2018 Corporate Accountability Index

Research Indicators

Including Indicator guidance and definitions

July 2017

Acknowledgements

The following Ranking Digital Rights team members worked on the preparation of the 2018 Corporate Accountability Index methodology:

- Amy Brouillette, Research and Editorial Manager
- Laura Reed, Senior Research Analyst
- Nathalie Maréchal, Senior Research Fellow
- Priya Kumar, Senior Research Fellow

For a full list of project staff:
https://rankingdigitalrights.org/who/

We wish to thank Nat Meysenburg at Open Technology Institute for his input on the 2018 Index methodology. We also wish acknowledge former Ranking Digital Rights team members for their work in developing the 2015 and 2017 Index methodologies: Priya Kumar, Research Analyst; Allon Bar, Policy and Engagement Manager; Nathalie Maréchal, Senior Research Fellow, Ranking Digital Rights; Revati Prasad, PhD candidate, Annenberg School for Communication, University of Pennsylvania.

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/.

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

Table of Contents

About the Corporate Accountability Index

Ranking Digital Rights (RDR) produces a Corporate Accountability Index that ranks the world's largest internet, mobile, and telecommunications companies' disclosed commitments and policies affecting users' freedom of expression and privacy. The Index is a standard-setting tool aimed at encouraging companies to abide by international principles and standards safeguarding freedom of expression and privacy.

The standards the Index uses to measure companies build on more than decade of work by the human rights, privacy and security communities. These standards include the UN Guiding Principles on Business and Human Rights, which affirm that just as governments have a duty to protect human rights, companies also have a responsibility to respect human rights. The Index also builds on the Global Network Initiative principles and implementation guidelines, which address ICT companies' specific responsibilities towards freedom of expression and privacy in the face of government demands to restrict content or hand over user information. It further draws on a body of emerging global standards and norms around data protection, security, and access to information. The data and analysis produced by the Index informs the work of human rights advocates, policymakers, and responsible investors and is used by companies to improve their own policies and practices.

The Index methodology

The RDR Corporate Accountability Index was developed over three years of research, testing, consultation, and revision. Since its inception, the project has engaged closely with researchers around the globe. For methodology development, pilot study, and the inaugural Index we also partnered with Sustainalytics, a leading provider of ESG (environmental, social, and governance) research to investors.

In 2015, RDR launched its inaugural Index, which ranked 16 internet and telecommunications companies.

For the 2017 Index, RDR expanded the ranking to 22 companies, which included all of the companies ranked in 2015 plus an additional six companies. In addition to internet and telecommunications companies, the Index was expanded with new types of services, including those that produce software and devices that we call "mobile ecosystems." As a result, the RDR team further revised the 2017 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.

The 2018 Index applies the same methodology to evaluate the same 22 companies as in the 2017 Index. This will enable us to produce comparative analyses of each company's performance and to track overall trends.

We encourage stakeholders to read more about our methodology development: https://rankingdigitalrights.org/methodology-development/

The Companies

The 2018 Corporate Accountability Index evaluates 22 companies, listed below. Researchers will examine overarching "parent" company policies and practices, in addition to the disclosed policies and practices of selected services and/or local operating companies (depending on company structure).

Telecommunications companies: For these companies we evaluate global group-level policies for relevant indicators plus the home-country operating subsidiary's pre-paid and post-paid mobile service, and fixed-line broadband service where offered, as follows:

- América Móvil (Mexico)
- AT&T (US)
- Axiata (Malaysia)
- Bharti Airtel (India)
- Etisalat (UAE)
- MTN (South Africa)
- Ooredoo (Qatar)
- Orange (France)
- Telefónica (Spain)
- Vodafone (UK)

Internet companies and mobile ecosystems: These company types are evaluated together because Google is both an internet company and is also a mobile ecosystem company, and Apple also offers services such as iMessage and iCloud. We do not evaluate hardware attributes of devices, focusing our assessment on disclosures pertaining to the newest devices offered by those companies and their operating systems. The freedom of expression and privacy issues faced by mobile cloud data and operating systems overlap with the issues faced by traditional internet services. Additional elements relevant only to mobile ecosystems are added to some indicators. For each company we examined up to four services, as follows:

- Apple (US) — iOS mobile ecosystem, iMessage, iCloud
- Baidu (China) — Baidu Search, Baidu Cloud, Baidu PostBar
- Facebook (US) — Facebook, Instagram, WhatsApp, Messenger
- Mail.ru (Russia) — Vkontakte, Mail.ru email, Mail.ru Agent messaging
- Microsoft (US) — Bing, Outlook.com, Skype
- Kakao (South Korea) — Kakao Search, Kakao Mail, KakaoTalk

- Google (US) — Search, Gmail, Youtube, Android mobile ecosystem
- Samsung (South Korea) — Samsung implementation of Android
- Tencent (China) — QZone, QQ, WeChat
- Twitter (US) — Twitter, Periscope
- Yahoo (US) — Yahoo Mail, Flickr, Tumblr
- Yandex (Russia) — Yandex Mail, Yandex Search, Yandex Disk (cloud storage)

Research and Reporting Process

The research and evaluation process for the 2018 Corporate Accountability Index, conducted by RDR and a team of international researchers, includes the following steps.

- **Step 1: Data Collection.** Primary research team will collect data for each company and provide a preliminary assessment of company performance across all indicators. Researchers will also evaluate if company policies have changed or remained the same in comparison to the previous year (2017).

- **Step 2: Secondary Review.** A second team of researchers conducts a fact-check of assessments provided by primary researchers in Step 1.

- **Step 3: Review and Reconciliation.** The RDR team examines the results from Steps 1 and 2 and resolves any differences that arise.

- **Step 4: First Horizontal Review.** The RDR team cross-checks the indicators to ensure they have been evaluated consistently for each company.

- **Step 5: Company Feedback.** Initial results are sent to companies for comment and feedback.

- **Step 6: Secondary Horizontal Review.** RDR team conducts a second horizontal review, drawing in feedback from companies collected in Step 5, and cross-checking the indicators for consistency and quality control.

- **Step 7: Final Scoring.** RDR team calculates final scores. Results include an assessment of how companies performed in 2017 in comparison to 2018.

Companies will receive a cumulative score of their performance across all Index categories, and results will also show how companies performed by individual category and indicator. Results will also show comparative trends between the 2017 and 2018 Indexes.

The Index will be released in April 2018 on an interactive website and in downloadable PDF report. Company scores will be accompanied by a narrative analysis about key findings and trends.

In addition, company "report cards" will analyze each company's performance and include notable information that helps provide context and nuance to the results. Such information might include specific examples of company practice, legal and regulatory context, or other observations made by researchers on matters that fall outside the indicators' research parameters. Individual company results will also include comparative assessments of company performance between the 2017 and 2018 Indexes.

Note on national contexts affecting company performance: In most countries, certain laws, regulations, or political factors will either enhance or limit a company's ability to perform well on certain indicators. Our methodology does not compensate for these factors: in other words, the Index evaluates companies on what they do or don't do, regardless of the reason. However, narrative profiles for each company will include an analysis of how the company's home jurisdiction's legal, regulatory, and political environment may have affected its score. In some cases the reason for a company's strong or weak performance on a given indicator will be due to the legal, regulatory, or political environment of that company's home country. In situations where laws and regulations cause companies to perform poorly, we encourage companies to advocate for laws that enable them to fully respect users' rights to freedom of expression and privacy by disclosing strong commitments, policies, and practices.

The 2018 Index methodology

The 2018 Index ranks 22 companies with 35 indicators in three categories that measure companies' disclosure of policies affecting users' freedom of expression and privacy.

Each category contains **indicators** measuring company performance for that category; each indicator is comprised of **elements** that measure company performance for that indicator.

Index categories:

- **Governance (G)**: This category contains six indicators measuring company disclosure of commitments to freedom of expression and privacy principles along with measures taken to implement those commitments across the company's global operations.

- **Freedom of Expression (F):** this category contains 11 indicators measuring company disclosure of their policies and practices that affect users' freedom of expression rights.

- **Privacy (P):** this category contains 18 indicators measuring company disclosure of their policies and practices that affect users' privacy rights.

Each of these categories and indicators are outlined below. Each indicator is accompanied by a short "**Indicator guidance"** section that describes what the indicator is measuring.

A **Glossary** of terms is also appended below. The terms defined in Glossary are **bolded i**n the indicator text.

G: Governance

Indicators in this category seek evidence that the company 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** to human rights, including freedom of expression and privacy?

Indicator guidance: This indicator seeks evidence that the company has made explicit policy commitments to freedom of expression and privacy. This standard is outlined in the UN Guiding Principles on Business and Human Rights' Operational Principle 16, which states that companies should adopt formal policies publicly affirming their commitments to international human rights principles and standards. The company should clearly disclose these commitments in formal policy documents or other communications that reflect official company policy.

Note that this indicator evaluates a company's official policy commitment to *both* freedom of expression and privacy. These commitments must be publicly available. Companies with policies that mention only one (freedom of expression or privacy) will receive partial credit.

Potential sources:

- Company human rights policy
- Company statements, reports, or other communications that reflect official company policy
- Company annual report or sustainability report that refers to official policy documents

G2. Governance and management oversight

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

Elements:

1. Does the company **clearly disclose** that the **board of directors** exercises formal oversight over how company practices affect freedom of expression and privacy?

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

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

Indicator guidance: This indicator seeks evidence that the company's governance and internal management structures include consideration of freedom of expression and privacy. 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.

To receive full credit for this indicator, companies need to clearly disclose that there is clear oversight over both freedom of expression and privacy issues at each governance level (board, executive, managerial). At the board of directors level, oversight could be carried out explicitly by a board committee, or the company may provide another public explanation of how the board exercises oversight of freedom of expression and privacy. Below board-level, oversight may be carried out by 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
- Company governance documents
- Company sustainability report

- Company organizational chart
- Company human rights policy
- Global Network Initiative documents (if company is a member)
- Telecommunications Industry Dialogue documents (if the company is a member)

G3. Internal implementation

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

Elements:

1. Does the company **clearly disclose** that it provides employee training on freedom of expression and privacy issues?

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

Indicator guidance: While Indicator G2 evaluates whether company leaders at the senior governance level commit to overseeing freedom of expression and privacy issues, this indicator, G3, evaluates if the company discloses whether and how it institutionalizes these commitments within the company.

This indicator seeks disclosure about how the company helps the rest of its employees understand the importance of freedom of expression and privacy. When employees write computer code for a new product, review requests 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.

A company can only receive full credit on this indicator if it clearly discloses information about employee training on freedom of expression and privacy and the existence of a whistleblower program that also encompasses these issues. Disclosure should specify that employee training and whistleblower programs cover freedom of expression and privacy. Companies may still receive credit on this indicator if a company's whistleblower program does not specifically mention complaints related to freedom of expression and privacy so long as the company has made commitments to these principles elsewhere and in a way that makes clear that the company would entertain those complaints through their whistleblower program.

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 affect freedom of expression and privacy and to mitigate any risks posed by those impacts.

Elements:

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 freedom of expression and privacy risks associated with existing products and services?

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

4. Does the company assess freedom of expression and privacy risks associated with the processes and mechanisms used to enforce its terms of service?

5. Does the company conduct additional evaluation 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 their decision-making?

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

8. Are the company's assessments 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?

Indicator guidance: People face human rights risks when they use digital tools. Human rights impact assessments (HRIAs) are a way for companies to learn about and to address, or at the very least try to mitigate, those risks, especially when introducing products and services to new markets. This indicator examines whether companies disclose the existence of any human rights risk assessment processes, as well as whether and how companies incorporate

assessments of freedom of expression and privacy considerations into their decision making. These assessments represent a systematic internal examination to ensure that a company's decisions and practices align with its commitment (and responsibility) to respect freedom of expression and privacy.

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."

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. If a company conducts HRIAs but does not publicly disclose 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.

Elements:

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

2. If the company is not a member of a **multi-stakeholder initiative**, is the company a member of an organization that engages systematically and on a regular basis with non-industry and non-governmental stakeholders on freedom of expression and privacy?

3. If the company is not a member of one of these organizations, does the company disclose that it initiates or participates in meetings with **stakeholders** that represent,

advocate on behalf of, or are people whose freedom of expression and privacy are directly impacted by the company's business?

Indicator guidance: This indicator seeks evidence that the company engages with its stakeholders—and particularly with stakeholders who face clear human rights risks in connection with their online activities. We expect stakeholder engagement to be a core component of a company's policy development and impact assessment process. Stakeholder engagement should be carried out across the full range of issues related to users' freedom of expression and privacy, including a company's process for developing terms of service, privacy, and identity policies along with the enforcement practices for those policies.

Engaging with stakeholders, especially 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.

If a company receives full credit on Element 1, it will automatically receive full credit on Element 2 and Element 3.

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.

Elements:

1. Does the company **clearly disclose** its processes for receiving complaints?

2. Does the company **clearly disclose** that its process includes complaints related to freedom of expression and privacy?

3. Does the company **clearly disclose** its process for responding to complaints?

4. Does the company report on the number of complaints received related to freedom of expression and privacy?

5. Does the company provide clear evidence that it is responding to complaints?

Indicator guidance: Human rights can only be protected and respected if people have redress when they believe their rights have been violated. This indicator examines whether companies provide such 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. We expect companies to disclose information about how the company responds to complaints or grievance reports from people who believe that their rights to freedom of expression or privacy have been infringed by the company or in connection with the company's business. This remedy should include a user's ability to appeal a company's decision to block or remove content or deactivate an account, since such decisions can directly affect that user's rights to freedom of expression.

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 offer **terms of service** that are **easy to find** and **easy to understand**.

Elements:

1. Are the company's **terms of service easy to find**?

2. Are the **terms of service** available in the language(s) most commonly spoken by the company's users?

3. Are the **terms of service** presented in an **understandable manner**?

Indicator guidance: A company's terms of service outline the relationship between the user and the company. The terms contain rules for what activities and content users are permitted to engage in and share on a company's services, and as such, these terms can directly affect users' freedom of expression rights. Companies can also take action against users for violating the conditions described in the terms. Given this, we expect companies to ensure that users can easily locate these terms and understand what they mean.

This indicator expects companies to provide terms of service that are easy to find, are available in the languages of the primary markets in which the company operates, and to ensure that the policies are easy to understand. If the company offers multiple products and services, it should be clear to what products and services the terms apply.

A document that is easy to find is located on the homepage of the company or service, or one or two clicks away from the homepage, or in a logical place where users can expect to find it. The terms should also be available in the major language(s) of the primary operating market. In addition, we expect a company to take 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.

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" category.

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 **clearly disclose** that it provides **notice** and **documentation** to users when it changes its **terms of service**.

Elements:

1. Does the company **clearly disclose** that it notifies users about changes to its **terms of service**?

2. Does the company **clearly disclose** how it will directly notify **users** of changes?

3. Does the company **clearly 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**?

Indicator guidance: It is common for companies to change their terms of service as their business evolves. However these changes can have a significant impact on how users can or cannot use the service, with potential impact on users' freedom of expression rights. We therefore expect companies to commit to notify users when they change these terms and to provide users with information that helps them understand what these changes mean.

This indicator seeks clear disclosure by companies of the method and timeframe for notifying users about changes to their terms of service. We expect companies to commit to directly notify users prior to those changes coming into effect.. The method of direct notification may differ according to 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. This indicator 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.

Potential sources:

- Company terms of service

F3. Process for terms of service enforcement

The company should **clearly disclose** the circumstances under which it may restrict **content** or **user accounts**.

Elements:

1. Does the company **clearly disclose** what types of **content** or activities it does not permit?

2. Does the company **clearly disclose** why it may **restrict a user's account**?

3. Does the company **clearly disclose** information about the processes it uses to identify **content** or **accounts** that violate the company's rules?

4. Does the company **clearly disclose** whether any government authorities receive priority consideration when flagging content to be restricted for violating the company's rules?

5. Does the company **clearly disclose** whether any private entities receive priority consideration when flagging content to be restricted for violating the company's rules?

6. Does the company **clearly disclose** its process for enforcing its rules?

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

Indicator 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 violating these rules. For mobile ecosystems, this can include restricting access to an end-user's account or a developer's account.

We therefore expect companies to clearly 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 that allow users to flag other users' content and/or activity for company review. We also expect companies to clearly disclose whether they have a policy of granting priority or expedited consideration to any government authorities and/or members of private organizations or other entities that identify their organizational affiliation when they report content or users for allegedly violating the company's rules. 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.

Potential sources:

- Company terms of service, user contract
- Company 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. Data about terms of service enforcement

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

Elements:

1. Does the company **clearly disclose** data about the volume and nature of content and accounts restricted for violating the company's rules?

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

3. Can the data published by the company be exported as a **structured data** file?

Indicator guidance: Companies enforce their terms of service for a variety of reasons, and we expect companies to publicly disclose the number of instances in which they take action to restrict users' accounts or services. Disclosing this data provides the public with a more transparent and accurate view of the content removal process as well as companies' role in content removal.

This indicator evaluates company disclosure of data on the number of instances it 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. Companies can only receive full credit on this indicator if they provide evidence that they clearly disclose and regularly publish data about their decisions to remove content. This information should be published at least once a year and in a structured data file.

Potential sources:
- Company transparency report

F5. Process for responding to third-party requests for content or account restriction

The company should **clearly disclose** its process for responding to **government requests** (including judicial orders) and **private requests** to remove, filter, or restrict **content** or **accounts**.

Elements:

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

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

3. Does the company **clearly disclose** its process for responding to **government requests** from foreign jurisdictions?

4. Does the company **clearly disclose** its process for responding to **private requests**?

5. Do the company's explanations **clearly disclose** the legal basis under which it may comply with **government requests**?

6. Do the company's explanations **clearly disclose** the basis under which it may comply with **private requests**?

7. Does the company **clearly disclose** that it carries out due diligence on **government requests** before deciding how to respond?

8. Does the company **clearly disclose** that it carries out due diligence on **private requests** before deciding how to respond?

9. Does the company commit to push back on inappropriate or overbroad **requests made by governments**?

10. Does the company commit to push back on inappropriate or overbroad **private requests**?

11. Does the company provide clear guidance or examples of implementation of its process of responding to **government requests**?

12. Does the company provide clear guidance or examples of implementation of its process of responding to **private requests**?

Indicator guidance: Companies often receive requests to remove, filter, or restrict access to content and accounts. These requests can come from government agencies or courts (both domestic and foreign), as well as from private entities (i.e. non-governmental and non-judicial entities). We expect companies to publicly disclose their process for responding to requests from governments and courts, as well as to private requests that come through some type of defined or organized process. Private requests can come through 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 evaluates whether the company clearly discloses how it responds to government and private requests to remove, filter, or restrict content or accounts. The company should disclose the legal reasons why it would remove content**.** In some cases, the law might prevent a company from disclosing information referenced in this indicator's elements. RDR 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 terms of service
- Company help or support center
- Company blog posts
- Company policy on copyright or intellectual property

F6. Data about government requests for content or account restriction

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

Elements:

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 knowingly receives from government officials to restrict **content** or **accounts** through unofficial processes?
7. Does the company list the number of requests with which it complied?
8. Does the company publish the original requests or disclose that it provides copies to a **public third-party archive**?
9. Does the company report this data at least once a year?
10. Can the data be exported as a **structured data** file?

Indicator guidance: Companies frequently receive requests from governments to remove, filter, or restrict content or accounts. We expect a company to regularly publish data about the number and type of government requests it receives, and the number of such requests with

which it complies. Companies may receive these requests through official processes, such as a court order, or through informal channels, like a flagging system intended to allow 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. Disclosing this data helps the public gain a greater understanding of the environment for freedom of expression online and it helps the public hold companies and governments accountable for their obligations to respect and protect freedom of expression rights.

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 nonetheless lose points if it fails to meet all elements. This represents a situation where the law causes companies to fall short of best practice for this indicator, 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

F7. Data about private requests for content or account restriction

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

Elements:

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 disclose that it provides copies to a **public third-party archive**?
8. Does the company report this data at least once a year?

9. Can the data be exported as a **structured data** file?

10. Does the company **clearly disclose** that its reporting covers all types of **private requests** that it receives?

Indicator guidance: Companies frequently receive requests from private parties to remove, filter, or restrict content or accounts. We expect companies to regularly publish data about the number and type of private requests it receives, and the number of such requests with which it complies.. 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 F4.

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. User notification about content and account restriction

The company should **clearly disclose** that it **notifies users** when it restricts **content** or **accounts**.

Elements:

1. If the company hosts user-generated **content**, does the company **clearly disclose** that it notifies **users** who generated the **content** when it is restricted?

2. Does the company **clearly disclose** that it notifies users who attempt to access **content** that has been restricted?

3. In its notification, does the company **clearly disclose** a reason for the **content** restriction (legal or otherwise)?

4. Does the company **clearly disclose** that it notifies users when it restricts their **account**?

Indicator guidance: Indicator F3 examines company disclosure of restrictions on what users can post or do on a service. This indicator, F8, focuses on whether companies clearly disclose that they notify users when they take these types of actions (whether due to terms of service enforcement or third-party restriction requests). A company's decision to restrict or remove access to content or accounts can have a significant impact on users' freedom of expression and access to information rights. We therefore expect companies to disclose that they notify users when they have removed content, restricted a user's account, or otherwise restricted users' abilities to access a service. If a company removes content that a user has posted, we expect the company to inform that user about its decision. If a different user attempts to access content that the company has restricted, we expect the company to notify that user about the content restriction. We also expect companies to specify reasons for their decisions. This disclosure should be part of companies' explanations of their content and access restriction practices.

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

F9. Network management (telecommunications companies)

The company should **clearly disclose** that it does not **prioritize**, block, or delay certain types of traffic, **applications**, **protocols**, or **content** for any reason beyond assuring quality of service and reliability of the network.

Elements:

1. Does the company **clearly 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 **clearly disclose** its purpose for doing so?

Indicator guidance: This indicator is only applicable to telecommunications companies. This indicator evaluates whether companies clearly disclose if they engage in practices that affect the flow of content through their networks, such as **throttling** or **traffic shaping**. We expect

companies to publicly commit to avoid prioritization or degradation of content. In some cases companies may engage in legitimate traffic shaping practices in order to ensure the flow of traffic through their networks. 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, however, include company disclosure related to blocking of services, apps, or devices, which are considered a type of prioritization.

Potential Sources:

- Company explanation of network management or traffic management practices

F10. Network shutdown (telecommunications companies)

The company should clearly 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.

Elements:

1. Does the company clearly explain the reason(s) why it may shut down service to a particular area or group of users?
2. Does the company clearly explain why it may 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 clearly 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 **clearly disclose** that it notifies users directly when it **shuts down the network or restricts access to a service**?
6. Does the company list the number of **network shutdown** requests it receives?
7. Does the company clearly identify the specific legal authority that makes the request?
8. Does the company list the number of requests with which it complied?

Indicator guidance: This indicator is only applicable to telecommunications companies. Network shutdowns are a growing threat to human rights. The UN Human Rights Council has condemned network shutdowns as a violation of international human rights law and called on

governments to refrain from taking these actions. Yet governments are increasingly ordering telecommunications companies to shut down their networks, which in turn puts pressure on companies to take actions that violate their responsibility to respect human rights. We expect companies to fully disclose to the circumstances under which they might take such action and to report on the requests they receive to take such actions.

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

F11. Identity policy

The company should not **require** users to verify their identity with their **government-issued identification**, or other forms of identification that could be connected to their offline identity.

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

Indicator guidance: The ability to communicate anonymously is essential to freedom of expression both on and offline. The use of a real name online, or requiring users to provide a company with identifying information, provides a link between online activities and a specific person. This presents human rights risks to those who, for example, voice opinions that don't align with a government's views or who engage in activism that a government does not permit. It also presents risks for people who are persecuted for religious beliefs or sexual orientation.

We therefore 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. However, 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.

This indicator is applicable to internet companies, mobile ecosystem companies, and pre-paid mobile services (for telecommunications companies).

Potential sources:

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

P: Privacy

Indicators in this category seek evidence that 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 these indicators 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 offer **privacy policies** that are **easy to find** and **easy to understand**.

Elements:

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 disclose that it requires apps made available through its **app store** to provide users with a privacy policy?

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

This indicator expects companies to provide privacy policies that are easy to find, are available in the languages of the primary markets in which the company operates, and to ensure that the policies are easy to understand. If the company offers multiple products and services, it should be clear to what products and services the policies apply.

A document that is "easy to find" should be located on the homepage of the company or service, or one or two clicks away from the homepage, or in a logical place where users are likely to find it. The terms should also be available in the major language(s) of the primary operating market.

In addition, we expect a company to take steps to help users understand the information presented in their documents. This may include, 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. Terms of Service are not included in this indicator since they are covered in separate indicators in the "Freedom of Expression" category.

Potential sources:

- Company privacy policy
- Company data use policy

P2. Changes to privacy policies

The company should **clearly disclose** that it provides **notice** and **documentation** to users when it changes its **privacy policies**.

Elements:

1. Does the company **clearly disclose** that it notifies users about changes to its privacy policies?
2. Does the company **clearly disclose** how it will directly notify users of changes?
3. Does the company **clearly 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 **clearly disclose** that it requires apps sold through its **app store** to notify users when the **app** changes its privacy policy?

Indicator guidance: It is common for companies to change their privacy policies as their business evolves. However, these changes can significantly impact a user's privacy rights and what user information companies can collect, share and store. We therefore expect companies to commit to notify users when they change these policies and to provide users with information to help them understand what these changes mean.

This indicator seeks clear disclosure by companies of their method and timeframe for notifying users about changes to privacy policies. We expect companies to commit to directly notifying users prior to changes coming into effect. 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. 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.

Potential sources:

- Company privacy policy
- Company data use policy

P3. Collection of user information

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

Elements:

1. Does the company **clearly disclose** what types of user information it **collects**?

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

3. Does the company **clearly disclose** that it limits collection of **user information** to what is directly relevant and necessary to accomplish the purpose of its service?

4. (For **mobile ecosystems**): Does the company **clearly disclose** that it evaluates whether the **privacy policies** of third-party **apps** made available through its **app store** disclose what **user information** the apps collect?

5. (For **mobile ecosystems**): Does the company **clearly disclose** that it evaluates 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?

Indicator guidance: Companies collect a wide range of personal information from users—from personal details and account profiles to a user's activities and location. We expect companies to clearly disclose what user information (*as RDR defines it*) they collect and how they do so. We also expect companies to commit to the principle of **data minimization** and to 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 the company to clearly disclose whether the privacy policies of the apps that are available in its app store specify what user information the apps collect and whether those policies comply with data minimization principles.

The term "**user information**" appears in many indicators throughout the Privacy category. RDR takes an expansive interpretation of user information, which according to our definition constitutes: "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."

This expansive 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.

In some cases, laws or regulations may require companies to collect certain information or may 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 **clearly disclose** what **user information** it **shares** and with whom.

Elements:

1. For each type of **user information** the company collects, does the company **clearly disclose** whether it shares that user information?

2. For each type of **user information** the company shares, does the company **clearly disclose** the types of **third parties** with which it shares that user information?

3. Does the company **clearly disclose** that it may share user information with government(s) or legal authorities?

4. For each type of **user information** the company shares, does the company **clearly disclose** the names of all **third parties** with which it shares user information?

5. (For **mobile ecosystems**): Does the company **clearly disclose** that it evaluates whether the **privacy policies** of third-party **apps** made available through its **app store** disclose what user information the apps share?

6. (For **mobile ecosystems**): Does the company **clearly disclose** that it evaluates whether the **privacy policies** of third-party **apps** made available through its **app store** disclose the types of third parties with whom they share user information?

Indicator guidance: Companies collect a wide range of personal information from users—from personal details and account profiles to a user's activities and location. Companies also often share this information with third parties, such as advertisers, governments, and legal authorities. We expect companies to clearly disclose what user information (as RDR defines it) they share and with whom. Company disclosure should specify if it shares user information with governments and with commercial entities. For mobile ecosystems, we expect the company to clearly disclose whether the privacy policies of the apps that are available in its app store specify what user information the apps share with third parties.

In some cases, laws or regulations may 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**.

Elements:

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** whether it combines **user information** from various company services and if so, why?

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

4. Does the company **clearly disclose** that it limits its use of **user information** to the purpose for which it was collected?

Indicator guidance: We expect companies to clearly disclose the purpose for collecting and sharing user information for each type of user information it collects and shares. 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 publicly commit to the principle of use limitation**,** which is part of the OECD privacy guidelines, among other frameworks.

Potential Sources:

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

P6. Retention of user information

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

Elements:

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

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

3. Does the company **clearly disclose** the process for **de-identifying user information**?

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

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

6. (For **mobile ecosystems**): Does the company **clearly disclose** that it evaluates whether the privacy policies of third-party **apps** made available through its **app store** disclose how long they retain user information?

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

Indicator guidance: Companies collect a wide range of personal information from users in exchange for the use of and access to the company's products and services. This information can range from personal details, profiles, and account activities to information about a user's activities and location. We expect companies to clearly 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 that 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 disclose whether the privacy policies of the apps that are available in their app store state how long the app retains user information and whether all user information is deleted if users terminate or delete the app.

In some cases, laws or regulations may 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 fall short of best practice, 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

P7. Users' control over their own user information

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

Elements:

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

2. For each type of **user information** the company collects, does the company **clearly disclose** whether users can delete this user information?

3. Does the company **clearly disclose** that it provides users with **options to control** how their user information is used for targeted advertising?

4. Does the company **clearly disclose** that targeted advertising is off by default?

5. (For **mobile ecosystems**): Does the company **clearly disclose** that it provides users with options to control the **device**'s **geolocation** functions?

Indicator guidance: We expect companies to clearly disclose what options users have to control the information that companies collect and retain about them. Enabling users to control what information about them that a company collects and retains would mean giving users the ability to delete specific types of user information without requiring them to delete their entire account. We therefore expect companies to clearly disclose whether users have the option to delete specific types of user information.

In addition, we expect companies to enable users to control the use of their information for the purpose of targeted advertising. Targeted advertising requires extensive collection and retention of user information that is tantamount to tracking. Companies should therefore clearly disclose whether users have options to control how their information is being used for these purposes.

For mobile ecosystems, we expect companies to clearly disclose what options users have to control the collection of their location information. 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 how other products and services access their location information. For instance, mobile apps may enable users to control location information. However, if the device on which those mobile apps run collects geolocation data by default and does not give users a way to turn this off, users may not be able to limit that mobile app's collection of their location information. For these reasons, we expect companies to disclose that users can control how their device interacts with their location information.

Potential sources:
- Company privacy policy
- Company account settings page

P8. Users' access to their own user information

Companies should allow users to obtain all of their **user information** the company holds.

Elements:

1. Does the company **clearly disclose** that users can obtain a copy of their **user information**?

2. Does the company **clearly disclose** what **user information** users can obtain?

3. Does the company **clearly disclose** that users can obtain their **user information** in a **structured data** format?

4. Does the company **clearly disclose** that users can obtain all public-facing and private **user information** a company holds about them?

5. (For **mobile ecosystems**): Does the company **clearly disclose** that it evaluates whether the privacy policies of third-party **apps** made available through its **app store** disclose that users can obtain all of the **user information** about them the app holds?

Indicator g**uidance:** Users should be able to obtain all information that companies hold about them**.** We expect companies to clearly disclose what options users have to obtain this information, what data this record contains, and what formats users can obtain it in. For mobile ecosystems, we expect the company to disclose to users whether the apps that are available in its app store specify that users can obtain all of the user information that app holds about them.

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

P9. Collection of user information from third parties (internet and mobile ecosystem companies)

The company should **clearly disclose** its practices with regard to **user information** it **collects** from third-party websites or **apps** through technical means.

Elements:

1. Does the company **clearly disclose** what **user information** it collects from third-party websites through technical means?

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

3. Does the company **clearly disclose** its purpose for collecting **user information** from third parties through technical means?

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

5. Does the company **clearly disclose** that it respects **user-generated signals** to opt-out of data collection?

Indicator guidance: We expect companies to disclose what information about users they collect from third parties, which in this case typically means information collected from third-party websites or apps through technical means, for instance through cookies, plug-ins, or widgets. Company disclosure of these practices helps users understand if and how their activities are being tracked by companies even when they are not on a host company's website. One prominent user-generated signal is the "Do Not Track" standard. 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.

Potential sources:

- Company privacy policy
- Company policy on third parties

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

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

Elements:

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

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

3. Does the company **clearly disclose** its process for responding to government requests from foreign jurisdictions?

4. Does the company **clearly disclose** its process for responding to **requests made by private parties**?

5. Do the company's explanations **clearly disclose** the legal basis under which it may comply with **government requests**?

6. Do the company's explanations **clearly disclose** the basis under which it may comply with **requests from private parties**?

7. Does the company **clearly disclose** that it carries out due diligence on **government requests** before deciding how to respond?

8. Does the company **clearly disclose** that it carries out due diligence on **private requests** before deciding how to respond?

9. Does the company commit to push back on inappropriate or overbroad **government requests**?

10. Does the company commit to push back on inappropriate or overbroad **private requests**?

11. Does the company provide clear guidance or examples of implementation of its process for **government requests**?

12. Does the company provide clear guidance or examples of implementation of its process for **private requests**?

Indicator guidance: Companies increasingly receive requests to turn over user information. These requests can come from government agencies or courts (both domestic and foreign), as well as from private entities (i.e. non-governmental and non-judicial entities) We expect companies to publicly disclose their process for responding to requests from each type of third party, along with the basis for complying with these requests. Companies should also publicly commit to pushing back on inappropriate or overbroad government and private requests.

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 fall short of best practice, 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. Data about third-party requests for user information

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

Elements:

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?

Indicator guidance: Companies frequently receive requests from third parties to hand over user information. These requests can come from government agencies or courts (both domestic and foreign), as well as from private entities (i.e. non-governmental and non-judicial entities). We expect companies to regularly publish data about the number and type of such requests they receive, and the number of such requests with which they comply. Companies should disclose data about requests they receive by country, including from their home and foreign governments, as well as from law enforcement, courts and private parties. We also expect

company disclosure to indicate the number of accounts affected by these requests and to delineate by category the requests with which the company has complied. We recognize that companies are sometimes not allowed to disclose requests for user information made by governments. However, in these cases, we expect companies to report what types of government requests they are not allowed to disclose by law. Companies should also report this data once a year and should ensure the data can be exported in structured data file.

In some cases, the law might prevent a company from disclosing information referenced in this indicator. 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 fall short of best practice, 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

P12. User notification about third-party requests for user information

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

Elements:

1. Does the company **clearly disclose** that it notifies users when **government entities (including courts or other judicial bodies)** request their **user information**?

2. Does the company **clearly disclose** that it notifies users when private parties request their **user information**?

3. Does the company **clearly disclose** 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?

Indicator guidance: We expect companies to clearly disclose a commitment to notifying users when governments and private parties request data about users. We acknowledge that this notice may not be possible in legitimate cases of an ongoing investigation; however, we expect companies to specify what types of government requests they are prohibited by law from disclosing.

Potential sources:

- Company transparency report
- Company law enforcement guidelines

P13. Security oversight

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

Elements:

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

2. Does the company **clearly disclose** that it has a security team that conducts security audits on the company's products and services?

3. Does the company **clearly disclose** that it commissions third-party security audits on its products and services?

Indicator guidance: Companies have access to immense amounts of information about users and 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 information about their oversight processes for keeping user information secure. We therefore expect companies to clearly disclose that they have systems in place to limit and monitor employee access to user information. We also expect the company to clearly disclose that it deploys both internal and external security teams to conduct security audits on its products and services.

Potential sources:
- Company privacy policies
- Company security guide

P14. Addressing security vulnerabilities

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

Elements:

1. Does the company **clearly disclose** that it has a mechanism through which **security researchers** can submit **vulnerabilities** they discover?

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

3. Does the company commit not to pursue legal action against researchers who report **vulnerabilities** within the terms of the company's reporting mechanism?

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

6. (For mobile ecosystems and telecommunications companies) Does the company **clearly 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 **clearly 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 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?

Indicator 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 these companies to disclose information that may affect a user's ability to access these critical updates.

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

P15. Data breaches

The company should publicly disclose information about its processes for responding to **data breaches**.

Elements:

1. Does the company **clearly disclose** that it will notify the relevant authorities without undue delay when a **data breach** occurs?

2. Does the company **clearly disclose** its process for notifying data subjects who might be affected by a **data breach**?

3. Does the company **clearly disclose** what kinds of steps it will take to address the impact of a **data breach** on its users?

Indicator guidance: When the security of users' data has been compromised due to a data breach, companies should have clearly disclosed processes in place for addressing the security threat and for notifying affected users. Given that data breaches can result in significant threats to an individual's financial or personal security, in addition to exposing private information, companies should make these security processes publicly available. Individuals can then make informed decisions and consider the potential risks before signing up for a service or giving a company their information.

Company press releases or blog posts addressing a data breach after it has occurred do not qualify as sufficient disclosure for this indicator. We expect companies to have formal policies in place regarding their handling of data breaches if and when they occur, and companies to make this information about these policies and commitments public.

Potential sources:
- Company terms of service or privacy policy
- Company security guide

P16. Encryption of user communication and private content (internet and mobile ecosystem companies)

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

Elements:

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

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

3. Does the company **clearly disclose** that users can secure their private content using **end-to-end encryption,** or **full-disk encryption** (where applicable)?

4. Does the company **clearly disclose** that **end-to-end encryption**, or **full-disk encryption**, is enabled by default?

Indicator guidance: Encryption is an important tool for protecting freedom of expression and privacy. The UN Special Rapporteur on Freedom of Expression has stated unequivocally that encryption and anonymity are essential for the exercise and protection of human rights. We expect companies to clearly disclose that user communications are encrypted by default, that transmissions are protected by "perfect forward secrecy," that users have an option users have to turn on end-to-end encryption, and if the company offers end-to-end encryption by default. For mobile ecosystems, we expect companies to clearly disclose that they enable full-disk encryption.

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

P17. Account Security (internet and mobile ecosystem companies)

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

Elements:

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

2. Does the company **clearly disclose** that users can view their recent account activity?

3. Does the company **clearly disclos**e that it notifies users about unusual account activity and possible unauthorized access to their accounts?

Indicator guidance: This indicator is applicable to internet and mobile ecosystem companies. 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 clearly disclose that they use advanced authentication techniques to prevent unauthorized access to user accounts and information. We also expect companies to provide

users with tools that enable them to secure their accounts and to know when their accounts may be compromised.

Potential Sources:

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

P18. Inform and educate users about potential risks

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

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

Indicator guidance: Companies hold significant amounts of user information, making them targets for malicious actors. We expect companies to help users protect themselves against such risks. This can include materials on how to set up advanced account authentication; adjust privacy settings; avoid malware, phishing, and social engineering attacks; avoid third-party tracking; avoid or address bullying or harassment online; and what “safe browsing” means. 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 risks companies and users can face. These can include tips, tutorials, how-to guides, or other resources and should be presented in a way that users can easily understand (for instance with visuals, graphics, bullet points, and lists).

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 username 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.

Board of directors – Board-level oversight should involve members of the board having direct oversight of issues related to freedom of expression and privacy. This does not have to be a formal committee, but the responsibility of board members in overseeing company practices on these issues should be clearly articulated and disclosed on the company's website.

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

Clearly disclose(s) — The company presents or explains its policies or practices in its public-facing materials in a way that is easy for users to find and understand.

Collect / Collection — All means by which a company may gather information about users. For example, a company may collect this information directly in a range of situations, including when users upload content for public sharing, submit phone numbers for account verification, transmit personal information in private conversation with one another, etc. 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 in 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, including in both 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 risks — Situations in which a user's security, privacy, or other related rights might be threatened by a malicious actor (including but not limited to criminals, insiders, or nation states) who may gain unauthorized access to user data using hacking, phishing, or other deceptive techniques.

Data breach — A data breach occurs when an unauthorized party gains access to user information that a company collects, retains, or otherwise processes, and which compromises the integrity, security, or confidentiality of that information.

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 means removing explicit identifiers like names, email addresses, and any government-issued ID numbers, as well as identifiers like IP addresses, cookies, and unique device numbers.

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.

Documentation — The company provides records that users can consult, such as a log of changes to terms of service or privacy policy documents.

Do Not Track — Also known by the acronym "DNT," this refers to a setting in a user's browser preferences that tells companies or third parties 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.

Easy to find — The terms of service or privacy policy is located one or two clicks away from on the homepage of the company or service, or is located in a logical place where users are likely to find it.

Easy to understand / understandable manner — The company has taken steps to help users actually understand its terms of service and privacy policy. 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.

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 user 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, 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

End-to-end encryption — With end-to-end encryption, only the sender and receiver can read the content of the encrypted communications. Third parties, including the company, would not be able to decode the content.

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

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.

Explicit — The company specifically states its support for freedom of expression and privacy.

Forward secrecy / perfect forward secrecy — An encryption method notably used in HTTPS web traffic and in messaging apps, in which a new key pair is generated for each session (HTTPS), or for each message exchanged between the parties (messaging apps). This way, if an adversary obtains one decryption key, it will not be able to decrypt past or future transmissions or messages in the conversation. Forward secrecy is distinct from end-to-end encryption, which refers to the data being encrypted while "at rest" on remote company servers. For more, see "Pushing for Perfect Forward Secrecy," Electronic Frontier Foundation, https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-important-web-privacy-protection.

Full-disk encryption — Comprehensive encryption of all data stored on a physical device, in ƒsuch a way that only the user is able to access the content by providing the user-generated password(s) and/or other means of decryption (fingerprint, two-factor authentication code, physical token, etc.)

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 — RDR takes its definition of grievance from the UN Guiding Principles: "[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.

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 or through GPS or Wi-FI positioning.
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, or other software.

Management-level — 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.The core functionality is the most essential functions or affordances of a product or service. For example, a smartphone's core functionality would include sending and receiving phone calls, text messages, and emails, downloading and running apps, and accessing the internet.This applies to Android smartphones produced by companies other than Google.

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 in the ICT sector.

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.

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."

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 of the computer program, application, or operating system.

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 — A publicly available statement that represents official company policy which has been approved at the highest levels of the company.

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

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 a company's policies, such as its terms of service or privacy policy, or comprehensively explains each round of changes the company makes to these policies.

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).

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

Require — The requirement may take place at the time a user signs up for an account or later, upon company request.

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 indefinite. 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 — 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.

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.

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 legitimate 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 collecting such information and should not use the information 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-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 examples 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.