Company Terms of Service, acceptable use policy, community standards, content guidelines, abusive behavior policy, or similar document that explains the rules users have to follow.
- Company transparency report
- Company law enforcement guidelines

F12. Identity policy (Internet, software, and device companies)

The company should not require users to verify their identity with identification connected to their government-issued identity.

1. Does the company require users to verify their identity with government-issued identification, or with other forms of identification connected to their government-issued identity?

Guidance: This indicator is applicable to Internet, software, and device companies. We expect companies to disclose whether they might ask users to verify their identities using government-issued ID or other forms of identification that could be connected to their offline identity. We acknowledge that users may have to provide information that could be connected to their offline identity in order to access paid features of various products and services. To receive full credit on this indicator, users should be able to access features that don't require payment without needing to provide information that can be tied to their offline identity.

Evaluation: A company will receive full credit if its answer is "No," and a company will receive no credit if its answer is "Yes."

Potential sources:

- Company terms of service or equivalent document
- Company help center
- Company sign up page

P: Privacy

In its disclosed policies and practices, the company demonstrates concrete ways in which it respects the right to privacy of users, as articulated in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and other international human rights instruments. The company's disclosed policies and practices demonstrate how it works to avoid contributing to actions that may interfere with users' privacy, except where such actions are lawful, proportionate and for a justifiable purpose. They will also demonstrate a strong commitment to protect and defend users' digital security. Companies that perform well on this indicator demonstrate a strong public commitment to transparency not only in terms of how they respond to government and others' demands, but also how they determine, communicate, and enforce private rules and commercial practices that affect users' privacy.

P1. Access to privacy policies

The company should provide **privacy policies** that are easy to find and easy to understand.

Checklist elements (select all that apply):

1. Are the company's privacy policies easy to find?
2. Are the privacy policies available in the language(s) most commonly spoken by the company's users?
3. Are the policies presented in an understandable manner?
4. (For **mobile ecosystems**): Does the company require **apps** made available through its **app store** to provide users with a privacy policy?

Guidance: Privacy policies address how companies collect, manage, use, and secure information about users as well as information provided by users. Given this, we expect companies to ensure that users can easily locate the policy and to make an effort to help users understand what they mean.

A document that is "easy to find," should be located on the home page of the company or service, or at most, on a page that is one click away from the home page.

In addition, we expect a company to steps to help users understand the information presented in their documents. This includes, but is not limited to, providing summaries, tips, or guidance that explain what the terms mean, using section headers, readable font size, or other graphic features to help users understand the document, or writing the terms using readable syntax.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist. Terms of Service are NOT included in this indicator since they are covered in separate indicators in the "Freedom of Expression" section.

Potential sources:

- Company privacy policy, data use policy

P2. Changes to privacy policies

The company should provide meaningful **notice** and **documentation** to users when it changes its **privacy policies**.

Checklist elements (select all that apply):

1. Does the company commit to notify users about changes to its privacy policies?
2. Does the company disclose how it will directly notify users of changes?
3. Does the company disclose the time frame within which it provides notification prior to changes coming into effect?
4. Does the company maintain a **public archive** or **change log**?
5. (For **mobile ecosystems**): Does the company require **apps** sold through its **app store** to notify users when the app changes its privacy policy?

Guidance: It is common for companies to change their privacy policies as their business evolves. We expect companies to commit to notify users when they change these policies and to provide users with information to understand what these changes mean. This indicator seeks company disclosure on the method and timeframe within which companies commit to notify users about changes in the privacy policies. It also seeks evidence that a company provides publicly available records of previous policies so that people can understand how the company's policies have evolved over time. Regarding element 2, the method of direct notification may differ based on the type of service. For services that contain user accounts, direct notification may involve sending an email or an SMS. For services that do not require a user account, direct notification may involve posting a prominent notice on the main page where users access the service.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential sources:

- Company privacy policy, data use policy

P3. Collection of user information

The company should disclose what **user information** it **collects** and how.

Checklist elements (select all that apply):

1. Does the company commit to limit collection of user information to what is directly relevant and necessary to accomplish the purpose of its service?

2. Does the company provide evidence that it only collects user information that is directly relevant and necessary for the service?

3. Does the company clearly disclose what user information it collects?

4. For each type of user information the company collects, does the company clearly disclose how it collects user information?

5. (For **mobile ecosystems**): Does the company evaluate whether third-party **apps** made available through its **app store** limit collection of user information to what is directly relevant and necessary to accomplish the purpose of the app?

6. (For **mobile ecosystems**): Does the company evaluate whether the privacy policy of third-party **apps** made available through its **app store** discloses what user information the apps collect?

Guidance: We expect companies to clearly disclose what user information they collect and how they do so. We also expect companies to commit to the principle of **data minimization** and demonstrate how this principle shapes their practices regarding user information. If companies collect multiple types of information, we expect them to provide detail on how they handle each type of information. For mobile ecosystems, we expect companies to determine whether the apps that are available on their app store also adhere to practices that respect users' privacy.

The term "user information" appears in many indicators throughout this section. RDR takes an expansive interpretation of what constitutes user information:

"User information is any data that is connected to an identifiable person, or may be connected to such a person by combining datasets or utilizing data-mining techniques."

As further explanation, user information is any data that documents a user's characteristics and/or activities. This information may or may not be tied to a specific user account. This information includes, but is not limited to, personal correspondence, user-generated content, account preferences and settings, log and access data, data about a user's activities or preferences collected from third parties either through behavioral tracking or purchasing of data, and all forms of metadata. User information is never considered anonymous except when included solely as a basis to generate global measures (e.g. number of active monthly users). For example, the statement, 'Our service has 1 million monthly active users,' contains anonymous data, since it does not give enough information to know who those 1 million users are.

Anonymous data is "data that is in no way connected to another piece of information that could enable a user to be identified."

The expansive nature of this view is necessary to reflect several facts. First, skilled analysts can de-anonymize large data sets. This renders nearly all promises of anonymization unattainable. In essence, any data tied to an "anonymous identifier" is not anonymous; rather, this is often pseudonymous data that may be tied back to the user's offline identity. Second, metadata may be as or more revealing of a user's associations and interests than content data, thus this data is of vital interest. Third, entities that have access to many sources of data, such as data brokers and governments, may be able to pair two or more data sources to reveal information

about users. Thus, sophisticated actors can use data that seems anonymous to construct a larger picture of a user.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

In some cases, laws or regulations might require companies to collect certain information or might prohibit or discourage the company from disclosing what user information they collect. Researchers will document situations where this is the case, but a company will still lose points if it fails to meet all elements. This represents a situation where the law causes companies to be uncompetitive, and we encourage companies to advocate for laws that enable them to fully respect users' rights to freedom of expression and privacy.

Potential sources:

- Company privacy policy
- Company webpage or section on data protection or data collection

P4. Sharing of user information

The company should disclose what **user information** it **shares** and with whom.

Checklist elements (select all that apply):

1. Does the company clearly disclose what user information it shares?
2. For each type of user information the company shares, does the company provide a detailed description of the types of third parties with which it shares that information?
3. Does the company disclose that it may share user information with government(s) or legal authorities?
4. The company clearly discloses why it shares user information.
5. The company provides a detailed description of the types of third parties with which it shares user information.
6. Does the company disclose the names of all third parties with which it shares user information and explain what information it shares with each third party?
7. (For **mobile ecosystems**): Does the company evaluate whether the privacy policy of third-party **apps** made available through its **app store** discloses what user information the apps share?
8. (For **mobile ecosystems**): Does the company evaluate whether the privacy policy of third-party **apps** made available through its **app store** discloses the types of third parties with whom it shares user information?

Guidance: We expect companies to clearly disclose what user information they share and to provide enough detail so that users can understand the scope of this sharing. We expect company disclosure to address company sharing of user information with governments and with commercial entities. If companies collect multiple types of information, we expect them to provide detail on how they handle each type of information. For mobile ecosystems, we expect companies to determine whether the apps that are available on their app store also adhere to practices that respect users' privacy.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

In some cases, laws or regulations might require companies to share certain information or might prohibit or discourage the company from disclosing what user information they share. Researchers will document situations where this is the case, but a company will still lose points if it fails to meet all elements. This represents a situation where the law causes companies to be uncompetitive, and we encourage companies to advocate for laws that enable them to fully respect users' rights to freedom of expression and privacy.

Potential sources:

- Company privacy policy
- Company policies related to sharing data, interaction with third parties

P5. Purpose for collecting and sharing user information

The company should clearly disclose why it **collects** and **shares user information**.

Checklist elements (select all that apply):

1. For each type of user information the company collects, does the company clearly disclose its purpose for collection?

2. Does the company clearly disclose its purpose for combining user information between other company services or services?

3. For each type of user information the company shares, does the company clearly disclose its purpose for sharing?

4. Does the company commit to limit its use of user information to the purpose for which it was collected?

Guidance: We expect companies to clearly disclose why they collect and share user information. In addition, many companies own or operate a variety of products and services, and we expect companies to clearly disclose how user information can be shared or combined across services. Finally, companies should commit to the principle of **use limitation**, which is part of the OECD privacy guidelines, among other frameworks. If companies collect multiple types of information, we expect them to provide detail on how they handle each type of information.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential Sources:

- Company privacy policy
- Company webpage or section on data protection or data collection

P6. Users' control over information

The company should clearly disclose to users what **options they have to control** the company's **collection**, **retention** and use of their information?

Checklist elements (select all that apply):

1. For each type of user information the company collects, does the company disclose whether users can control the company's collection of their information?

2. For each type of user information the company collects, does the company provide users with options to delete that information?

3. Does the company provide users with options to control how their information is used to target advertising?

4. Does the company clearly explain how users can control whether their information is used for targeted advertising?

5. (For **mobile ecosystems**): Does the company provide users with options to control the **device's geolocation** functions?

Guidance: We expect companies to proactively provide users with options to control what user information the company collects and retains. Users should be able to access these options after they sign up for the service, not simply at the time of sign-up. Simply signing up for the service does not represent consent. In addition, we expect companies to enable users to control the use of their information for a specific purpose – targeted advertising. This particular use of information requires extensive collection and retention of user information, which makes it tantamount to tracking. With regard to mobile ecosystems, we expect companies to enable users to control the collection of location information in particular. A user's location changes frequently and many users carry their mobile devices nearly everywhere, making the collection of this type of information particularly sensitive. In addition, the location settings on mobile ecosystems can influence a user's ability to control how other products and services access her location information.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist. We expect companies to disclose what the options to control are, rather than simply disclose that the users have options.

Potential sources:

- Company privacy policy

- Company account settings page

P7. Users' access to their own information

Companies should allow users to obtain all of the **information** about them that the company holds.

Checklist elements (select all that apply):

1. Does the company allow users to obtain a copy of their information?
2. Does the company disclose what information users can obtain?
3. Does the company allow users to obtain their information in a structured data format?
4. Does the company allow users to obtain all public-facing and private information a company holds about them?
5. (For **mobile ecosystems**): Does the company evaluate whether the privacy policy of third-party **apps** made available through its **app store** discloses that users can obtain all of the information about them the app holds?

Guidance: We expect companies to give users the ability to obtain copies of their information that the company holds. Company disclosure should explain what data this record contains and what formats users can obtain it in. For mobile ecosystems, we expect companies to determine whether the apps that are available on their app store also adhere to practices that respect users' privacy.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential sources:
- Company privacy policy
- Company account settings
- Company help center
- Company blog posts

P8. Retention of user information

The company should clearly disclose how long it **retains user information**.

Checklist elements (select all that apply):

1. For each type of user information the company collects, does the company disclose how long it retains that information?

2. Does the company disclose that it deletes all user information after users terminate their account?

3. Does the company disclose the time frame in which it will delete user information after users terminate their account?

4. Does the company disclose what **de-identified** user information it retains?

5. Does the company clearly disclose the process it uses to **de-identify** user information?

6. (For **mobile ecosystems**): Does the company evaluate whether the privacy policy of third-party **apps** made available through its **app store** discloses how long it retains user information?

7. (For **mobile ecosystems**): Does the company evaluate whether the privacy policy of third-party **apps** made available through its **app store** discloses that the all user information is deleted when users terminate their accounts or delete the app?

Guidance: We expect companies to disclose how long they retain user information and the extent to which they remove identifiers from user information they retain. Users should also be able to understand what happens when they delete their accounts. Companies who choose to retain user information for extended periods of time should take steps to ensure that data is not tied to a specific user. Acknowledging the ongoing debates about the efficacy of de-identification processes, and the growing sophistication around re-identification practices, we still consider de-identification a positive step that companies can take to protect the privacy of their users. If companies collect multiple types of information, we expect them to provide detail on how they handle each type of information. For mobile ecosystems, we expect companies to determine whether the apps that are available on their app store also adhere to practices that respect users' privacy.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

In some cases, laws or regulations might require companies to retain certain information for a given period of time. Researchers will document situations where this is the case, but a company will still lose points if it fails to meet all elements. This represents a situation where the law causes companies to be uncompetitive, and we encourage companies to advocate for laws that enable them to fully respect users' rights to freedom of expression and privacy.

P9. Collection of user information from third parties (Internet companies)

The company should publish clear information about its practices with regard to **collecting user information** from third parties through technical means.

Checklist elements (select all that apply):

1. Does the company clearly explain how it collects user information from third parties through technical means?

2. Does the company clearly state what user information it collects from third parties through technical means?

3. Does the company clearly state how it uses the information it collects from third parties through technical means?

4. Does the company clearly state how long it retains information it collects from third parties through technical means?

5. Does the company respect **user-generated signals** to opt-out of data collection?

Guidance: We expect companies to disclose what user information they collect from third parties, which in this case typically means collecting information from third-party websites, apps, etc. This helps users understand how their activities outside the service can affect their use of the service.

One prominent user-generated signal is the "**Do Not Track**" standard.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential sources:
- Company privacy policy
- Company policy on third parties

P10. Process for responding to third-party requests for user information

The company should publish information about its process for responding to **requests from governments** and other **third parties** for **user information**.

Checklist elements (select all that apply):

1. Does the company explain its process for responding to **non-judicial government requests**?

2. Does the company explain its process for responding to **court orders**?

3. Does the company explain its process for responding to **requests made by private parties**?

4. Does the company explain its process for responding to requests from foreign jurisdictions?

5. Do the company's explanations include the legal basis under which it may comply?

6. Does the company commit to carry out due diligence on requests before deciding how to respond?

7. Does the company commit to push back on unlawful requests?

8. Does the company provide guidance or examples of implementation of its process?

Guidance: Companies increasingly receive requests from third parties – especially governments but sometimes other parties or entities – to turn over data about users or the contents of their communications. This indicator covers requests from government agencies, courts, and private parties. We expect companies to publicly disclose their process explaining how they respond to requests from each type of third party.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

In some cases, the law might prevent a company from disclosing information referenced in this indicator's elements. Researchers will document situations where this is the case, but a company will still lose points if it fails to meet all elements. This represents a situation where the law causes companies to be uncompetitive, and we encourage companies to advocate for laws that enable them to fully respect users' rights to freedom of expression and privacy.

Potential sources:

- Company transparency report
- Company law enforcement guidelines
- Company privacy policy
- Company blog posts

P11. User notification about third-party requests for user information

The company should commit to **notify** users to the extent legally possible when their **information** has been **requested by governments** and **other third parties**?

Checklist elements (select all that apply):

1. Does the company commit to notify users when government entities (including courts or other judicial bodies) request their user data?

2. Does the company commit to notify users when non-government entities request their user data?

3. Does the company discloses situations when it might not notify users, including a description of the types of government requests it is prohibited by law from disclosing to users?

Guidance: We expect companies to disclose a commitment to notify users, when legally possible, in cases where third parties request data about users. We acknowledge that this notice may not be possible in legitimate cases of an ongoing investigation; however, companies should explain this to users.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential sources:

- Company transparency report
- Company law enforcement guidelines

P12. Data about third-party requests for user information

The company should regularly publish data about **government** and other **third-party** requests for **user information**.

Checklist elements (select all that apply):

1. Does the company list the number of requests it receives by country?
2. Does the company list the number of requests it receives for stored user information and for **real-time communications access**?
3. Does the company list the number of accounts affected?
4. Does the company list whether a demand sought communications **content** or **non-content** or both?
5. Does the company identify the specific legal authority or type of legal process through which law enforcement and national security demands are made?
6. Does the company include requests that come from **court orders**?
7. Does the company list the number of requests it receives from private parties?
8. Does the company list the number of requests it complied with, broken down by category of demand?
9. Does the company list what types of government requests it is prohibited by law from disclosing?
10. Does the company report this data at least once per year?
11. Can the data reported by the company be exported as a **structured data** file?

Guidance: This indicator examines company reporting on the government and other third party requests companies receive for users' data.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

In some cases, the law might prevent a company from disclosing information referenced in this indicator's elements. For example, we expect companies to publish exact numbers rather than ranges of numbers. We acknowledge that laws sometimes prevent companies from doing so, and researchers will document situations where this is the case. But a company will lose points if it fails to meet all elements. This represents a situation where the law causes companies to be

uncompetitive, and we encourage companies to advocate for laws that enable them to fully respect users' rights to freedom of expression and privacy.

Potential sources:

- Company transparency report

P13. Security oversight

The company should disclose information about its institutional processes to ensure the security of its products and services.

Checklist elements (select all that apply):

1. Does the company disclose that it has systems in place to limit and monitor employee access to user information?

2. Does the company have a security team that conducts security audits on the company's products and services?

3. Does the company commission third-party security audits on its products and services?

Guidance: Companies have access to immense amounts of information about users, and they should take the highest possible measures to keep this information secure. Just as companies should clearly disclose their oversight processes related to freedom of expression and privacy, they should also provide general information about their oversight processes to keep user information secure.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential sources:

- Company privacy policies
- Company security guide

P14. Addressing security vulnerabilities

The company should address security **vulnerabilities** when they are discovered.

Checklist elements (select all that apply):

1. Does the company have a mechanism through which **security researchers** can submit vulnerabilities they discover?

2. Does the company disclose the timeframe in which it will review reports of vulnerabilities?

3. Does the company commit not to pursue legal action against researchers trying to find security flaws in the company's software?

4. (For **mobile ecosystems**) Does the company disclose that **software updates**, security **patches**, add-ons, or extensions are downloaded over an **encrypted** channel?

5. (For **mobile ecosystems** and telecommunications companies) Does the company disclose what, if any, **modifications it has made to a mobile operating system**?

6. (For **mobile ecosystems** and telecommunications companies) Does the company disclose what, if any, effect such modifications have on the company's ability to send **security updates** to users?

7. (For **mobile ecosystems**) Does the company disclose the date through which it will continue to provide **security updates** for the **device**/**OS**?

8. (For **mobile ecosystems**) Does the company commit to provide **security updates** for the **operating system** and other **critical software** for a minimum of five years after release?

9. (For **mobile ecosystems**) Does the company enable users to receive **security updates** without providing user information?

10. (For **mobile ecosystems** and telecommunications companies) If the company uses an operating system adapted from an existing system, does the company commit to provide security **patches** within one month of a vulnerability being announced to the public?

Guidance: Computer code is not perfect. When companies learn of vulnerabilities that could put users and their information at risk, they should take action to mitigate those concerns. This includes ensuring that people are able to share any vulnerabilities they discover with the company. We believe it is especially important for companies to provide clear disclosure to users about the manner and time period in which users will receive security updates. In addition, since telecommunications providers can alter open-source mobile operating systems, we expect them to disclose information that may affect a user's ability to access these critical updates.

Evaluation:
This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist. Elements 1-3 are assessed for all companies. Elements 4-10 are assessed for mobile ecosystems. Elements 5-6 and 10 are also assessed for telecommunications companies.

Potential Sources:
- Company privacy policies
- Company security guide
- Company "help" forums

P15. Encryption of user communication and private content (Internet, software, and device companies)

The company should **encrypt** user communication and private **content** so users can control who has access to it.

Checklist elements (select all that apply):

1. Does the company disclose that the transmission of user communications is encrypted by default?

2. Does the company disclose that transmissions of user communications are encrypted using unique keys?

3. Does the company enable users to secure their content using end-to-end encryption?

4. Does the company disclose that end-to-end encryption is enabled by default?

Guidance: This indicator is applicable to Internet, software, and device companies. Users entrust significant amounts of their content to online services. Companies should enable users to easily encrypt this data and dramatically increase its security.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential sources:

- Company terms of service or privacy policy
- Company security guide
- Company help center
- Company sustainability reports
- Official company blog and/or press releases

P16 Account Security (Internet, software, and device companies)

The company should help users keep their **accounts** secure.

Checklist elements (select all that apply):

1. Does the company disclose that it deploys advanced authentication methods to prevent fraudulent access?

2. Does the company allow users to view their recent account activity?

3. Does the company commit to notify users about unusual account activity and possible unauthorized access to the account?

Guidance: This indicator is applicable to Internet, software, and device companies. Companies should provide users with tools that enable them to secure their accounts and to know when their accounts may be compromised.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential Sources:

- Company security center
- Company help pages or community support page
- Company account settings page
- Company blog

P17. Inform and educate users about potential threats

The company should publish information to help users defend against **cyber threats**.

1. Does the company publish practical materials that educate users on how to protect themselves from cyber threats relevant to their services?

Guidance: Companies hold significant amounts of user information, making them targets for malicious actors. We expect companies to help users protect themselves against such threats. Companies should present this guidance to the public using clear language, ideally paired with visual images, designed to help users understand the nature of the threats companies and users can face.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist.

Potential sources:

- Company security center
- Company help pages or community support page
- Company blog

Glossary

Note: This is not a general glossary. The definitions and explanations provided below were written specifically to guide researchers in evaluating ICT companies on this project's research indicators.

Account / user account – A collection of data associated with a particular **user** of a given computer system, service, or platform. At a minimum, the user account comprises a user name and password, which are used to authenticate the user's access to his/her data.

Account restriction / restrict a user's account – Limitation, suspension, deactivation, deletion, or removal of a specific user account or permissions on a user's account.

Anonymous data — Data that is in no way connected to another piece of information that could enable a user to be identified.

The expansive nature of this definition used by the Ranking Digital Rights project is necessary to reflect several facts. First, skilled analysts can de-anonymize large data sets. This renders nearly all promises of anonymization unattainable. In essence, any data tied to an "anonymous identifier" is not anonymous; rather, this is often pseudonymous data which may be tied back to the user's offline identity. Second, metadata may be as or more revealing of a user's associations and interests than content data, thus this data is of vital interest. Third, entities that have access to many sources of data, such as data brokers and governments, may be able to pair two or more data sources to reveal information about users. Thus, sophisticated actors can use data that seems anonymous to construct a larger picture of a user.

App – A self-contained program or piece of software designed to fulfill a particular purpose; a software application, especially as downloaded by a user to a mobile device.

App store — The platform through which a company makes its own apps as well as those created by third-party developers available for download. An app store (or app marketplace) is a type of digital distribution platform for computer software, often in a mobile context.

Change log — A record that depicts the specific changes in a document, in this case, a terms of service document.

Collect / Collection – All means by which a company may gather information about users. A company may collect this information directly from users, for example, when users submit user-generated content to the company. A company may also collect this information indirectly, for example, by recording log data, account information, metadata, and other related information that describes users and/or documents their activities.

Content – The information contained within wire, oral, or electronic communications (e.g., a conversation that takes place over the phone or face-to-face, the text written and transmitted in an SMS or email).

Core functionality — The most essential functions or affordances of a product or service. For example, a smartphone's core functionality would include making a receiving phone calls, text messages and emails, downloading and running apps, and accessing the Internet.

Court orders – Orders issued by a court. They include court orders in criminal and civil cases.

Critical (software) update — A widely released fix for a product-specific, security-related vulnerability. Security vulnerabilities are rated by their severity: critical, important, moderate, or low.

Cyber threat – The process by which a malicious actor (including but not limited to criminals, insiders, or nation states) may gain unauthorized access to user data using hacking, phishing, or other deceptive techniques.

Data minimization – According to the European Data Protection Supervisor (EDPS), "The principle of 'data minimization' means that a data controller ["the institution or body that determines the purposes and means of the processing of personal data"] should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose. In other words, data controllers should collect only the personal data they really need, and should keep it only for as long as they need it."

Source: European Data Protection Supervisor, Data Protection Glossary, https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/74

De-identified – This refers to user information that companies collect and retain, but only after removing or obscuring any identifiable information from it. This explicit identifiers like names, email addresses and any government-issued ID numbers, as well as identifiers like IP addresses, cookies and unique device numbers.

Documentation – The company provides records that users can consult.

Do Not Track – Also known by the acronym "DNT", this refers to a setting in a user's browser preferences which tells entities not to "track" them. In other words, every time a user loads a website, any parties that are involved in delivering the page (of which there are often many, primarily advertisers) are told not to collect or store any information about the user's visit to the page. However, this is merely a polite request – a company may ignore a DNT request, and many do.

Developer/third-party developer — An individual (or group of individuals) who creates a software program or application that is distributed through a company's app store.

Device/handheld device/mobile device — A physical object, such as a smartphone or feature phone, used to access telecommunication networks that is designed to be carried by the user and used in a variety of locations.

Encryption – This essentially hides the content of communications so only the intended recipient can view it. The process uses an algorithm to convert the message (plaintext) into a coded format (ciphertext) so that the message looks like a random series of characters to anyone who looks at it. Only someone who has the appropriate encryption key can decrypt the message, reversing the ciphertext back into plaintext. Data can be encrypted when it is stored and when it is in transmission.

For example, users can encrypt the data on their hard drive so that only the intended recipient with the encryption key can decipher the contents of the drive. Additionally, users can send an

encrypted email message, which would prevent anyone from seeing the email contents while the message is moving through the network to reach the intended recipient. With encryption in transit (for example visible when a website uses HTTPS), the communication between a user and a website is encrypted, so that outsiders, such as the user's Internet Service Provider can only see the initial visit to the website, but not what the user communicates on that website, or the sub-pages that the user visits.

For more information, see this resource: http://www.explainthatstuff.com/encryption.html

Executive-level oversight – The executive committee or a member of the company's executive team directly oversees issues related to freedom of expression and privacy.

Geolocation — Identification of the real-world geographic location of an object, such as a radar source, mobile phone or Internet-connected computer terminal. Geolocation may refer to the practice of assessing the location, or to the actual assessed location.

Government requests – This includes requests from government ministries or agencies, law enforcement, and court orders in criminal and civil cases.

Grievance – "[A] perceived injustice evoking an individual's or a group's sense of entitlement, which may be based on law, contract, explicit or implicit promises, customary practice, or general notions of fairness of aggrieved communities." (p. 32 of 42.)

Source: "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy Framework," 2011, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

Human Rights Impact Assessments (HRIA) – For the purpose of this methodology, HRIAs are a systematic approach to due diligence. A company carries out these assessments or reviews to see how its products, services, and business practices affect the freedom of expression and privacy of its users.

For more information about Human Rights Impact Assessments and best practices in conducting them, see this special page hosted by the Business & Human Rights Resource Centre: https://business-humanrights.org/en/un-guiding-principles/implementation-tools-examples/implementation-by-companies/type-of-step-taken/human-rights-impact-assessments

The Danish Institute for Human Rights has developed a related Human Rights Compliance Assessment tool (https://hrca2.humanrightsbusiness.org), and BSR has developed a useful guide to conducting a HRIA: http://www.bsr.org/en/our-insights/bsr-insight-article/how-to-conduct-an-effective-human-rights-impact-assessment

For guidance specific to the ICT sector, see the excerpted book chapter ("Business, Human Rights and the Internet: A Framework for Implementation") by Michael Samway on the project website at: http://rankingdigitalrights.org/resources/readings/samway_hria

Also see Part 3 Section 2 on assessment in the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights: http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr-sme/csr-ict-hr-business_en.pdf

Location data — Information collected by a network or service about where the user's phone or other device is or was located – for example, tracing the location of a mobile phone from data collected by base stations on a mobile phone network.

Malware — An umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software

Management-level oversight – A committee, program, team, or officer that is not part of the company's board of directors or the executive team.

Mobile ecosystem — The indivisible set of goods and services offered by a mobile device company, comprising the device hardware, operating system, app store and user account.

Modifications to a mobile operating system — Changes made to the stock version of a mobile OS that may affect core functionality, the user experience, or the process of deploying software updates.

Multi-stakeholder initiative – A credible multi-stakeholder organization includes and is governed by members of at least three other stakeholder groups besides industry: civil society, investors, academics, at-large user or customer representatives, technical community, and/or government. Its funding model derives from more than one type of source (corporations, governments, foundations, public donations, etc.). Its independence, rigor, and professionalism are of a high standard, with strong participation by human rights organizations that themselves have solid track records of independence from corporate and/or government control. The Global Network Initiative is an example of a multi-stakeholder initiative focused on freedom of expression and privacy.

Non-content – Data about an instance of communication or about a user. Companies may use different terms to refer to this data, including metadata, basic subscriber information, non-content transactional data, account data, or customer information. The Guardian has a useful guide with examples of what counts as metadata on various services.

In the U.S., the Stored Communications Act defines non-content customer communications or records as, "name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity (including any temporarily assigned network address); and means and source of payment for such service (including any credit card or bank account number)." The European Union's Handbook on European Data Protection Law states, "Confidentiality of electronic communications pertains not only to the content of a communication but also to traffic data, such as information about who communicated with whom, when and for how long, and location data, such as from where data were communicated."

http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=1100110

Non-judicial government requests – These are requests that come from government entities that are not judicial bodies, judges, or courts. They can include requests from government

ministries, agencies, police departments, police officers (acting in official capacity) and other non-judicial government offices, authorities, or entities.

Notice / Notify – The company communicates with users or informs users about something related to the company or service.

Officer – A senior employee accountable for an explicit set of risks and impacts, in this case privacy and freedom of expression.

Operating system (OS) — The software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals. A mobile operating system is the OS for a mobile device such as a smartphone or tablet.

Options to control – The company provides the user with a direct and easy-to-understand mechanism to opt-in or opt-out of data collection, use, or sharing. “Opt-in” means the company does not collect, use, or share data for a given purpose until users explicitly signal that they want this to happen. “Opt-out” means the company uses the data for a specified purpose by default, but will cease doing so once the user tells the company to stop. Note that this definition is potentially controversial as many privacy advocates believe only “opt-in” constitutes acceptable control. However, for the purposes of RDR, we have elected to count “opt-out” as a form of control.

Oversight / Oversee – The company’s governance documents or decision-making processes assign a committee, program, team, or officer with formal supervisory authority over a particular function. This group or person has responsibility for the function and is evaluated based on the degree to which it meets that responsibility.

Patch — A piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually called bugfixes or bug fixes, and improving the usability or performance.

Platform — A computing platform is, in the most general sense, whatever a pre-existing piece of computer software or code object is designed to run within, obeying its constraints, and making use of its facilities. The term computing platform can refer to different abstraction levels, including a certain hardware architecture, an operating system (OS), and runtime libraries.[1] In total it can be said to be the stage on which computer programs can run.

Policy commitment – The company’s commitment should be part of a human rights policy document. This represents a formal statement that has gone through an evaluation process and has received approval at the highest levels of the company. General commitments or statements made in non-policy documents (e.g., CSR reports, webpages, blog posts, press releases) do not count.

Privacy policies – Documents that outline a company’s practices involving the collection and use of information, especially information about users.

Source: “Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,” U.S. Federal Trade Commission, March 2012, p. 77.

https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

Private requests – Requests made by any person or entity that is not acting under direct governmental or court authority. Private requests for content restriction can come from a self-regulatory body such as the Internet Watch Foundation, or a notice-and-takedown system, such as the U.S. Digital Millennium Copyright Act. For more information on notice-and-takedown, as well as the DMCA specifically, see the recent UNESCO report, "Fostering Freedom Online: The Role of Internet Intermediaries" at http://unesdoc.unesco.org/images/0023/002311/231162e.pdf (p. 40-52 of 211).

Prioritization – Prioritization occurs when a network operator "manage[s] its network in a way that benefits particular content, applications, services, or devices." For RDR's purposes, this definition of prioritization includes a company's decision to block access to a particular application, service, or device.

Source: U.S Federal Communications Commission's 2015 Open Internet Rules, p. 7 of 400, https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf

Protocol — A set of rules governing the exchange or transmission of data between devices.

Public archive – A publicly available resource that contains previous versions of the terms of service or comprehensively explains each round of changes the company makes to its terms of service.

Real-time communications access – Surveillance of a conversation or other electronic communication in "real time" while the conversation is taking place, or interception of data at the very moment it is being transmitted. This is also sometimes called a "wiretap." Consider the difference between a request for a wiretap and a request for stored data. A wiretap gives law enforcement authority to access future communications, while a request for stored data gives law enforcement access to records of communications that occurred in the past. The U.S. government can gain real-time communications access through the Wiretap Act and Pen Register Act, both part of the Electronic Communications Privacy Act (ECPA); the Russian government can do so through "System for Operative Investigative Activities" (SORM).

For more information on how wiretaps and pen registers affected online communications under the USA Patriot Act (through May 2015), see the following sections of the ACLU webpage "Surveillance Under the USA Patriot Act":

Expansion of the "pen register" exception in wiretap law
"Nationwide" pen register warrants
Pen register searches applied to the Internet
Source: https://www.aclu.org/surveillance-under-usa-patriot-act?redirect=national-security/surveillance-under-usa-patriot-act

Remedy – "Remedy may include apologies, restitution, rehabilitation, financial or non-financial compensation and punitive sanctions (whether criminal or administrative, such as fines), as well as the prevention of harm through, for example, injunctions or guarantees of non-repetition. Procedures for the provision of remedy should be impartial, protected from corruption and free from political or other attempts to influence the outcome." (p. 22 of 27.)

Source: "Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie. Guiding

Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework," 2011.
http://business-humanrights.org/sites/default/files/media/documents/ruggie/ruggie-guiding-principles-21-mar-2011.pdf

Also see: the Telco Remedy Plan by Access:
https://s3.amazonaws.com/access.3cdn.net/fd15c4d607cc2cbe39_0nm6ii982.pdf

Retention of user information – A company may collect data and then delete it. If the company does not delete it, the data is "retained." The time between collection and deletion is the 'retention period'. Such data may fall under our definition of 'user information', or it may be anonymous. Keep in mind that truly anonymous data may in no way be connected to a user, the user's identity, behavior or preference, which is very rare.

A related topic is the 'retention period'. For example, a company may collect log data on a continual basis, but purge (delete) the data once a week. In this case, the data retention period is one week. However, if no retention period is specified, the default assumption must be that the data is never deleted, and the retention period is therefore infinite. In many cases users may wish for their data to be retained while they are actively using the service, but would like it to be deleted (and therefore not retained) if and when they quit using the service. For example, users may want a social network service to keep all of their private messages, but when the user leaves the network they may wish that all of their private messages be deleted.

Roll out — A series of related product announcements that are staged over time; the process of making patches, software updates, and software upgrades available to end users.

Security researcher — Someone who studies how to secure technical systems and/or threats to computer and network security in order to find a solution.

Security update — A widely released fix for a product-specific, security-related vulnerability. Security vulnerabilities are rated by their severity: critical, important, moderate, or low.

Security vulnerability — A weakness which allows an attacker to reduce a system's information assurance. A vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

Senior executives – CEO and/or other members of the executive team as listed by the company on its website or other official documents such as an annual report. In the absence of a company-defined list of its executive team, other chief-level positions and those at the highest level of management (e.g., executive/senior vice president, depending on the company) are considered senior executives.

Shares / Sharing – The company allows a third party to access user information, either by freely giving the information to a third party (or the public, or other users) or selling it to a third party.

Shut down or restrict access to the network: For the purpose of this methodology, network shutdown refers to the intentional disruption of internet or electronic communications, including telecom services such as cellular telephony and SMS. This includes a blanket shut down of all cellular or internet services within a geographic area and targeted blocking of specific services, such as social media or messaging apps.

Access Now has developed a crowd-sourced definition of an internet shutdown and leads a campaign to highlight the human rights implications of the growing practice. "An intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information."

https://www.accessnow.org/keepiton/

Software update — A software update (also sometimes called a software patch) is a free download for an application or software suite that provides fixes for features that aren't working as intended or adds minor software enhancements and compatibility. An update can also include driver updates that improve the operation of hardware or peripherals, or add support for new models of peripherals.

Software upgrade — A software upgrade is a new version of a piece of software that offers a significant change or improvement over the current version.

Stakeholders – People who have a "stake" because they are affected in some way by a company's actions or decisions.

Note that stakeholders are not the same as "rights holders" and that there are different kinds of stakeholders: those who are directly affected, and "intermediary stakeholders" whose role is to advocate for the rights of direct stakeholders.

Rights holders are the individuals whose human rights could be directly impacted. They interact with the company and its products and services on a day-to-day basis, typically as employees, customers, or users.

Intermediary stakeholders include individuals and organizations informed about and capable of speaking on behalf of rights holders, such as civil society organizations, activist groups, academics, opinion formers, and policymakers." (p. 10 of 28).

Source: Stakeholder Engagement in Human Rights Due Diligence: Challenges and Solutions for ICT Companies by BSR, Sept. 2014
http://www.bsr.org/reports/BSR_Rights_Holder_Engagement.pdf

Stakeholder Engagement – Interactions between the company and stakeholders. Companies or stakeholders can initiate these interactions, and they can take various formats, including meetings, other communication, etc.

Stock Android — The version of the Android operating system that is made available by Google, without any modifications to the code. Can refer to any version of the operating system (ie Kit Kat, Marshmallow, etc).

Structured data – "Data that resides in fixed fields within a record or file. Relational databases and spreadsheets are examples of structured data. Although data in XML files are not fixed in location like traditional database records, they are nevertheless structured, because the data are tagged and can be accurately identified." Conversely, unstructured data is data that "does not reside in fixed locations. The term generally refers to free-form text, which is ubiquitous.

Examples are word processing documents, PDF files, e-mail messages, blogs, Web pages and social sites."

Sources: PC Mag Encyclopedia

"structured data" http://www.pcmag.com/encyclopedia/term/52162/structured-data

"unstructured data" http://www.pcmag.com/encyclopedia/term/53486/unstructured-data

Team / Program – A defined unit within a company that has responsibility over how the company's products or services intersect with, in this case, freedom of expression and/or privacy.

Terms of Service – This document may also be called Terms of Use, Terms and Conditions, etc. The terms of service "often provide the necessary ground rules for how various online services should be used," as stated by the EFF, and represent a legal agreement between the company and the user. Companies can take action against users and their content based on information in the terms of service.

Source: Electronic Frontier Foundation, "Terms of (Ab)use" https://www.eff.org/issues/terms-of-abuse

Third party – A "party" or entity that is anything other than the user or the company. For the purposes of this methodology, third parties can include government organizations, courts, or other private parties (e.g., a company, an NGO, an individual person). (Note that this is an intentionally broad and inclusive definition.)

Throttling – A blunt form of traffic shaping in which a network operator slows the flow of packets through a network. Mobile operators may throttle traffic to enforce data caps.

For more information, see: Open Signal, "Data throttling: Why operators slow down your connection speed," http://opensignal.com/blog/2015/06/16/data-throttling-operators-slow-connection-speed/

Traffic shaping – Adjusting the flow of traffic through a network. This can involve conditionally slowing certain types of traffic. Traffic shaping can be used for network management purposes (e.g., prioritizing VoIP traffic ahead of normal web traffic to facilitate real-time communication) or for reasons that counter net neutrality principles (e.g., intentionally slowing video traffic to dissuade users from using high-bandwidth applications).

Use/Purpose Limitation: The OECD privacy guidelines state that entities that work with user information should state their purpose for colleting such data and should not use the data for any other purpose, unless they receive consent from the user or if the use is legally authorized.

Source: OECD Privacy Guidelines, Part Two: Basic Principles of National Application, p. 14 https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Users – Individuals who use a product or service. This includes people who post or transmit the content online as well as those who try to access or receive the content. For indicators in the freedom of expression category, this includes third-party developers who create apps that are housed or distributed through a company's product or service.

User data – Content or non-content data about users and their communications (see definitions of “content” and “non-content” for more details). Note that indicators P9-P11 use the term “user data” to match the language used in companies’ “transparency reports” regarding third-party requests for information about users. The rest of this methodology uses the term “user information,” as defined below, when referring to information a company has pertaining to a specific user.

User-generated signals – Many companies allow users to “opt-out” of tracking by setting an array of company-specific cookies. If a user deletes cookies in order to protect privacy, they are then tracked until they re-set the “opt-out” cookie. Furthermore, some companies may require a user to install a browser add-on to prevent tracking. These two common scenarios are example of users being forced to use signals which are company-specific; and therefore do not count. Rather, a user-generated signal comes from the user and is a universal message that the user should not be tracked. The primary option for user-generated signal today is the “Do Not Track” header (covered above), but this wording leaves the door open to future means for users to signal they do not want to be tracked.

User Information — Any data that is connected to an identifiable person, or may be connected to such a person by combining datasets or utilizing data-mining techniques. As further explanation, user Information is any data that documents a user’s characteristics and/or activities. This information may or may not be tied to a specific user account. This information includes, but is not limited to, personal correspondence, user-generated content, account preferences and settings, log and access data, data about a user’s activities or preferences collected from third parties either through behavioral tracking or purchasing of data, and all forms of metadata. User Information is never considered anonymous except when included solely as a basis to generate global measures (e.g. number of active monthly users). For example, the statement, ‘Our service has 1 million monthly active users,’ contains anonymous data, since it does not give enough information to know who those 1 million users are.

Whistleblower program – This is a program through which company employees can report any alleged malfeasance they see within the company, including issues related to human rights. This typically takes the form of an anonymous hotline and is often the responsibility of a chief compliance or chief ethics officer.