Ranking Digital Rights

Corporate Accountability Index

2015 Research Indicators

Including definitions and parameters

June 2015

Produced by

rankingdigitalrights.org

www.sustainalytics.com

Acknowledgments

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

The John S. and James L. Knight Foundation
The John D. and Katherine T. MacArthur Foundation
Hivos People Unlimited
The Ford Foundation
Open Society Foundations
The William and Flora Hewlett Foundation
University of Pennsylvania
Annenberg COMPASS Fellowships

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

About Ranking Digital Rights

Ranking Digital Rights is a project hosted by New America's Open Technology Institute dedicated to evaluating the world's most powerful ICT companies on policies and practices affecting users' free expression and privacy. For more about the project please visit rankingdigitalrights.org

For more about New America please visit www.newamerica.org

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

About Sustainalytics

Sustainalytics is a leading independent environmental, social and governance (ESG) research and analysis firm that supports investors around the world with the development and implementation of responsible investment strategies. As the research partner for the Ranking Digital Rights pilot project, Sustainalytics helped design the research methodology for the initiative and rank leading global ICT companies on policies and practices on free expression and privacy in relation to human rights standards and laws.

With 13 offices globally, Sustainalytics has over 200 staff members, including more than 100 analysts with a broad range of industry and language expertise. The firm is the primary research partner for the 2014 Access to Medicine Index, among other leading rankings and indices. For the past three years, Sustainalytics was voted best independent responsible investment research firm in Extel's IRRI survey. For more information about Sustainalytics, please visit www.sustainalytics.com.

Table of Contents

About the 2015 Index

In November 2015, the Ranking Digital Rights project will launch the inaugural Corporate Accountability Index. 16 Internet and telecommunications companies will be ranked according to 31 indicators focused on corporate disclosure of policies and practices that affect users' freedom of expression and privacy.

The data produced by the Index will inform the work of human rights advocates, policymakers, and responsible investors. It will also help companies improve their own policies and practices.

The Companies

In its first year the Index will evaluate 16 companies, evenly divided between Internet and telecommunications companies. Researchers will examine over-arching "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). The 2015 companies are:

Telecommunications companies:
(Parent-company level, plus fixed broadband and mobile services in each company's home jurisdiction)

- **América Móvil**
- **AT&T**
- **Axiata**
- **Bharti Airtel**
- **Etisalat**
- **MTN**
- **Orange**
- **Vodafone**

Internet companies:
(Company-wide policies plus 2-3 selected services, as specified below)

- **Daum Kakao** – Daum Search, KakaoTalk, Daum Mail
- **Facebook** – Facebook, WhatsApp, Instagram
- **Google** – Search, Gmail, YouTube
- **Mail.ru** – VKontakte, Mail, Mail.ru Agent
- **Microsoft** – Bing, Outlook.com, Skype
- **Tencent** – WeChat, Qzone, QQ
- **Twitter** – Twitter, Vine
- **Yahoo** – Mail, Flickr, Tumblr

Research and Reporting Process

The research and evaluation process for the 2015 Corporate Accountability Index, carried out jointly by Ranking Digital Rights, Sustainalytics, and a team of international researchers, includes the following steps:

1. Primary research – researchers evaluate each company for each indicator (see Appendix 2 for more information about the research parameters);

2. Peer review – a second set of researchers check the work of the primary researchers, raise questions, and suggest changes;

3. Reconciliation – lead researchers from RDR and Sustainalytics resolve differences between the primary research results and peer review;

4. Company review – initial results from step 3 are sent to companies for comment and feedback;

5. Revision and initial scoring – RDR and Sustainalytics process company feedback and make decisions about results;

6. Horizontal review – Sustainalytics examines companies' results across indicators to ensure consistency and quality control;

7. Final results – Final decisions are made about companies' results.

The results will then be weighted and converted into numerical scores for each company.

The Index will be released in November 2015 on an interactive website and in downloadable PDF versions of a report. The scoring methodology will be released jointly with the results of the Index. The scores will be accompanied by an over-arching narrative analysis about key findings and trends. In addition, company profiles 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, or other observations made by researchers on matters that fall outside the indicators' research parameters.

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.

For more information about how the indicators and research methodology were developed, plus documents describing the research parameters and definitions being used to guide the research, please see the project website at https://rankingdigitalrights.org.

Terms defined in Appendix 1 are bolded in the indicator text below.

C: Commitment

The company demonstrates a clear commitment in words and deeds to respect 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 commitment 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.

C1. Policy and leadership

A. Does the company make **explicit**, **prominent**, and clearly articulated **policy commitment** to human rights including freedom of expression and privacy?

Answer categories (select one):

1. Yes
2. No

B. Do **senior executives** of the company make **meaningful commitment** to advance users' freedom of expression and privacy?

Answer categories (select one):

1. **Executive-level** comment: A senior executive has made statements in a **prominent venue**.
2. **Managerial-level** comment: Company managers or spokesperson(s) have made statements in a prominent venue.
3. None/no-evidence: Company representatives have not made related statements in a prominent venue.

C2. Governance and management oversight

Is there **oversight** at board, executive, and management levels on how the company's policies and practices affect freedom of expression and privacy?

Checklist elements (select all that apply):

1. **Board-level** oversight: A board **committee** has formal oversight over how company practices affect freedom of expression and privacy.

2. **Executive-level** responsibility: An executive-level committee, **team**, **program** or **officer** oversees how company practices affect freedom of expression and privacy.

3. **Management-level** responsibility: A management-level committee, team, program or officer oversees how company practices affect freedom of expression and privacy.

C3. Internal implementation

Does the company have mechanisms in place to implement its commitment to freedom of expression and privacy?

Checklist elements (select all that apply):

1. The company provides employee training on freedom of expression and privacy issues.

2. The company maintains an employee **whistleblower program**.

C4. Impact assessment

Does the company conduct regular, comprehensive, and credible due diligence, such as **human rights impact assessments**, to identify how all aspects of their business impact freedom of expression and privacy?

Checklist elements (select all that apply):

1. The company examines laws affecting privacy and freedom of expression in jurisdictions where it operates and uses this analysis to inform company policies and practices.

2. The company regularly assesses free expression and privacy risks associated with existing products and services.

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

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

5. The company conducts in-depth due diligence wherever the company's risk assessments identify concerns.

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

7. The company conducts assessments on a regular schedule.

8. The company's assessment is assured by an external third party.

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

C5. Stakeholder engagement

Does the company **engage** with a range of **stakeholders** on freedom of expression and privacy issues?

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

B. If not, does the company satisfy any of the following elements?

   1. The company is a member of an industry organization that engages with non-industry and non-governmental stakeholders on freedom of expression and privacy.

   2. The company initiates or participates in meetings with stakeholders that represent, advocate on behalf of, or are people directly and adversely impacted by the company's business.

C6. Remedy

Does the company have **grievance** and **remedy** mechanisms?

Checklist elements (select all that apply):

1. The company discloses its processes for receiving complaints or grievances.

2. The company lists the kinds of complaints it is prepared to respond to.

3. The company articulates its process for responding to complaints.

4. The company reports on the number of complaints received.

5. The company provides evidence that it is responding to complaints, including examples of outcomes.

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. Availability of Terms of Service

Are the company's **Terms of Service freely available** and **easy to understand**?

Checklist elements (select all that apply):

1. Free: The company's terms of service (ToS) are **easy to find** and **freely available** without needing to sign up or subscribe.

2. Language: The ToS is available in the language(s) most commonly spoken by the company's users.

3. Easy to understand: The ToS are presented in an **understandable manner**.

F2. Terms of Service, notice and record of changes

Does the company commit to provide meaningful **notice** and **documentation** to users when it changes its **Terms of Service**?

Checklist elements (select all that apply):

1. The company discloses the method of direct notification to users (e.g., email, SMS, etc.).

2. The company discloses the timeframe within which it provides notification (e.g., two weeks prior to changes occurring).

3. The company maintains a **public archive** or **change log**.

F3. Reasons for content restriction

Does the company disclose whether it prohibits certain types of **content** or activities?

Checklist elements (select all that apply):

1. The company explains what types of content or activities it does not permit.
2. The company explains its **process for enforcing its rules**.
3. The company provides examples to help the user understand what the rules are and how they are enforced.

F4. Reasons for account or service restriction

Does the company explain the circumstances under which it may restrict or deny users from accessing the service?

Checklist elements (select all that apply):

1. The company explains the reason(s) why it may **restrict a user's account**.
2. The company explains why it may shut down or **restrict service** to a particular area or group of users (where applicable).
3. The company provides specific examples of situations that may trigger restriction or denial of service by the company.

F5. Notify users of restriction

If the company restricts **content** or access, does it disclose how it **notifies** users?

Checklist elements (select all that apply):

1. If the company hosts user-generated content, the company commits to notify users who generated the content when it is restricted.
2. The company commits to notify users who attempt to access content that has been restricted.
3. In its notification, the company includes an explanation of the basis for the content restriction (legal or otherwise).
4. The company commits to notify users when it restricts access to the service.

F6. Process for responding to third-party requests

Does the company publish information about its process for evaluating and responding to **requests from governments** and other **third parties** to restrict **content** or service?

Checklist elements (select all that apply):

1. The company explains its process for receiving and responding to **non-judicial government requests**.
2. The company explains its process for responding to **court order**s.
3. The company explains its process for responding to **requests made by private parties**.
4. The company explains its process for responding to requests from foreign jurisdictions.
5. The company's explanations include the legal basis under which it may comply.
6. The company commits to carry out due diligence on requests before deciding how to respond.
7. The company's process commits to push back on unlawful requests.
8. The company provides guidance or examples of policy implementation.

F7. Data about government requests

Does the company regularly publish data about **government requests** (including judicial orders) to remove, filter, or restrict **content** or access to service, plus data about the extent to which the company complies with such requests?

Checklist elements (select all that apply):

1. The company breaks out the number of requests it receives by country.
2. The company lists the number of accounts affected.
3. The company lists the number of pieces of content or URLs affected.
4. The company lists the types of subject matter associated with the requests it receives.
5. The company identifies the specific legal authority making the requests.

6. The company lists the number of requests it complied with.

7. The company either publishes the original requests or provides copies to a third-party archive such as Chilling Effects or a similar organization.

8. The company reports this data at least once a year.

9. The data reported by the company can be exported as a **structured data** file.

F8. Data about private requests

Does the company regularly publish data about **requests from non-governmental** (and **non-judicial**) **parties** to remove, filter, or restrict access to **content**, plus data about the extent to which the company complies with such requests?

Checklist elements (select all that apply):

1. The company breaks out the number of requests it receives by country.

2. The company lists the number of accounts affected.

3. The company lists the number of pieces of content or URLs affected.

4. The company lists the reasons for removal associated with the requests it receives (e.g., copyright violation, hate speech, incitement to violence, child abuse images, etc.).

5. The company describes the types of parties from which it receives requests (e.g. requests made under a notice-and-takedown system, requests from a non-governmental organization, requests from a voluntary industry self-regulatory body, etc.).

6. The company lists the number of requests it complied with.

7. The company either publishes the original requests or provides copies to a third-party archive such as Chilling Effects or a similar organization.

8. The company reports this data at least once a year.

9. The data reported by the company can be exported as a **structured data** file.

F9. Data about Terms of Service enforcement

Does the company regularly publish information about the volume and nature of actions taken to enforce the company's own **terms of service**?

Checklist elements (select all that apply):

1. The company lists the number of accounts affected.

2. The company lists the number of pieces of content or URLs restricted.

3. The company lists the types of content restricted during the reporting period (e.g., hate speech, harassment, incitement to violence, sexually explicit content, etc.).

4. The company provides examples of why it took action in different types of cases.

5. The company reports this data at least once a year.

6. The data reported by the company can be exported as a **structured data** file.

F10. Network management (telecommunications companies)

Does the company disclose whether it **prioritizes** or degrades **transmission** or **delivery** of different types of **content** (e.g., **traffic shaping** or **throttling**) and if so, for what purpose?

Answer categories (select one):

1. The company discloses that it does not prioritize or degrade the delivery of content.

2. The company discloses that it prioritizes or degrades content delivery and the purpose of doing so.

3. The company discloses that it prioritizes or degrades content delivery but doesn't explain the purpose.

4. The company does not disclose information about prioritizing or degrading the delivery of content.

F11. Identity policy (Internet companies)

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

Answer categories (select one):

1. No

2. Yes

P: Privacy

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

P1. Availability of Privacy Policies

Are the company's **privacy policies freely available** and **easy to understand**?

Checklist elements (select all that apply):

1. Free: The company's privacy policies are **easy to find** and freely available without needing to sign up or subscribe.

2. Language: The privacy policies are available in the language(s) most commonly spoken by the company's users.

3. Easy-to-understand: The policies are presented in an understandable manner.

P2. Privacy Policies, notice and record of changes

Does the company commit to provide meaningful **notice** and **documentation** to users when it changes its **privacy policies**?

Checklist elements (select all that apply):

1. The company discloses the method of direct notification to users (e.g., email, SMS, etc.).

2. The company discloses the time frame within which it provides notification (e.g., two weeks prior to changes occurring).

3. The company maintains a **public archive** or **change log**.

P3. Collection of user information

Does the company disclose what **user information** it **collects**, how it collects this information, and why?

A. The company discloses that it collects no user information.

B. If not, does the company satisfy any of the following elements?

1. **Data minimization**: The company commits to limit collection of user information to what is directly relevant and necessary to accomplish the purpose of its service.
2. The company clearly discloses what user information it collects.
3. The company clearly discloses how it collects user information.
4. The company clearly discloses why it collects user information.

P4. Sharing of user information

Does the company disclose if and why it **shares user information** with **third parties**?

A. The company discloses that it does not share user information.

B. If not, does the company satisfy any of the following elements?

1. The company clearly discloses what user information it shares.
2. The company clearly discloses why it shares user information.
3. The company provides a detailed description of the types of third parties with which it shares user information.
4. The company discloses the names of all third parties with which it shares user information and explains what information it shares with each third party.
5. If the company offers multiple services, it clearly discloses whether and how it will share user information between different services.

P5. User control over information collection and sharing

Does the company provide users with **options to control** the company's **collection** and **sharing** of their information?

Checklist elements (select all that apply):

1. The company provides users with options to control the company's collection of their information.

2. The company provides users with options to control the company's sharing of their information.

P6. Users' access to their own information

Are users able to view, download or otherwise obtain, in **structured data** formats, all of the information about them that the company holds?

Checklist elements (select all that apply):

1. The company allows users to view their data.

2. The company allows users to receive a copy of their data.

3. The data can be downloaded in a structured data format.

4. This data includes all public-facing and private information a company holds about a user.

P7. Retention of user information

Does the company disclose how long it **retains user information**?

A. The company discloses that it does not retain user information.

B. If not, does the company satisfy any of the following elements?

   1. The company discloses that it retains user information (not actively submitted by the user for the purpose of storage or publication) in an **anonymized** form.

   2. The company discloses the types of user information it retains.

   3. The company discloses how long it retains user information.

   4. The company discloses that it deletes all user information after users terminate their account.

P8. Collection of user information from third parties (Internet companies)

Does the company publish clear information about whether it **collects user information** from **third parties**?

A. The company discloses that it does not collect user information from third parties.

B. If not, does the company satisfy any of the following elements?

1. The company clearly explains how it may collect user information from third parties (e.g. use of a widget or advertising service).

2. The company clearly states how it uses the information it collects.

3. The company clearly states how long it retains information it collects.

4. The company respects **user-generated signals** (e.g. "**Do Not Track**" headers) to opt-out of data collection.

P9. Process for responding to third-party requests for user information

Does the company publish information about its process for evaluating and responding to requests from government and other **third parties** for stored **user data** and/or **real-time communications**, including the legal basis for complying with such requests?

Checklist elements (select all that apply):

1. The company explains its process for receiving and responding to **non-judicial government requests**.

2. The company explains its process for responding to **court order**s.

3. The company explains its process for responding to **requests made by private parties**.

4. The company explains its process for responding to requests from foreign jurisdictions.

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

6. The company commits to carry out due diligence on requests before deciding how to respond.

7. The company's process commits to push back on unlawful requests.

8. The company provides guidance or examples of policy implementation.

P10. User notification about third-party requests for user information

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

Checklist elements (select all that apply):

1. The company commits to notify users when **government entities** (including courts or other judicial bodies) request their **user data**.

2. The company commits to notify users when non-government entities request their user data.

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

P11. Data about third-party requests for user information

Does the company regularly publish data about government and other third-party requests for **user information**, plus data about the extent to which the company complies with such requests?

Checklist elements (select all that apply):

1. The company breaks out the number of **user data** and real-time communications access demands it receives by country.

2. The company lists the number of accounts affected.

3. The company lists whether a demand sought communications **content** or **non-content** (e.g., metadata, basic subscriber information, or non-content transactional data) or both.

4. The company identifies the specific legal authority or type of legal process through which law enforcement and national security demands are made.

5. The company includes requests that come from **court orders** or subpoenas (including civil cases).

6. The company includes other non-governmental requests.

7. The company lists the number of requests it complied with, broken down by category of demand.

8. The company lists what types of **government requests** it is prohibited by law from disclosing.

9. The company reports this data at least once per year.

10. The data reported by the company can be exported as a **structured data** file.

P12. Security standards

Does the company deploy industry standards of **encryption** and security for its products and services?

Checklist elements (select all that apply):

1. The company commits to keep up-to-date with the latest encryption and security standards and publishes evidence that it does so.

2. The company commits to address security vulnerabilities when they are discovered and publishes general information about how it does so.

3. The company discloses that it has systems in place to limit and monitor employee access to user information.

4. The company discloses that it regularly conducts security audits on its technologies and practices affecting user information.

5. The company discloses that the transmission of user communications is encrypted by default.

6. The company discloses that it deploys advanced authentication methods to prevent fraudulent access.

P13. Encryption of users' private content (Internet companies)

Can users **encrypt** their own **content** and thereby control who has access to it?

Answer categories (select one):

1. Private user content is encrypted by default; the company itself has no access.
2. The company offers a built-in option to encrypt private content.

3. The company's terms or other policies explain that the user may deploy third party encryption technologies.

4. No disclosure.

5. The company's terms or other policies prohibit encryption.

P14. Inform and educate users about potential threats

Does the company publish information to help users defend against **cyber threats**?

Checklist elements (select all that apply):

1. The company commits to inform users about unusual account activity, most recent account activity, and possible unauthorized access.

2. The company publishes practical materials that educate users on how to protect themselves from cyber threats relevant to their services.

Appendix 1 – Definitions and Key References

Note: **This is not a general glossary. The definitions and explanations provided below were written specifically to guide researchers in evaluating Internet and telecommunications companies on this project's Research Indicators.**

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.

Board-level committee — A committee of the company's board of directors (or similar governing body).

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

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

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

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

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

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

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

Delivery – When data packets reach an end user.

Documentation – The company provides records that users can consult.

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

Easy to find – The information or document is located on the home page of the company or service, or at most, on a page that is one click away from the home page.

Easy to understand & understandable manner – The company has taken steps to help users actually understand the information. 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 intended recipient with the encryption key can decipher the contents of the drive. Additionally, users can send an encrypted email message, which would prevent anyone from seeing the email contents while the message is moving through the network to reach the intended recipient. With encryption in transit (for example visible when a website uses HTTPS), the communication between a user and a website is encrypted, so that outsiders, such as the user's Internet Service Provider can only see the initial visit to the website, but not what the user communicates on that website, or the sub-pages that the user visits.

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

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.

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.

Freely available – A person can see the information without having to sign in, make a purchase, download software, add a plugin or cookie, or otherwise provide information or take action in exchange for viewing the the information.

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

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

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

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

For more information about Human Rights Impact Assessments and best practices in conducting them, see this special page hosted by the Business & Human Rights Resource Centre: *http://www.business-humanrights.org/UNGuidingPrinciplesPortal/ToolsHub/Companies/StepTaken/ImpactAssessment*

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

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

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

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

Managerial-level comment – Comment from company employees with management roles and titles who are not part of the executive team.

Meaningful commitment – The company discusses freedom of expression and privacy in its own materials as well as in external appearances (e.g., presentations, media, etc). The company has discussed freedom of expression and privacy several times, rather than just once. The company responds to free expression and privacy concerns (e.g., making public statements, filing lawsuits, etc).

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

is an example of a multi-stakeholder initiative focused on freedom of expression and privacy.

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

In the U.S., the Stored Communications Act defines non-content customer communications or records as, "name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity (including any temporarily assigned network address); and means and source of payment for such service (including any credit card or bank account number)." The European Union's Handbook on European Data Protection Law states, "Confidentiality of electronic communications pertains not only to the content of a communication but also to traffic data, such as information about who communicated with whom, when and for how long, and location data, such as from where data were communicated."
http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=1100110

Non-judicial government requests – These are requests that come from government entities that are not judicial bodies, judges, or courts. They can include requests from government ministries, agencies, police departments, police officers (acting in official capacity) and other non-judicial government offices, authorities, or entities.

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

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

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.

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

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

Source: "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," U.S. Federal Trade Commission, March 2012, p. 77. *https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf*

Private requests – Requests made by any person or entity not acting under direct governmental or court authority. These requests 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*

Process for enforcing its rules – This includes cases where a company blocks, filters, removes, deletes, or otherwise renders a piece of content inaccessible. It also includes cases where a company shuts down, blocks, or otherwise denies service (either by deleting user accounts or shutting down the service) to an individual or group of individuals due to something the user(s) have done on the service.

Program / Team – 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.

Prominent – The company's disclosure is easy to locate on the company's website.

Prominent venue – This may include public statements or declarations made before a significant public audience, including at a major public conference, in a press interview, in a company blog post, in a public securities filing, etc. This does not include company press releases.

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

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

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

- Expansion of the "pen register" exception in wiretap law
- "Nationwide" pen register warrants
- Pen register searches applied to the Internet

Source: *https://www.aclu.org/surveillance-under-usa-patriot-act?redirect=national-security/surveillance-under-usa-patriot-act*

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

corruption and free from political or other attempts to influence the outcome." (p. 22 of 27.)

Source: "Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie. Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework," 2011. *http://business-humanrights.org/sites/default/files/media/documents/ruggie/ruggie-guiding-principles-21-mar-2011.pdf*

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

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

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

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).

Service restriction – The company blocks, shuts down, or otherwise prevents access to the service. This service restriction can occur for a specific user, a group of users, or users in a particular area.

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.

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

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*

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. (Updated July 10, 2015)

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/*

Transmission – The movement of data packets through a network.

Traffic shaping – Adjusting the flow of traffic through a network. This can involve conditionally slowing certain types of traffic. Traffic shaping can be used for network management purposes (e.g., prioritizing VoIP traffic ahead of normal web traffic to facilitate real-time communication) or for reasons that counter net neutrality principles (e.g., intentionally slowing video traffic to dissuade users from using high-bandwidth applications). (Updated July 10, 2015)

Users – This includes people who post or transmit the content online as well as those who try to access or receive the content.

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

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

User Information — Any data which 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 which 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.

Appendix 2 – Research Guidance

Below are further details explaining how each indicator is evaluated, excerpted from a longer Researcher Guide that all RDR researchers and reviewers are required to follow.

C1

This indicator seeks evidence that the company and the people who lead the company have made public commitments about the importance of freedom of expression and privacy.

Evaluation: This indicator is evaluated in two parts. A company can only receive full credit for this indicator if it receives a "Yes" for part A and "executive-level comment" for part B. We expect to see company commitments that relate to both freedom of expression and privacy.

Potential sources:

- Company human rights policy
- A company's listing of its executive leadership team to identify who the company defines to be executive-level (for element B1). Company organization chart, annual reports, or proxy statements may also identify who is part of the company's executive leadership team.
- Major media outlets
- Recordings or transcripts from public conferences
- Public responses, letters, or other communications with legislators or government agencies
- Public communications with civil society organizations
- Company blog posts (with author clearly listed)

C2

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

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if they disclose information about how they consider these issues at the board, executive, and management levels. At the board level, this would be a committee. Below board-level, it can include a company unit or individual that reports to the executive or managerial level. The committee, program, team, officer, etc. should

specifically identify freedom of expression and privacy in its description of responsibilities.

Potential sources:

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

C3

Indicators C1 and C2 focus on company leaders and decision-makers. This indicator seeks company disclosure about how the company also helps the rest of its employees understand the importance of freedom of expression and privacy. When staffers write code for a new product, review a request for user data, or answer customer questions about how to use a service, they act in ways that can directly affect people's freedom of expression and privacy. We expect companies to disclose information about whether they provide training that informs employees of their role in respecting human rights and that provides employees with an outlet to voice concerns they have regarding human rights.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if they disclose information about employee training on freedom of expression and privacy and they disclose the existence of a whistleblower program that encompasses these issues. Disclosure around employee training should specify that the training covers freedom of expression, privacy, or both.

Potential sources:

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

C4

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

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

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

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

Potential sources:

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

C5

This indicator seeks evidence that company engages with its stakeholders, particularly those who face clear human rights risks in connection with their online activities.

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

Evaluation: A company will only receive full credit for this indicator if it fulfills element A. A company will receive partial credit if it meets one or both of the elements under B.

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

C6

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

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if they demonstrate that their remedy and grievance mechanisms include all elements in the checklist.

Potential sources:

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

.

F1

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

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

Potential sources:

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

F2

It is common for companies to change their terms of service as their business evolves. We expect companies to commit to notify users when they change these terms and to provide users with information to understand what these changes mean. This indicator seeks company disclosure on the method and timeframe within which companies commit to notify users about changes in the terms of service. It also seeks evidence that a company provides publicly available records of previous terms so that people can understand how the company's terms have evolved over time.

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

Potential sources:

- Company terms of service

F3

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. We expect companies to disclose to their users what these rules are and how companies enforce them. This includes legal requirements to block certain types of content as well as restrictions related to intellectual property (e.g., copyright infringement). In this disclosure, the company should also provide examples to help users understand what these rules mean.

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

Potential sources:

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

F4

Indicator F3 examines company disclosure of restrictions on what users can post or do on a service, while this indicator looks at company disclosure of restrictions on a user's ability to access a service. Companies can restrict access to a service by deleting a user's account or by shutting down a service entirely. We expect companies to explain to their users the circumstances under which they might take such action.

Evaluation: This indicator is scored using a checklist, meaning companies can only receive full credit if their disclosure meets all elements in the checklist. Element 2 is only applicable to telecommunications companies; Internet companies will receive a N/A

(non-applicable) score for element 2. Internet companies must fulfill elements 1 and 3 to receive full credit for this indicator.

Potential Sources

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

F5

Indicator F3 examines company disclosure of restrictions on what users can post or do on a service, and indicator F4 looks at company disclosure of restrictions on a user's ability to access a service. This indicator, F5, focuses on whether companies disclose that they notify users when they take these types of actions. We expect companies to disclose a commitment to notify users when they have removed content, restricted a user's account, or otherwise restricted users' abilities to access a service. This disclosure should be part of companies' explanations of content and access restriction practices.

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

Potential sources:

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

F6

Companies increasingly receive requests to remove, filter, or restrict access to content. They also receive requests to restrict access to users or, in rare cases, shut down a network. These requests can come from governments agencies, courts, or private parties. We expect companies to publicly disclose their process explaining how they respond to requests from each type of third party.

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

Potential sources:

- Company transparency report
- Company law enforcement guidelines

- Company terms of service
- Company policy on copyright or intellectual property
- Company help or support center
- Company blog posts

F7

This indicator examines company disclosure of data on the requests it receives from governments to remove content. Publicizing this data helps the public gain a greater understanding of how freedom of expression operates online, and it helps the public hold companies and governments accountable for their respective roles to respect and protect freedom of expression. For these reasons, we expect companies to regularly publish data about the government requests they receive to remove content.

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.

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

Potential sources:

- Company transparency report

F8

This indicator examines company disclosure of data on the requests it receives from private parties (non-governmental and non-judicial) to remove content. We expect companies to regularly publish data about the **private requests** they receive to remove content. (See definition of "private requests" in Appendix 1.)

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

Potential sources:

- Company transparency report

F9

Companies may employ staff to review content and/or user activity or they may rely on community flagging mechanisms through which other users flag content and/or activity for company review. This indicator seeks company disclosure of data on the number of instances a company has removed content or restricted users' access due to violations of the company's terms of service. Publicizing this data will provide the public with a more accurate view of the content removal ecosystem as well as companies' own role in content removal. We expect companies to regularly publish data about their own decisions to remove content.

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

Potential sources:

- Company transparency report

F10

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

Evaluation: Researchers are instructed to select one of four possible answer categories. Only companies that meet the criteria for the first answer category, "The company discloses that it does not prioritize or degrade the delivery of content." will receive full credit for this indicator. Other answer categories receive progressively less credit.

Potential Sources:

- Company explanation of network management or traffic management practices

F11

This indicator is only applicable to Internet companies. We expect companies to disclose whether they might ask users to verify their identities using government-issued ID or other forms of identification that could be connected to their offline identity.

Evaluation: This indicator has two possible answers. A company will receive full credit if its answer is "No," and a company will receive no credit if its answer is "Yes."

Potential sources:

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

P1

Privacy policies address how companies collect, manage, use, and secure information about users as well as information provided by users. We expect companies to provide these policies freely and to make an effort to help users understand what they mean.

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

Potential sources:

- Company privacy policy, data use policy

P2

It is common for companies to change their privacy policies as their business evolves. We expect companies to commit to notify users when they change these policies and to provide users with information to understand what these changes mean. This indicator seeks company disclosure on the method and timeframe within which companies commit to notify users about changes in the privacy policies. It also seeks evidence that a company provides publicly available records of previous policies so that people can understand how the company's policies have evolved over time.

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

Potential sources:

- Company privacy policy, data use policy

P3

We expect companies to clearly disclose whether they collect user information (as we define it), and if so, to provide enough detail that users can understand what information the company collects, how it does so, and its reason for doing so.

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

“User Information is any data which 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 which 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. Our definition is:

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

The expansive nature of this view is necessary to reflect several facts. First, skilled analysts can de-anonymize large data sets. This renders nearly all promises of anonymization unattainable. In essence, any data tied to an ‘anonymous identifier’ is not anonymous; rather, this is often pseudonymous data 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.

Evaluation: If a company’s disclosure states that it does not collect any user information, fulfilling element A, the company receives full credit for the indicator. If a company does not fulfill element A, the researcher will look for company disclosure to meet the checklist elements of B. A company can receive partial credit if its disclosure meets all elements in the B checklist.

In some cases, laws or regulations might require companies to collect certain information or might prohibit or discourage the company from disclosing what user information they collect. Researchers will document situations where this is the case, but a company will still lose points if it fails to meet all elements. This represents a situation where the law causes companies to be uncompetitive, and we encourage

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

Potential sources:

- Company privacy policy (primary source)
- Company section on data protection or data collection (secondary source)

P4

We expect companies to clearly disclose whether they share user information, as we define it, and if so, to provide enough detail that users can understand the scope of this sharing. We expect company disclosure to address company sharing of user information with governments and with commercial entities.

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

"User Information is any data which 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 which 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. Our definition is:

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

The expansive nature of this view is necessary to reflect several facts. First, skilled analysts can de-anonymize large data sets. This renders nearly all promises of anonymization unattainable. In essence, any data tied to an 'anonymous identifier' is not anonymous; rather, this is often pseudonymous data 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.

Evaluation: If a company's disclosure states that it does not share any user information, fulfilling element A, the company receives full credit for the indicator. If a company does not fulfill element A, the researcher will look for company disclosure to meet the checklist elements of B. A company can only receive partial credit if its disclosure meets all elements in the B checklist.

Potential sources:

- Company privacy policy (primary source)
- Company policies related to sharing data, interaction with third parties (secondary source)

P5

We expect companies to proactively provide users with options to control what user information the company collects and shares. Users should be able to access these options after they sign up for the service, not simply at the time of sign-up. Simply signing up for the service does not represent consent.

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

Potential sources:

- Company privacy policy
- Company account settings

P6

We expect companies to give users the ability to view and obtain copies of their data that the company holds. Company disclosure should explain what data this record contains and what formats users can obtain it in.

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

Potential sources:

- Company privacy policy
- Company account settings
- Company help center
- Company blog posts

P7

We expect companies to disclose information pertaining to data retention. When considering user information, companies should be specific about the purpose for which they collect data, use it only for that purpose, and safely discard the data when it's no longer needed for that purpose.

Evaluation: If a company's disclosure states that it does not retain any user information, fulfilling element A, the company receives full credit for the indicator. If a company does not fulfill element A, the researcher will look for company disclosure to meet the checklist elements of B. A company can only receive partial credit if its disclosure meets all elements in the B checklist.

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

P8

We expect companies to disclose what user information they collect from third parties. This helps users understand how their activities outside the service can affect their use of the service.

Evaluation: If a company's disclosure states that it does not collect any user information from third parties, fulfilling element A, the company receives full credit for the indicator. If a company does not fulfill element A, the researcher will look for company disclosure to meet the checklist elements of B. A company can only receive partial credit if its disclosure meets all elements in the B checklist.

Potential sources:

- Company privacy policy
- Company policy on third parties

P9

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

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

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

Potential sources:

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

P10

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

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

Potential sources:

- Company transparency report
- Company law enforcement guidelines

P11

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

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

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

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

Potential sources:

- Company transparency report

P12

Companies can have access to immense amounts of personal information about users, and they should take the highest possible measures to keep this information secure. We expect companies to disclose information about how they keep data secure so that users can make informed decisions about where to send their data.

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

Potential sources:

- Company privacy policies
- Company security guide

P13

This indicator is only applicable to Internet companies. Users entrust significant amounts of their content to online services. Companies should enable users to easily encrypt this data and dramatically increase its security. This indicator focuses on encryption of stored user content, not encryption of the transmission of content. For this reason, the indicator is only applicable to Internet companies.

Evaluation: This is a single-choice indicator, meaning researchers should only select one answer. The answer categories will be scored on a scale. The highest possible score is awarded to answer #1, and companies that meet it will receive full credit. Companies meeting #2 will receive partial credit (percentage to be determined), and companies meeting #3 will receive a smaller percentage of credit. Companies that receive answer #4 or answer #5 will receive zero credit for this indicator.

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

P14

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

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

Potential sources:

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