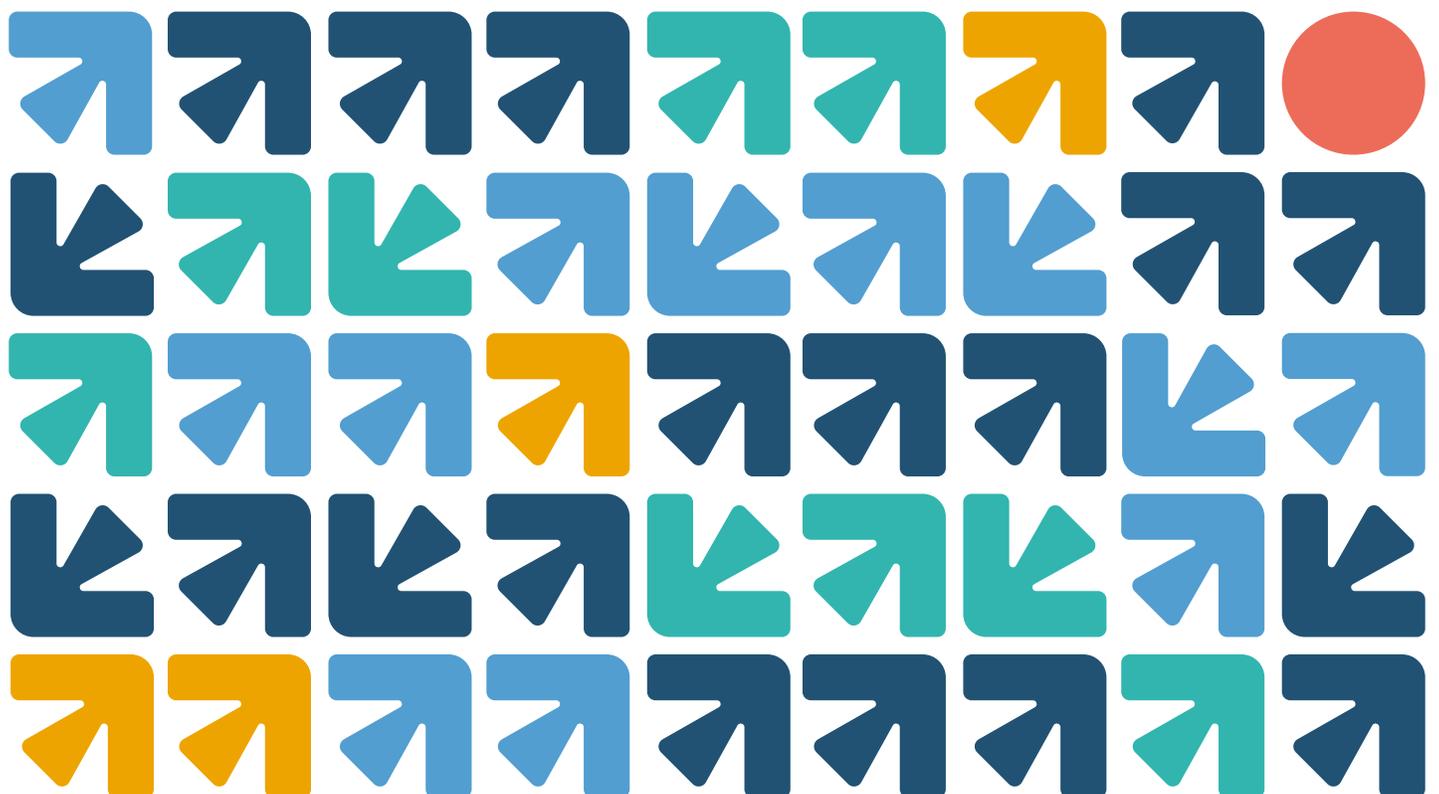


Ranking
Digital
Rights

**Corporate Accountability Index
Research Indicators**

Including indicator guidance and glossary



Acknowledgements

The following Ranking Digital Rights (RDR) team members were involved in the research and stakeholder outreach for the 2020 RDR Corporate Accountability Index methodology:

- Amy Brouillette, Research Director
- Veszna Wessenauer, Research Manager
- Nathalie Maréchal, Senior Policy Analyst
- Afef Abrougui, Research Analyst
- Zak Rogoff, Research Analyst
- Jan Rydzak, Company Engagement Lead and Research Analyst
- Jie Zhang, Research Analyst

For a full list of project staff:

<https://rankingdigitalrights.org/who/>

RDR would like to thank the more than 100 stakeholders who offered essential feedback throughout this methodology development process. We wish also to acknowledge former RDR research team members Laura Reed and Andrea Hackl for key contributions during the initial phase of our methodology expansion work that began in early 2019.

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/>.



Contents

Acknowledgements	1
About Ranking Digital Rights	1
Contents	2
1. About Ranking Digital Rights	5
2. About the RDR Index methodology	5
3. About the 2020 RDR Index methodology revision	6
4. Companies included in the 2020 RDR Index	8
5. Research process	9
6. Evaluation and scoring	10
Governance	12
G1. Policy Commitment	12
G2. Governance and management oversight	13
G3. Internal implementation	14
G4: Human rights due diligence	15
G4(a). Impact assessment: Governments and regulations	15
G4(b). Impact assessment: Processes for policy enforcement	17
G4(c) Impact assessment: Targeted advertising	18
G4(d). Impact assessment: Algorithmic systems	19
G4(e) Impact assessment: Zero-rating	21
G5. Stakeholder engagement and accountability	23
G6. Remedy and appeals	24
G6(a). Remedy	24
G6(b). Process for content moderation appeals	26
Freedom of Expression and Information	28
F1: Access to policies	28
F1(a). Access to terms of service	28
F1(b). Access to advertising content policies	29
F1(c). Access to advertising targeting policies	30
F1(d). Access to algorithmic system use policies	31
F2: Notification of policy changes	32
F2(a). Changes to terms of service	32



F2(b). Changes to advertising content policies	33
F2(c). Changes to advertising targeting policies	34
F2(d). Changes to algorithmic system use policies	35
F3: Process for policy enforcement	36
F3(a). Process for terms of service enforcement	36
F3(b). Advertising content rules and enforcement	37
F3(c). Advertising targeting rules and enforcement	38
F4: Data about policy enforcement	39
F4(a). Data about content restrictions to enforce terms of service	39
F4(b). Data about account restrictions to enforce terms of service	40
F4(c). Data about advertising content and advertising targeting policy enforcement	41
F5: Process for responding to third-party requests to restrict content or accounts	42
F5(a). Process for responding to government demands to restrict content or accounts	42
F5(b). Process for responding to private requests for content or account restriction	43
F6. Data about government demands to restrict for content and accounts	44
F7. Data about private requests for content or account restriction	45
F8. User notification about content and account restriction	46
F9. Network management (telecommunications companies)	47
F10. Network shutdown (telecommunications companies)	48
F11. Identity policy	49
F12. Algorithmic content curation, recommendation, and/or ranking systems	50
F13. Automated software agents (“bots”)	51
Privacy	54
P1: Access to policies affecting users’ privacy	54
P1(a). Access to privacy policies	54
P1(b). Access to algorithmic system development policies	55
P2: Notification of changes	56
P2(a). Changes to privacy policies	56



P2(b). Changes to algorithmic system development policies	57
P3: User information collection and inference	58
P3(a). Collection of user information	58
P3(b). Inference of user information	59
P4. Sharing of user information	60
P5. Purpose for collecting, inferring, and sharing user information	61
P6. Retention of user information	61
P7. Users' control over their own user information	63
P8. Users' access to their own user information	64
P9. Collection of user information from third parties	66
P10. Process for responding to demands for user information	67
P10(a). Process for responding to government demands for user information	67
P10(b). Process for responding to private requests for user information	68
P11. Data about demands for user information	69
P11(a). Data about government demands for user information	69
P11(b). Data about private requests for user information	70
P12. User notification about third-party requests for user information	71
P13. Security oversight	72
P14. Addressing security vulnerabilities	72
P15. Data breaches	74
P16. Encryption of user communication and private content (digital platforms)	74
P17. Account security (digital platforms)	75
P18. Inform and educate users about potential risks	76
Glossary	77



1. About Ranking Digital Rights

[Ranking Digital Rights](#) (RDR) works to promote freedom of expression and privacy on the internet by creating global standards and incentives for companies to respect and protect users' rights. We do this by producing the Ranking Digital Rights Corporate Accountability Index, which evaluates the world's most powerful digital platforms and telecommunications companies on relevant commitments and policies, based on international human rights standards. We work with companies as well as advocates, researchers, investors, and policymakers to establish and advance global standards for corporate accountability.

The RDR Corporate Accountability Index offers a roadmap for companies to build and operate internet platforms and services that respect and protect human rights. The 2019 RDR Index ranked 24 companies on 35 indicators,¹ using a rigorous, seven-step [research process](#) and an [open methodology](#) that looked at companies' governance mechanisms to identify and prevent potential threats to users' human rights, alongside companies' disclosed policies affecting users' freedom of expression and privacy.

2. About the RDR Index methodology

The standards the RDR Index uses to measure companies are built on more than a decade of work by the human rights, privacy, and security communities. These standards include the [U.N. 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 RDR 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 RDR Index methodology has been developed over years of research, testing, and consultation. Since its inception, the project has engaged closely with researchers around the globe. For the initial methodology development, pilot study, and the inaugural RDR Index, we also partnered with Sustainalytics, a leading provider of environmental, social, and governance (ESG) research to investors.

¹ 2019 RDR Index, May 2019, <https://rankingdigitalrights.org/index2019/>.



Previous iterations of the RDR Index:

- In 2015, we launched the inaugural RDR Index, which [ranked](#) 16 internet and telecommunications companies on [31 indicators](#).
- The [2017 RDR Index](#) expanded the ranking to [22 companies](#), which included all of the companies ranked in 2015, plus an additional six companies. Along with internet and telecommunications companies, the RDR Index was expanded to include new types of services, including those that produce software and devices that we call “[mobile ecosystems](#).” As a result, we [further revised the 2017 methodology](#) based on a detailed review of the raw data from the 2015 RDR Index as well as consultations with stakeholders from civil society, academia, investors, and companies.
- The [2018 RDR Index](#) applied the same methodology to evaluate the same [22 companies](#) as in the 2017 Index. This enabled us to produce comparative analyses of each company’s performance and to track overall trends.
- The [2019 RDR Index](#) methodology introduced changes to two indicators in the Governance category.² These revisions were aimed at introducing baseline standards for identifying and mitigating human rights risks associated with companies’ use of algorithms and for their targeted advertising policies and practices. We also revised one indicator (Indicator G6) in order to strengthen and clarify our evaluation of company grievance and remedy mechanisms and procedures.³ In addition, the 2019 RDR Index expanded to include two new companies⁴—Deutsche Telekom and Telenor—and five additional cloud services.

3. About the 2020 RDR Index methodology revision

Since its launch in 2015, the RDR Index has contributed to improved company disclosure of policy and practice across a number of areas, including transparency reporting, content removals, account restrictions, network shutdowns, and handling and securing user information. However, given the geopolitical and technological developments with clear human rights implications that have taken place in the years since the RDR Index methodology was first developed, it has become clear that the methodology needs to be updated if companies are to be held fully accountable for the range of potential online threats to human rights.

² “2019 Corporate Accountability Index Research Indicators,” *Ranking Digital Rights*, September 2019, <https://rankingdigitalrights.org/index2019/assets/static/download/RDRindex2019indicators.pdf>

³ “Proposed revisions to the 2019 Corporate Accountability Index methodology (consultation draft),” *Ranking Digital Rights*, July 2018, <https://rankingdigitalrights.org/wp-content/uploads/2018/06/2019-Index-Methodology - Consultation-Draft.pdf>

⁴ See 2019 company list: <https://rankingdigitalrights.org/2019-companies/>.



In January 2019, RDR began a process of expanding and revising the methodology to include new issue areas and new company types.⁵ This work has focused on three main areas:

- **Improving 2019 RDR Index methodology:** We reviewed the 2019 RDR Index methodology to identify key areas for revision and improvement.
- **Incorporating new indicators on targeted advertising and algorithms:** Since early 2019, RDR has been developing new indicators that set global accountability and transparency standards for how companies can demonstrate respect for human rights online as they develop and deploy these new technologies. In October 2019, RDR published [draft indicators on targeted advertising and algorithms](#), based on nearly a year of internal research and incorporating feedback from more than 90 expert stakeholders. These draft indicators were pilot-tested by the RDR research team. The results of this pilot study were published in [March 2020](#).
- **Incorporating new companies:** In early 2019, we began the process of research and public consultation on ways to expand the RDR Index to include Amazon and Alibaba. This process laid the groundwork for incorporating two new services—e-commerce platforms and “personal digital assistant ecosystems”—into the 2020 RDR Index methodology.

In April 2020, RDR published a draft version of the final 2020 RDR Index methodology, which integrated work across these three areas.⁶ We then opened a final round of public consultation to solicit key feedback from stakeholders, which informed decisions we made as we finalized the methodology.

To read a summary of key changes to the 2020 RDR Index methodology:
<https://rankingdigitalrights.org/wp-content/uploads/2020/06/2020-methodology-revision-final-summary.pdf>

To learn more about our methodology development process:
<https://rankingdigitalrights.org/methodology-development/>

⁵“RDR 2019 Index Launch Slated for May; Big Plans Ahead,” *Ranking Digital Rights*, February 2019, <https://rankingdigitalrights.org/2019/02/13/rdr-2019-index-launch-plans/>

⁶ “2020 Ranking Digital Rights Corporate Accountability Index Draft Indicators,” *Ranking Digital Rights*, April 2020, <https://rankingdigitalrights.org/wp-content/uploads/2020/04/2020-draft-methodology-redline-version.pdf>

4. Companies included in the 2020 RDR Index

The 2020 RDR Index will evaluate 26 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).

Digital platform companies: The 2020 RDR Index will evaluate 14 digital platform companies. This includes all of the 12 digital platform companies evaluated previously plus two new companies (Amazon and Alibaba). As noted above, due to the expansion of the 2020 RDR Index to include new services offered by Amazon and Alibaba—specifically, e-commerce platforms and personal digital assistant ecosystems—we have renamed the “internet and mobile ecosystem” category to “digital platforms,” the scope of which includes a range of products and services offered by internet companies, as well as mobile ecosystems, e-commerce platforms, and personal digital assistant ecosystems.

For each of these companies we evaluate global group-level policies for relevant indicators plus policies of the companies’ home market. (For example: we evaluate Facebook’s privacy policy that is applicable to users in the U.S.)

For each company we examine up to five services, as follows:

- **Alibaba (China)** — Taobao.com (e-commerce platform); AliGenie (personal digital assistant ecosystem)
- **Amazon (US)** — Amazon.com (e-commerce platform); Amazon Alexa (personal digital assistant ecosystem), Amazon Drive
- **Apple (US)** — iOS mobile ecosystem, iMessage, iCloud
- **Baidu (China)** — Baidu Search, Baidu Cloud, Baidu PostBar
- **Facebook (US)** — Facebook, Instagram, WhatsApp, Messenger
- **Google (US)** — Search, Gmail, Youtube, Android mobile ecosystem, Google Drive
- **Kakao (South Korea)** — Kakao Search, Kakao Mail, KakaoTalk
- **Mail.Ru (Russia)** — V Kontakte, Mail.ru email, Mail.ru Agent messaging, Mail.Ru Cloud
- **Microsoft (US)** — Bing, Outlook.com, Skype, OneDrive



- **Oath (US)** — Yahoo Mail, Tumblr
- **Samsung (South Korea)** — Samsung implementation of Android, Samsung Cloud
- **Tencent (China)** — QZone, QQ, WeChat, Tencent Cloud
- **Twitter (US)** — Twitter
- **Yandex (Russia)** — Yandex Mail, Yandex Search, Yandex Disk (cloud storage)

Telecommunications companies: The 2020 RDR Index will rank all of the 12 telecommunications companies we previously ranked. No new telecommunications companies have been added for the 2020 research cycle.

For each of 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):** Telcel (pre- and postpaid mobile)
- **AT&T (U.S.):** AT&T (pre- and postpaid mobile, broadband)
- **Axiata (Malaysia):** Celcom (pre- and postpaid mobile, broadband)
- **Bharti Airtel (India):** Airtel India (pre- and postpaid mobile, broadband)
- **Deutsche Telekom AG (Germany):** Deutsche Telekom (pre- and postpaid mobile, broadband)
- **Etisalat (UAE):** Etisalat UAE (pre- and postpaid mobile, broadband)
- **MTN (South Africa):** MTN South Africa (pre- and postpaid mobile, broadband)
- **Ooredoo (Qatar):** Ooredoo Qatar (pre- and postpaid mobile, broadband)
- **Orange (France):** Orange France (pre- and postpaid mobile, broadband)
- **Telefónica (Spain):** Movistar (pre- and postpaid mobile, broadband)
- **Telenor ASA (Norway):** Telenor (pre- and postpaid mobile, broadband)
- **Vodafone (UK):** Vodafone UK (pre- and postpaid mobile, broadband)

5. Research process

The RDR Index is produced using a rigorous seven-step process of data collection, cross-checking, and review. Research is carried out by a network of more than 30 researchers from around the world. Steps for the 2020 RDR Index are outlined below:

- ▶ **Step 1: Primary Data Collection.** At this step, primary researchers are responsible for verifying results of the previous (2019) RDR Index. If the company policy has changed, or for new indicators and elements, primary researchers are responsible



for evaluating those policies. Step 1 researchers will also conduct an evaluation of how the (current) policy compares to the previous (2019) RDR Index.

- ▶ **Step 2: Secondary Review:** At this step, secondary reviewers will fact check the assessments provided by primary researchers in Step 1, including agreeing or disagreeing with the year-on-year-analysis.
- ▶ **Step 3: Review and Reconciliation:** RDR team will discuss the results from Steps 1 and 2 and resolve any differences that arise.
- ▶ **Step 4: Company Feedback.** At this step, companies have the opportunity to review the preliminary evaluation and provide feedback to the RDR team. The team evaluates the input from companies to determine if it warrants a change in the evaluation.
- ▶ **Step 5: Processing company feedback.** RDR considers the feedback from companies, and makes any adjustments to evaluations, as needed.
- ▶ **Step 6: Horizontal Review.** The RDR team will conduct a horizontal review, drawing in feedback from companies collected in Step 4, and cross-checking the indicators to ensure they have been evaluated consistently across each company.
- ▶ **Step 7: Final Scoring:** RDR team assigns final scores. Evaluations include if the company's policy or disclosure has changed from the previous previous year's evaluation

6. Evaluation and scoring

The 2020 RDR Index cycle evaluates company policies that have been active from January 25, 2019 to September 14, 2020. Companies receive a cumulative score of their performance across all RDR Index categories, and results show how companies performed by each category and indicator.

Each indicator has a list of elements, and companies receive credit (full, partial, or no credit) for each element they fulfill. The evaluation includes an assessment of disclosure for every element of each indicator, based on one of the following possible answers:

- **“Yes”/ full disclosure.** Company disclosure meets the element requirement.



- **“Partial.”** Company disclosure has met some but not all aspects of the element, or the disclosure is not comprehensive enough to satisfy the full scope of the what the element is asking for.
- **“No disclosure found.”** Researchers were not able to find information provided by the company on their website that answers the element question.
- **“No.”** Company disclosure exists, but it specifically does not disclose to users what the element is asking. This is distinct from the option of “no disclosure found,” although both result in no credit.
- **“N/A.”** Not applicable. This element does not apply to the company or service. Elements marked as N/A will not be counted for or against a company in the scoring process.

Points

- Yes/full disclosure = 100
- Partial = 50
- No = 0
- No disclosure found = 0
- N/A excluded from the score and averages



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,⁷ and are enshrined in the International Covenant on Civil and Political Rights.⁸ They apply online as well as offline.⁹ In order for a company to perform well in this category, the company's disclosure should at least follow, and ideally surpass, the U.N. Guiding Principles on Business and Human Rights¹⁰ and other industry-specific human rights standards focused on freedom of expression and privacy such as those adopted by the Global Network Initiative.¹¹

G1. Policy Commitment

The company should publish a formal **policy commitment** to respect users' human rights to freedom of expression and information and privacy.

Elements:

1. Does the company make an **explicit**, clearly articulated **policy commitment** to human rights, including to freedom of expression and information?
2. Does the company make an **explicit**, clearly articulated **policy commitment** to human rights, including to privacy?
3. Does the company disclose an **explicit**, clearly articulated **policy commitment** to human rights in its development and use of **algorithmic systems**?

Indicator guidance: This indicator seeks evidence that the company has made explicit policy commitments to freedom of expression and information, and to privacy. These standards are outlined in the U.N. 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.¹²

⁷ "Universal Declaration of Human Rights," <https://www.un.org/en/universal-declaration-human-rights/>

⁸ "International Covenant on Civil and Political Rights," *UN Human Rights Office of the High Commissioner*, <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

⁹ UN Human Rights Council, *Resolution adopted by the Human Rights Council on 27 June 2016 - Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development*, available at: <https://daccess-ods.un.org/TMP/2969264.09006119.html>

¹⁰ "Guiding Principles on Business and Human Rights," *UN Human Rights Office of the High Commissioner*, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

¹¹ "The GNI Principles," *Global Network Initiative*, <https://globalnetworkinitiative.org/gni-principles/>.

¹² "Guiding Principles on Business and Human Rights," *UN Human Rights Office of the High Commissioner*, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

Companies should also publish a formal commitment to uphold human rights as they develop and deploy algorithmic decision making systems, in line with Council of Europe recommendations, in its [Recommendation on the human rights impacts of algorithmic systems](#) (2020). The company should clearly disclose these commitments in formal policy documents or other communications that reflect official company policy.

Potential sources:

- Company human rights policy
- Company statements, reports, or other communications that reflect official company policy
- Company annual report or sustainability report
- Company “AI principles” policy

G2. Governance and management oversight

The company’s **senior leadership** should exercise **oversight** over how its policies and practices affect freedom of expression and information, 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 information?
2. Does the company **clearly disclose** that the **board of directors** exercises formal **oversight** over how company practices affect privacy?
3. Does the company **clearly disclose** that an **executive-level** committee, team, program or officer **oversees** how company practices affect freedom of expression and information?
4. Does the company **clearly disclose** that an **executive-level** committee, team, program or officer **oversees** how company practices affect privacy?
5. Does the company **clearly disclose** that a **management-level** committee, team, program or officer **oversees** how company practices affect freedom of expression and information?
6. Does the company **clearly disclose** that a **management-level** committee, team, program or officer **oversees** how company practices affect privacy?

Indicator guidance: This indicator seeks evidence that the company has strong governance and oversight over freedom of expression and information and privacy issues at all levels of its operations. Companies should clearly disclose that senior leadership—from the board to



management level—oversees and is accountable for its policies and practices affecting these human rights.

To receive full credit for this indicator, companies need to clearly disclose that at each governance level (board, executive, managerial), there is clear oversight of both freedom of expression and information, and privacy issues. At the board level, this oversight could include a board of directors or another public explanation of how the board exercises oversight over these issues. Below board level, it can include a company unit, program, 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)

G3. Internal implementation

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

Elements:

1. Does the company **clearly disclose** that it provides employee training on freedom of expression and information issues?
2. Does the company **clearly disclose** that it provides employee training on privacy issues?
3. 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 information rights?
4. 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' privacy rights?



Indicator guidance: Indicator G2 evaluates whether a company’s senior leadership commits to overseeing freedom of expression and privacy issues. This indicator, G3, evaluates if the company discloses whether and how these commitments are institutionalized across the company. More specifically, this indicator seeks disclosure of whether and how the company helps 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 users’ 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 information, and privacy, as well as the existence of whistleblower programs addressing 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: Human rights due diligence

G4(a). Impact assessment: Governments and regulations

Companies should conduct regular, comprehensive, and credible due diligence, through robust **human rights impact assessments**, to identify how government regulations and policies affect freedom of expression and information and privacy, and to mitigate any risks posed by those impacts in the jurisdictions in which it operates.

Elements:

1. Does the company **assess** how laws affect freedom of expression and information in jurisdictions where it operates?
2. Does the company **assess** how laws affect privacy in jurisdictions where it operates?



3. Does the company **assess** freedom of expression and information risks associated with existing products and services in jurisdictions where it operates?
4. Does the company **assess** privacy risks associated with existing products and services in jurisdictions where it operates?
5. Does the company **assess** freedom of expression and information risks associated with a new activity, including the launch and/or acquisition of new products, services, or companies, or entry into new markets or jurisdictions?
6. Does the company **assess** privacy risks associated with a new activity, including the launch and/or acquisition of new products, services, or companies, or entry into new markets or jurisdictions?
7. Does the company conduct additional evaluation whenever the company's **risk assessments** identify concerns?
8. 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?
9. Does the company conduct **assessments** on a regular schedule?
10. Are the company's **assessments** assured by an external **third party**?
11. Is the external **third party** that assures the **assessment** accredited to a relevant and reputable human rights standard by a credible organization?

Indicator guidance: This indicator examines whether companies conduct regular, robust, and accountable human rights risk assessments of government regulations and policies in the jurisdictions in which they operate. These assessments should be part of the company's formal, systematic due diligence activities that are aimed at ensuring that their decisions and practices do not cause, contribute to, or exacerbate human rights harms. Assessments enable companies to identify possible risks to users' freedom of expression and privacy rights and to take steps to mitigate possible harms if they are identified.

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

Potential sources:

- Company CSR/sustainability reports
- Company human rights policy
- Global Network Initiative assessment reports



G4(b). Impact assessment: Processes for policy enforcement

The company should conduct regular, comprehensive, and credible due diligence, such as through robust **human rights impact assessments**, to identify how its processes for policy enforcement affect users' fundamental rights to freedom of expression and information, to privacy, and to non-discrimination, and to mitigate any risks posed by those impacts.

Elements:

1. Does the company **assess** freedom of expression and information risks of enforcing its terms of service?
2. Does the company conduct **risk assessments** of its enforcement of its privacy policies?
3. Does the company **assess** discrimination risks associated with its processes for enforcing its **terms of service**?
4. Does the company **assess discrimination** risks associated with its processes for enforcing its **privacy policies**?
5. Does the company conduct additional evaluation whenever 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: This indicator examines whether companies disclose if they conduct robust, regular, and accountable human rights risk assessments of the impact of their own policies on users' fundamental rights to freedom of expression, privacy, and non-discrimination. These assessments should be part of the company's formal, systematic due diligence activities that are aimed at ensuring that a company's decisions and practices do not cause, contribute to, or exacerbate human rights harms. Assessments enable



companies to identify possible risks of their own policies to users' rights to expression and information, privacy, and to non-discrimination, and to take steps to mitigate possible harms if they are identified.

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

Potential sources:

- Company CSR/sustainability reports
- Company human rights policy
- Global Network Initiative assessment reports

G4(c) Impact assessment: Targeted advertising

The company should conduct regular, comprehensive, and credible due diligence, such as through robust **human rights impact assessments**, to identify how all aspects of its **targeted advertising** policies and practices affect users' fundamental rights to freedom of expression and information, to privacy, and to non-discrimination, and to mitigate any risks posed by those impacts.

Elements:

1. Does the company **assess** freedom of expression and information risks associated with its **targeted advertising** policies and practices?
2. Does the company **assess** privacy risks associated with its **targeted advertising** policies and practices?
3. Does the company **assess** discrimination risks associated with its **targeted advertising** policies and practices?
4. Does the company conduct additional evaluation whenever the company's **risk assessments** identify concerns?
5. 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?
6. Does the company conduct **assessments** on a regular schedule?
7. Are the company's **assessments** assured by an external **third party**?

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

Indicator guidance: Targeted advertising can have adverse affects on human rights, specifically on users’ rights to freedom of information, and freedom from discrimination.¹³ Discrimination occurs when platforms allow third-party advertisers to show different advertisements to different users on the basis of disclosed and inferred information, including membership in protected categories (race, ethnicity, age, gender identity and expression, sexual orientation, health, disability, etc.). Discrimination need not be illegal or immediately harmful to result in harmful effects at scale, such as at the population level or over the course of an individual’s lifetime. Considering the fact that targeted advertisements are less transparent than other forms of advertisement and companies’ significant financial incentives to deploy the technology quickly, these potential rights harms need to be considered in risk assessments.

This indicator examines whether companies disclose if they conduct robust, regular, and accountable human rights risk assesments of the impact of targeted advertising on users’ fundamental rights to freedom of expression and information, privacy, and non-discrimination. These assessments should be part of the company’s formal, systematic due diligence activities that are aimed at ensuring that a company’s decisions and practices do not cause, contribute to, or exacerbate human rights harms. Assessments enable companies to identify possible risks of targeted advertising policies and practices on users’ human rights and to take steps to mitigate possible harms if they are identified.

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

Potential sources:

- Company CSR/sustainability reports
- Company human rights policy
- Global Network Initiative assessment reports

G4(d). Impact assessment: Algorithmic systems

The company should conduct regular, comprehensive, and credible due diligence, such as through robust **human rights impact assessments**, to identify how all aspects of its policies and practices related to the development and use of **algorithmic systems** affect users’

¹³ “Human Rights Risk Scenarios: Targeted advertising,” *Ranking Digital Rights*, February 2019, <https://rankingdigitalrights.org/wp-content/uploads/2019/02/Human-Rights-Risk-Scenarios-targeted-advertising.pdf>.



fundamental rights to freedom of expression and information, to privacy, and to **non-discrimination**, and to mitigate any risks posed by those impacts.

Elements:

1. Does the company **assess** freedom of expression and information risks associated with its development and use of **algorithmic systems**?
2. Does the company **assess** privacy risks associated with its development and use of **algorithmic systems**?
3. Does the company **assess discrimination** risks associated with its development and use of **algorithmic systems**?
4. Does the company conduct additional evaluation whenever the company's **risk assessments** identify concerns?
5. 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?
6. Does the company conduct **assessments** on a regular schedule?
7. Are the company's **assessments** assured by an external **third party**?
8. Is the external **third party** that assures the **assessment** accredited to a relevant and reputable human rights standard by a credible organization?

Indicator guidance: There are a variety of ways in which algorithmic systems may pose harms to human rights.¹⁴ The development of such systems can rely on user information, often without the knowledge or explicit, informed consent of the data subject, constituting a privacy violation. Such systems can also cause or contribute to expression and information harms. In addition, the purpose of many algorithmic decision-making systems is to automate the personalization of users' experiences on the basis of collected and inferred user information, which may cause or contribute to discrimination. Companies should therefore conduct human rights risk assessments related to their development and use of algorithms, as recommended by the Council of Europe in its [Recommendation on the human rights impacts of algorithmic systems](#) (2020).

This indicator examines whether companies conduct robust, regular, and accountable

¹⁴ "Human Rights Risk Scenarios: Algorithms, machine learning and automated decision-making," *Ranking Digital Rights*, July 2019, <https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios -algorithms-machine-learning-automated-decision-making.pdf>.



human rights risk assessments that evaluate their policies and practices relating to their development and deployment of algorithmic systems. These assessments should be part of the company's formal, systematic due diligence activities that are aimed at ensuring that a company's decisions and practices do not cause, contribute to, or exacerbate human rights harms. Assessments enable companies to identify possible risks of their development and deployment of algorithmic systems on users' human rights and to take steps to mitigate possible harms if they are identified.

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

Potential sources:

- Company CSR/sustainability reports
- Company human rights policy
- Global Network Initiative assessment reports

G4(e) Impact assessment: Zero-rating

If the company engages in **zero-rating**, it should conduct regular, comprehensive, and credible due diligence, such as through robust **human rights impact assessments**, to identify how all aspects of its zero-rating policies and practices affect users' fundamental rights to freedom of expression and information, to privacy, and to freedom from discrimination, and to mitigate any risks posed by those impacts.

Elements:

1. Does the company assess freedom of expression and information risks associated with its **zero-rating** programs?
2. Does the company assess privacy risks associated with its **zero-rating** programs?
3. Does the company assess discrimination risks associated with its **zero-rating** programs?
4. Does the company conduct additional evaluation wherever the company's **risk assessments** identify concerns?
5. 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?



6. Does the company conduct assessments on a regular schedule?
7. Are the company's assessments assured by an external **third party**?
8. Is the external **third party** that assures the assessment accredited to a relevant and reputable human rights standard by a credible organization?

Indicator guidance: “Zero-rating” refers to programs—which can be offered by both telecommunications companies and by platforms in partnership with telecommunications companies—that provide access to certain online services or platforms without counting against a person’s data plan. Many telecommunications providers, including RDR-ranked companies, offer such programs, either as the sole provider of the program or in partnership with social media platforms, such as Facebook’s “Free Basics.” These types of programs are a form of network prioritization that undermine net neutrality principles—and can trigger a range of other possible human rights harms, including by undermining the right to freedom of expression and information. In addition, Global Voices Advox has identified Facebook’s Free Basics as “a mechanism for collecting profitable data from users” ([Global Voices, 2017](#)), raising serious privacy concerns about the program. Zero-rating programs can also be discriminatory in the sense that they prioritize certain types of data over others, either on the basis of the protocol in question (HTTP, HTTPS, VoIP, etc.) or on the basis of the content (i.e., prioritizing one social networking site over another). This discrimination (against types of data) can in turn lead to human rights harms that affect people based on their personal characteristics, including gender, race or ethnicity, language(s) spoken, and myriad other traits.

This indicator examines whether companies conduct robust, regular, and accountable impact assessments of the effects of zero-rating programs on users’ human rights. Companies that offer such programs should conduct assessments of how these programs may impact users’ rights to expression and information, privacy, and non-discrimination. These assessments should be part of the company’s formal, systematic due diligence activities that are aimed at ensuring that a company’s decisions and practices do not cause, contribute to, or exacerbate human rights harms. Assessments enable companies to identify possible risks of zero-rating programs and to take steps to mitigate possible harms if they are identified.

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

Potential sources:

- Company CSR/sustainability reports



- Company human rights policy
- Global Network Initiative assessment reports

G5. Stakeholder engagement and accountability

The company should **engage** with a range of **stakeholders** on the company's impact on freedom of expression and information, privacy, and potential risks of related human rights harms such as **discrimination**.

Elements:

1. Is the company a member of one or more **multi-stakeholder initiatives** that address the full range of ways in which users' fundamental rights to freedom of expression and information, privacy, and non-discrimination may be affected in the course of the company's operations?
2. If the company is not a member of one or more such **multi-stakeholder initiatives**, is the company a member of any organizations that engages systematically and on a regular basis with non-industry and non-governmental stakeholders on freedom of expression and privacy issues?
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 rights to freedom of expression and information and to privacy are directly impacted by the company's business?

Indicator guidance: This indicator seeks evidence that the company engages with and is accountable to its stakeholders—particularly with those who face 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 information, privacy, and related rights, including a company's process for developing terms of service, privacy, and identity policies, as well as algorithmic use policies and policies governing targeted advertising, along with the enforcement practices for those policies. Stakeholder engagement and accountability mechanisms should include the full range of ways in which users' rights may be violated: government demands, actions by other third parties via the companies' products and services, or by the companies themselves. Companies that receive full credit on this indicator will not only engage with stakeholders but also commit to accountability processes such as independent assessments overseen by a body whose final decisions are not controlled by companies alone.



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 a 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 and that the engagement produces actual results is through its involvement in a multi-stakeholder initiative whose purpose is not only to create a safe space for engagement, but also to enable companies to make commitments, support them in meeting them, and hold companies accountable to them. Full and credible accountability mechanisms require multi-stakeholder governance in which companies alone do not control decision making regarding accountability processes and engagements, but rather share decision-making authority with representatives of other stakeholder constituencies.

If a company receives full credit on Element 1, it will automatically receive full credit on Element 2 and Element 3. Note that because the scope of the Global Network Initiative's work focuses on government demands, and at least half of RDR's methodology addresses human rights threats that do not originate from governments, for the 2020 RDR Index GNI membership (without evidence of engagement and accountability on other human rights risks beyond those posed by governments) will only result in partial credit for Element 1 of this indicator.

Potential sources:

- Company CSR/sustainability report
- Company annual report
- Company blog
- Company FAQ or Help Center

G6. Remedy and appeals

G6(a). Remedy

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

Elements:

1. Does the company **clearly disclose** it has a **grievance mechanism(s)** enabling users to submit complaints if they feel their freedom of expression and information rights have been adversely affected by the company's policies or practices?
2. Does the company **clearly disclose** it has a **grievance mechanism(s)** enabling users to submit complaints if they feel their privacy has been adversely affected by the company's policies or practices?



3. Does the company **clearly disclose** its procedures for providing **remedy** for freedom of expression and information-related **grievances**?
4. Does the company **clearly disclose** its procedures for providing **remedy** for privacy-related **grievances**?
5. Does the company **clearly disclose** timeframes for its **grievance** and **remedy** procedures?
6. Does the company **clearly disclose** the number of complaints received related to freedom of expression?
7. Does the company **clearly disclose** the number of complaints received related to privacy?
8. Does the company **clearly disclose** evidence that it is providing **remedy** for freedom of expression **grievances**?
9. Does the company **clearly disclose** evidence that it is providing **remedy** for privacy **grievances**?

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 publicly disclosed processes for responding to grievances from individuals who believe that the company has violated or directly facilitated violations of their freedom of expression or privacy.

We expect companies to clearly disclose a grievance mechanism enabling users to submit complaints if they feel their freedom of expression and privacy have been infringed by the company's policies or practices. To receive full credit on Element 1, a company's grievance mechanism does not have to explicitly state that it applies to freedom of expression and privacy related complaints. However it should be clear that this mechanism can be used to file any type of human rights-related grievance. We also expect a company's grievance mechanism to be clearly accessible to users. In addition, the company should explain its process for providing remedy to these types of complaints, and disclose evidence of doing so. Companies should describe clear timelines for addressing each stage of the grievance and remedy processes. These standards are outlined in Principle 31 of the UN Guiding Principles on Business and Human Rights, which states that businesses should publish clear, accessible, and predictable remedy procedures.¹⁵

Potential sources:

¹⁵ "Guiding Principles on Business and Human Rights," *UN Human Rights Office of the High Commissioner*, 2011, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

- 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)
- Company advertising policies

G6(b). Process for content moderation appeals

The company should offer users clear and predictable **appeals** mechanisms and processes for appealing **content-moderation actions**.

Elements:

1. Does the company **clearly disclose** that it offers **affected users** the ability to **appeal content-moderation actions**?
2. Does the company **clearly disclose** that it **notifies** the users who are **affected** by a **content-moderation action**?
3. Does the company **clearly disclose** a timeframe for **notifying affected users** when it takes a **content-moderation action**?
4. Does the company **clearly disclose** when **appeals** are not permitted?
5. Does the company **clearly disclose** its process for reviewing **appeals**?
6. Does the company **clearly disclose** its timeframe for reviewing **appeals**?
7. Does the company **clearly disclose** that such appeals are reviewed by at least one human not involved in the original **content-moderation action**?
8. Does the company **clearly disclose** what role automation plays in reviewing **appeals**?
9. Does the company **clearly disclose** that the **affected users** have an opportunity to present additional information that will be considered in the review?
10. Does the company **clearly disclose** that it provides the **affected users** with a statement outlining the reason for its decision?
11. Does the company **clearly disclose** evidence that it is addressing content moderation **appeals**?



Indicator guidance: No matter how carefully a platform crafts its terms of service, mistakes are inevitable in the demanding and subjective endeavor of content moderation. This is particularly true when content moderation is scaled rapidly through the use of automation. To respect users' freedom of expression and information rights, companies should provide a robust and transparent appeals system that enables users to appeal decisions made by the company that directly influence users' ability to exercise these rights. Companies should clearly disclose their process for appealing content moderation actions, including enabling affected users to immediately appeal that action. A robust appeals process should include oversight by a human reviewer and give affected users an opportunity to present additional information. Companies should also offer a clear timeframe for reviewing appeals and clearly disclose the circumstances in which appeals are not possible.

To receive full credit on this indicator, companies should inform users how to submit an appeal and describe what happens once the appeal enters the pipeline. This includes notifying users of their options for appeal as soon as the company takes an initial action on their content, clarifying the role of both automation and independent human moderators in the appeals process, clearly disclosing the reason for an appeals decision and the timeframes involved, and specifying circumstances in which the appeals process is not available. Companies should also clearly demonstrate they respond to appeals by publishing data on the appeals received and the outcome of those decisions.

Potential sources:

- Company terms of service or user agreements
- Company privacy policies
- Company sustainability report

Freedom of Expression and Information

Indicators in this category seek evidence that the company demonstrates it respects the right to freedom of expression and information, as articulated in the Universal Declaration of Human Rights,¹⁶ the International Covenant on Civil and Political Rights,¹⁷ 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' fundamental right to freedom of expression and information.

F1: Access to policies

F1(a). 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 primary language(s) spoken by users in the company's home jurisdiction?
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. These terms contain rules about prohibited content and activities, and companies can also take action against users for violating the rules described in the terms. Given this, we expect companies to ensure that the terms are easy to access and understand.

This indicator evaluates if the company's terms are easy for users to locate. 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 use of positioning or colour schemes that make a text or link less noticeable, or hard to find

¹⁶ "Universal Declaration of human Rights," <https://www.un.org/en/universal-declaration-human-rights/>.

¹⁷ "International Covenant on Civil and Political Rights," *UN Human Rights Office of the High Commissioner*, <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>,



on a webpage, means that the document is not easily accessible. The terms of service of an app should never be more than “two taps away” within the app (e.g. by including a “Privacy”/“Data Protection” option in the menu functionality of the app). 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 graphical features to help users understand the document, or writing the terms using readable syntax.

Potential sources:

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

F1(b). Access to advertising content policies

The company should offer **advertising content policies** that are **easy to find** and **easy to understand**.

Elements:

1. Are the company’s **advertising content policies easy to find**?
2. Are the company’s **advertising content policies** available in the primary language(s) spoken by users in the company’s home jurisdiction?
3. Are the company’s **advertising content policies** presented in an **understandable manner**?
4. (For **mobile ecosystems**): Does the company **clearly disclose** that it requires apps made available through its **app store** to provide users with an **advertising content policy**?
5. (For **personal digital assistant ecosystems**): Does the company **clearly disclose** that it requires **skills** made available through its **skill store** to provide users with an **advertising content policy**?

Indicator guidance: Companies that enable any type of advertising on their services or platforms should clearly disclose the rules for what types of ad content is prohibited—for example, ads that discriminate against individuals or groups based on personal attributes like age, religion, gender, and ethnicity. Companies should be transparent about these rules so that both users and advertisers can understand what types of ad content are not



permissible and so they can be accountable for the ad content that appears on their services or platforms.

Therefore, companies should make these rules easy to find (E1), easy to understand (E3), and available in the main languages of the company's home market (E2). Companies that operate mobile ecosystems (Apple iOS, Google Android, and Samsung's implementation of Android) and personal digital assistant ecosystems (Amazon's Alexa, Alibaba's AliGenie) should enable users to choose which apps or skills to download on the basis of their participation (or not) in advertising networks. Therefore, Element 4 and Element 5 ask whether the company discloses a requirement for apps or skills made available through its app store or skills store to provide users with an advertising content policy.

Potential sources:

- Company advertising policies
- Company business help center
- Company terms of use

F1(c). Access to advertising targeting policies

The company should offer **advertising targeting policies** that are **easy to find** and **easy to understand**.

Elements:

1. Are the company's **advertising targeting policies easy to find**?
2. Are the **advertising targeting policies** available in the primary language(s) spoken by **users** in the company's home jurisdiction?
3. Are the **advertising targeting policies** presented in an **understandable manner**?
4. (For **mobile ecosystems**): Does the company **clearly disclose** that it requires **apps** made available through its **app store** to provide users with an **advertising targeting policy**?
5. (For **personal digital assistant ecosystems**): Does the company clearly disclose that it requires **skills** made available through its **skill store** to provide users with an **advertising targeting policy**?

Indicator guidance: In addition to providing accessible ad content policies (Indicator F1b), companies should also clearly disclose their ad targeting policies. The ability for advertisers or other third parties to target users with tailored content—based on their browsing behaviors, location information, and other data and characteristics that have been inferred



about them¹⁸—can significantly shape (or in some cases, distort) a user’s online ecosystem. Targeting, which can include both paid and unpaid content, can amplify offline social inequities and can be overtly discriminatory. It can also result in so-called “filter bubbles” as well as amplify problematic content, including content intended to mislead or to spread falsehoods.¹⁹

Therefore, companies that enable advertisers and other third parties to target their users with tailored ads or content should publish targeting policies that users can easily find and understand, and that are available in the main languages of the company’s home market. Users should be able to access and understand these rules in order to make informed decisions using the information about the ad content they are receiving. For mobile ecosystems and personal digital assistant ecosystems, companies should disclose a requirement for apps or skills made available through their app stores or skill stores to provide users with an accessible advertising targeting policy.

.Potential sources:

- Company advertising policies
- Company business help center
- Company terms of use

F1(d). Access to algorithmic system use policies

The company should offer policies related to their use of **algorithms** that are **easy for users to find** and **understand**.

Elements:

1. Are the company’s **algorithmic system use policies easy to find**?
2. Are the **algorithmic system use policies** available in the primary language(s) spoken by users in the company’s home jurisdiction?
3. Are the **algorithmic system use policies** presented in an **understandable manner**?

Indicator guidance: The use of algorithmic systems can have adverse effects on fundamental human rights—and specifically, on the right to freedom of expression and

¹⁸ For more about data inference policies, see Section 6.2 of “2020 Pilot Study and Lessons Learned,” *Ranking Digital Rights*, March 16, 2020, <https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf>.

¹⁹ “Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems,” *Ranking Digital Rights*, October 2019, <https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators-Targeted-advertising-algorithms.pdf>.

information as well as the right to non-discrimination.²⁰ In addition to clearly committing to respect and protect human rights as they develop and deploy these technologies (*see Indicator G1, Element 3*), companies should also publish policies that clearly describe the terms for how they use algorithmic systems across their service and platforms. Similar to having terms of service policies or user agreements that outline the terms for what types of content or activities are prohibited, companies that use algorithmic systems with the potential to cause human rights harms should publish a clear and accessible policy stating the nature and functions of these systems. As recommended by the Council of Europe’s [Recommendation on the human rights impacts of algorithmic systems](#) (2020), this policy should be easy to find, presented in plain language, and contains options for users to manage settings.

Note that in this indicator, we are looking for a policy that explains terms for how the company deploys algorithmic systems across its platforms and services. We also look for companies to disclose terms that outline how they develop and test algorithmic systems, which is addressed in Indicator P1b.

Potential sources

- Algorithmic system use policies
- Guidelines for developing algorithmic systems
- Privacy policy or data policy
- Help center

F2: Notification of policy changes

F2(a). Changes to terms of service

The company should **clearly disclose** that it **directly notifies** users when it changes its terms of service, prior to these changes coming into effect.

Elements:

1. Does the company **clearly disclose** that it **directly notifies** users about all 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 **directly notifies users** of changes prior to these changes coming into effect?

²⁰ “Human Rights Risk Scenarios: Algorithms, machine learning and automated decision-making,” *Ranking Digital Rights*, July 2019, <https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios -algorithms-machine-learning-automated-decision-making.pdf>.

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, which can include rules about prohibited content and activities, can have a significant impact on users' freedom of expression and information rights. We therefore expect companies to commit to notifying users when they change these terms and to providing users with information that helps them understand what these changes mean.

This indicator evaluates whether companies clearly disclose the method and timeframe for notifying users about changes to their terms of service. We expect companies to commit to directly notifying users of these changes prior to changes coming into effect. The method of direct notification may differ according to the type of service; we expect companies to directly notify users in a way that users are sure to access. 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 where users access that 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

F2(b). Changes to advertising content policies

The company should **clearly disclose** that it **directly notifies users** when it changes its **advertising content policies**, prior to these changes coming into effect.

Elements:

1. Does the company **clearly disclose** that it **directly notifies users** about changes to its **advertising content policies**?
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 **directly notifies users** of changes prior to these 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** made available through its **app store** to **notify users** when the **apps** change their **advertising content policies**?



6. (For **personal digital ecosystems**): Does the company **clearly disclose** that it requires **skills** made available through its **skills store** to **notify users** when the **skills** change their **advertising content policies**?

Indicator guidance: It is common for companies to change their advertising content policies as their business and services evolve. However, these changes, which may include revising rules about prohibited content and activities, can affect users' freedom of expression and information as well as their right to non-discrimination. Companies therefore should commit to notifying users when they change these terms and to providing users with information that helps them understand what these changes mean.

This indicator evaluates whether companies clearly disclose the method and timeframe for notifying users about changes prior to changes coming into effect. The method of direct notification may differ according to the type of service; we expect companies to directly notify users in a way that users are sure to access. 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 where users access that 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:

- Advertising policies, guidelines, terms of use, etc.
- Company Ads or Business Help Center

F2(c). Changes to advertising targeting policies

The company should **clearly disclose** that it **directly notifies users** when it changes its **advertising targeting policies**, prior to these changes coming into effect.

Elements:

1. Does the company **clearly disclose** that it **directly notifies users** about changes to its **advertising targeting policies**?
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 **directly notifies users** of changes prior to these 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** made available through its **app store** to **directly notify users** when the **apps** change their **advertising targeting policies**?

6. (For **personal digital ecosystems**): Does the company **clearly disclose** that it requires **skills** made available through its **skills store** to **notify users** when the **skills** change their **advertising targeting policies**?

Indicator guidance: It is common for companies to change their advertising targeting policies as their business and services evolve. However, these changes can affect users' freedom of expression and information as well as their right to non-discrimination. Companies should therefore commit to notifying users when they change these terms and to providing users with information that helps them understand what these changes mean.

This indicator evaluates whether companies clearly disclose the method and timeframe for notifying users about changes prior to changes coming into effect. The method of direct notification may differ according to the type of service; we expect companies to directly notify users in a way that users are sure to access. 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 where users access that 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:

- Advertising policies, guidelines, terms of use, etc.
- Company Ads or Business Help Center

F2(d). Changes to algorithmic system use policies

The company should **clearly disclose** that it **directly notifies users** when it changes its **algorithmic system use policies**, prior to these changes coming into effect.

Elements:

1. Does the company **clearly disclose** that it **directly notifies users** about changes to its **algorithmic system use policies**?
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 **directly notifies users** of changes prior to these changes coming into effect?
4. Does the company maintain a **public archive** or **change log**?

Indicator guidance: When companies change their algorithm use policies, these changes can affect users' freedom of expression and information as well as their right to non-discrimination. Companies therefore should commit to notifying users when they change these policies and to providing users with information that helps them understand what

these changes mean. This standard is in line with the Council of Europe's [Recommendation on the human rights impacts of algorithmic systems](#) (2020).

This indicator evaluates whether companies clearly disclose the method and timeframe for notifying users about changes prior to changes coming into effect. The method of direct notification may differ according to the type of service; we expect companies to directly notify users in a way that users are sure to access. 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 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

- Algorithmic system use policies
- Guidelines for developing algorithmic systems
- Privacy policy or data policy
- Help center

F3: Process for policy enforcement

F3(a). 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** how it uses **algorithmic systems** to flag **content** that might violate the company's rules?
5. Does the company **clearly disclose** whether any government authorities receive priority consideration when **flagging content** to be restricted for violating the company's rules?



6. Does the company **clearly disclose** whether any private entities receive priority consideration when **flagging content** to be restricted for violating the company's rules?
7. Does the company **clearly disclose** its process for enforcing its rules once violations are detected?

Indicator guidance: It is fair to expect companies to set rules prohibiting certain content or activities—like toxic speech or malicious behavior. However, when companies develop and enforce rules about what people can do and say on the internet—or whether they can access a service at all—they must do so in a way that is transparent and accountable.

We therefore expect companies to clearly disclose what these rules are and how they enforce them. This includes information about how companies learn of material or activities that violate their terms. For example, companies may rely on outside contractors to review content and/or user activity. They may also rely on community flagging mechanisms that allow users to flag other users' content and/or activity for company review. They may also deploy algorithmic systems to detect and flag breaches, in which case, companies should explain how these systems are used and on what types of content. We 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. For personal digital assistant ecosystems, we expect companies to disclose the types of skills and search results 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 agreements
- 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

F3(b). Advertising content rules and enforcement

The company should **clearly disclose** its policies governing what types of advertising content is prohibited.

Elements:

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



2. Does the company **clearly disclose** whether it **requires** all **advertising content** be clearly labelled as such?
3. Does the company **clearly disclose** the processes and technologies it uses to identify **advertising content** or **accounts** that violate the company's rules?

Indicator guidance: Companies should clearly disclose policies for what types of advertising content are prohibited on a platform or service, and its processes for enforcing these rules. Specifically, this indicator asks if companies clearly disclose what types of advertising content are prohibited, if the company discloses a requirement that all advertising content be clearly labeled as such, and if it discloses its processes for enforcing these rules

Potential sources:

- Company advertiser portal, ad policy, political ad policy
- Company terms of service, user contract
- Company acceptable use policy, community standards, content guidelines
- Company support, help center, or FAQ

F3(c). Advertising targeting rules and enforcement

The company should **clearly disclose** its policies governing what type of **advertising targeting** is prohibited.

Elements:

1. Does the company **clearly disclose** whether it enables **third parties** to target its **users** with **advertising content**?
2. Does the company **clearly disclose** what types of **targeting parameters** are not permitted?
3. Does the company **clearly disclose** that it does not permit **advertisers** to target specific individuals?
4. Does the company **clearly disclose** that **algorithmically** generated **advertising audience categories** are evaluated by human reviewers before they can be used?
5. Does the company **clearly disclose** information about the processes and technologies it uses to identify **advertising content** or **accounts** that violate the company's rules?

Indicator guidance: The ability for advertisers or other third parties to target users with tailored content—based on their browsing behaviors, location information, and other data



and characteristics that have been inferred about them²¹—can significantly shape a user’s online ecosystem. Targeting, which can include both paid and unpaid content, can amplify offline social inequities and can be overtly discriminatory. It can also result in so-called “filter bubbles,” as well as spread problematic content, including content intended to mislead or to spread falsehoods.²²

Therefore, companies that enable advertisers and other third parties to target their users with tailored ads or content should have clear policies describing their ad targeting rules. Companies should clearly disclose whether they enable third parties to target their users with tailored ads or other types of sponsored content, and clearly disclose what targeting parameters—like using certain types of audience categories, like age, location, or other user characteristics—are not permitted. Companies should also disclose their processes for identifying breaches to targeting rules.

Potential sources:

- Company advertiser portal, ad policy, political ad policy
- Company acceptable use policy
- Company support, help center, or advertiser FAQ

F4: Data about policy enforcement

F4(a). Data about content restrictions to enforce terms of service

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

Elements:

1. Does the company publish data about the total number of pieces of **content restricted** for violating the company’s rules?
2. Does the company publish data on the number of pieces of **content restricted** based on which rule was violated?

²¹ For more about data inference policies, Section 6.2 of this report. “2020 Pilot Study and Lessons Learned,” *Ranking Digital Rights*, March 16, 2020, <https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf>

²² “Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems,” *Ranking Digital Rights*, October 2019, <https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators-Targeted-advertising-algorithms.pdf>.



3. Does the company publish data on the number of pieces of **content** it restricted based on the format of content? (e.g. text, image, video, live video)?
4. Does the company publish data on the number of pieces of **content** it **restricted** based on the method used to identify the violation?
5. Does the company publish this data at least four times a year?
6. Can the data be exported as a **structured data** file?

Indicator guidance: Companies can and should set clear rules about what types of content are not permitted on their platforms or services. This indicator expects companies to publicly disclose data about the actions they take to restrict or otherwise censor content due to breaches to the company’s rules. Publishing this data is an essential first step to holding companies accountable for enforcing their own rules and for the actions they take to moderate content on their platforms and services.

Companies should publish data about the aggregate number of pieces of content they restrict, remove, or—in the case of telecommunications companies—content they block or filter, as a result of terms of services violations. They should also break out this data by violation and by the method—such as a community flagger program or automation—through which the rules violation was detected. Companies should also publish this data at least four times a year, in line with the [Santa Clara Principles](#), and in a structured data file.

Potential sources:

- Company transparency report
- Company community standards enforcement report, community guidelines enforcement report, etc.

F4(b). Data about account restrictions to enforce terms of service

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

Elements

1. Does the company publish data on the total number of **accounts restricted** for violating the company’s own rules?
2. Does the company publish data on the number of **accounts restricted** based on which rule was violated?



3. Does the company publish data on the number of **accounts restricted** based on the method used to identify the violation?
4. Does the company publish this data at least four times a year?
5. Can the data be exported as a **structured data** file?

Potential sources:

- Company transparency report

Indicator guidance: Companies can and should set clear rules about what types of content or activities are not permitted on their platforms or services. This indicator expects companies to publicly disclose data about the actions they take to enforce these rules. Publishing this data is an essential first step to holding companies accountable for enforcing their own rules and for the actions they take to moderate content on their platforms and services.

Companies should publish data about the number of accounts they restrict as a result of terms of service violations. They should also break out this data by violation and by the method—such as a community flagger program or automation—through which the rules violation was detected. Companies should also publish this data at least four times a year, in line with the [Santa Clara Principles](#), and in a structured data file.

Potential sources:

- Company transparency report

F4(c). Data about advertising content and advertising targeting policy enforcement

The company should **clearly disclose** and regularly publish data about the volume and nature of actions taken to **restrict advertising content** that violates the company's **advertising content policies** and **advertising targeting policies**.

Elements

1. Does the company publish the total number of **advertisements** it **restricted** to enforce its **advertising content policies**?
2. Does the company publish the number of **advertisements** it **restricted** based on which **advertising content** rule was violated?
3. Does the company publish the total number of **advertisements** it **restricted** to enforce its **advertising targeting policies**?



4. Does the company publish the number of **advertisements** it **restricted** based on which **advertising targeting** rule was violated?
5. Does the company publish this data at least once a year?
6. Can the data be exported as a **structured data file**?

Indicator guidance: Indicators F3c and F3d ask companies to clearly disclose rules for what types of ad content and ad targeting is prohibited, respectively, and to describe its processes for enforcing these rules. This indicator, F4c, asks companies to publish evidence that it is enforcing these rules. Companies should publish data on the total number of ads it removes as a result of breaches to ad content policies, and they should also break out this data by what rule was violated. Companies should also provide evidence that it is enforcing its ad targeting policies by publishing data on the number of ads removed for violating targeting rules, and by what rule was violated. Companies should also publish this data at least once a year and in a structured data file.

Potential sources:

- Company transparency report

F5: Process for responding to third-party requests to restrict content or accounts

F5(a). Process for responding to government demands to restrict content or accounts

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

Elements:

1. Does the company **clearly disclose** its process for responding to **non-judicial government demands**?
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 demands** from foreign jurisdictions?
4. Do the company's explanations **clearly disclose** the legal basis under which it may comply with **government demands**?
5. Does the company **clearly disclose** that it carries out due diligence on **government demands** before deciding how to respond?



6. Does the company commit to push back on inappropriate or overbroad **demands made by governments?**
7. Does the company provide clear guidance or examples of implementation of its process of responding to **government demands?**

Indicator guidance: Companies often receive demands from governments to remove, filter, or restrict access to content and accounts. These requests can come from government agencies, law enforcement, and courts (both domestic and foreign). We expect companies to publicly disclose their processes for responding to these types of demands. Companies should disclose the legal reasons why it would comply with a government demand, as well as disclose a clear commitment to push back on overly broad demands.

Note that our definition of “government demands” includes those that come through a “non-judicial” process, such as orders from law enforcement, as well as civil cases made by private parties that come through civil courts. Takedown requests that are made via organized processes like the U.S. Digital Millennium Copyright Act or the European Right to be Forgotten ruling are defined as “private processes” and are evaluated in Indicator F5b below.

Potential sources:

- Company transparency report
- Company law enforcement guidelines
- Company annual reports

F5(b). Process for responding to private requests for content or account restriction

The company should **clearly disclose** its process for responding to **requests** to remove, filter, or restrict **content** or **accounts** that come through **private processes**.

Elements:

1. Does the company **clearly disclose** its process for responding to **requests** to remove, filter, or restrict **content** or **accounts** made through **private processes?**
2. Do the company’s explanations **clearly disclose** the basis under which it may comply with **requests** made through **private processes?**
3. Does the company **clearly disclose** that it carries out due diligence on **requests** made through **private processes** before deciding how to respond?
4. Does the company commit to push back on inappropriate or overbroad **requests** made through **private processes?**



5. Does the company provide clear guidance or examples of implementation of its process of responding to **requests** made through **private processes**?

Indicator guidance: In addition to demands from governments and other types of authorities, companies can receive requests to remove or restrict access to content and accounts through private processes. These types of requests can come through formal processes established by law, (e.g., requests made under the U.S. Digital Millennium Copyright Act, the European Right to be Forgotten ruling, etc.) or via self-regulatory arrangements (e.g., company agreements to block certain types of materials or images, such as via the EU’s Code of Conduct on Disinformation). Note that this indicator does not regard private requests to be requests that come through any kind of court or judicial process, which are considered under “government” requests (Indicator F5a).

This indicator evaluates whether the company clearly discloses how it responds to requests to remove, filter, or restrict content or accounts that come through these types of private processes (Element 1). The company should disclose the basis for complying with these types of requests (Element 2), and whether it conducts due diligence on these requests before deciding how to respond (Element 3). We also expect companies to commit to push back on overly broad requests to remove content or accounts that come through private processes (Element 4), and to publish clear examples that illustrate how a company handles these types of requests (Element 5).

Potential sources:

- Company transparency report
- Company help or support center
- Company blog posts
- Company policy on copyright or intellectual property

F6. Data about government demands to restrict for content and accounts

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

Elements:

1. Does the company break out the number of **demands** 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 **demands** it receives?



5. Does the company list the number of **demands** that come from different legal authorities?
6. Does the company list the number of **demands** it knowingly receives from government officials to restrict **content** or **accounts** through **unofficial processes**?
7. Does the company list the number of **demands** with which it complied?
8. Does the company publish the original **demands** 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 demands from governments to remove, filter, or restrict content or accounts. We expect companies to regularly publish data about the number and type of government demands it receives, and the number of such requests with which it complies. Companies may receive these demands through official processes, such as with a court order, or through informal channels, like through a company's flagging system intended to allow private individuals to report content that violates the terms of service. Companies should be transparent about the nature of these requests. 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 relationship between companies and governments in policing content online, and 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 the standards specified in all of the above 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

F7. Data about private requests for content or account restriction

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



Elements:

1. Does the company break out the number of requests to restrict **content** or **accounts** that it receives through **private processes**?
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 **clearly disclose** the **private processes** that made 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 requests that it receives through **private processes**?

Indicator guidance: Companies frequently receive requests to remove, filter, or restrict content or accounts through private processes, such as requests made under the U.S. Digital Millennium Copyright Act, the European Right to be Forgotten ruling, etc.) or through a self-regulatory arrangement (e.g., company agreements to block certain types of images). We expect companies to regularly publish data about the number and type of requests received through these private processes, and the number of such requests with which it complies.

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 a company clearly discloses that it notifies users when it takes 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 a company 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
- Company community standards
- Company support page, help center, or FAQ
- 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** a **policy commitment** to 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. Does the company engage in practices, such as offering **zero-rating programs**, that **prioritize** network traffic for reasons beyond assuring quality of service and reliability of the network?
3. If the company does engage in network **prioritization** practices for reasons beyond assuring quality of service and reliability of the network, does it **clearly disclose** its purpose for doing so?

Indicator guidance: This indicator evaluates whether telecommunications 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 these companies to publicly commit to avoid prioritization or degradation of content. In some cases, a company may engage in legitimate traffic shaping practices in order to ensure the flow of traffic through their networks. We expect the company to publicly disclose this and to explain their purpose for doing so. Companies may engage in paid prioritization or zero rating practices, which would not fall under legitimate network management practices. A company may have a statement on its website committing to net neutrality, for example, but also offer zero rating.

Potential sources:

- Company network management or traffic management policies
- Company annual reports

F10. Network shutdown (telecommunications companies)

The company should **clearly disclose** 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 disclose** the reason(s) why it may shut down a service to a particular area or group of users?
2. Does the company **clearly disclose** 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 disclose** its process for responding to **government demands** to **shut down a network or restrict access to a service**?



4. Does the company **clearly disclose** a commitment to push back on **government demands** 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 a network or restricts access to a service**?
6. Does the company **clearly disclose** the number of **network shutdown demands** it receives?
7. Does the company **clearly disclose** the specific legal authority that makes the **demands**?
8. Does the company **clearly disclose** the number of **government demands** with which it complied?

Indicator guidance: Network shutdowns are a growing threat to human rights. The U.N. 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.²³ Yet governments are increasingly ordering telecommunications companies to shut down their networks,²⁴ which in turn puts pressure on companies to take actions that violate their responsibility to respect human rights. We expect companies to fully disclose the circumstances under which they might take such action, to report on the demands they receive to take such actions, and to disclose commitments to push back on or mitigate the effects of government orders.

Potential Sources:

- Company terms of service
- Company transparency report
- Company law enforcement guidelines
- Company human rights policy

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?

²³ “The promotion, protection, and enjoyment of human rights on the Internet,” *United Nations Human Rights Council* (32nd Session), June 27, 2016, <https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement>.

²⁴ “#KeptOn”, *Access Now*, <https://www.accessnow.org/keepiton/>, last accessed April 2, 2020.



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. Other forms of identification can include credit cards and registered phone numbers. 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. In some cases, phone numbers can be connected to a user's offline identity, for example, in legal contexts where prepaid users are required to register with their IDs. When providing a phone number is necessary to the provision of the service (for example in the case of instant messaging apps), companies should receive full credit, unless they also require users to use their real names or submit documents that would tie their names to their offline identities. Services that require users to provide a phone number for purposes not necessary to the provision of the service will receive no credit: for example, some services may require phone numbers for two-factor authentication purposes, however, this should be optional and users should be provided with other two-factor authentication options.

This indicator is applicable to digital platform 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

F12. Algorithmic content curation, recommendation, and/or ranking systems

Companies should **clearly disclose** how users' online **content** is **curated, ranked, or recommended**.

Elements:

1. Does the company **clearly disclose** whether it uses **algorithmic systems** to **curate, recommend, and/or rank** the **content** that **users** can access through its platform?



2. Does the company **clearly disclose** how the **algorithmic systems** are deployed to **curate, recommend, and/or rank content**, including the variables that influence these systems?
3. Does the company **clearly disclose** what options users have to control the variables that the **algorithmic content curation, recommendation, and/or ranking system** takes into **account**?
4. Does the company **clearly disclose** whether **algorithmic systems** are used to automatically **curate, recommend, and/or rank content** by default?
5. Does the company **clearly disclose** that users can opt in to automated **content curation, recommendation, and/or ranking systems**?

Indicator guidance: Algorithmic content curation, recommendation, and ranking systems play a critical role in shaping what types of content and information users can see and access online. In addition, systems that are optimized for user engagement can have the effect of prioritizing controversial and inflammatory content, including content that is not protected under international human rights law. Over time, reliance on algorithmic curation and recommendation systems that are optimized for engagement can alter the news and information ecosystems of entire countries or communities. These systems can be manipulated to spread disinformation and otherwise distort the information ecosystem, which can in turn fuel human rights abuses.

Companies should therefore be transparent about their use of automated curation, recommendation, and ranking systems, including the variables that influence such systems. Companies should publish information about whether they use algorithmic systems to curate, recommend, and rank content. They should disclose how these systems work, what options users have to control how their information is used by these systems, whether such systems are automatically on by default, or whether users can “opt-in” to have their content automatically curated by the algorithmic system .

Potential sources:

- Company human rights policy
- Company artificial intelligence policies, including AI principles, frameworks, and use guidelines
- Help pages describing how feed settings, home page settings, search results, recommendations, user interests, or topics are affected by algorithms

F13. Automated software agents (“bots”)

Companies should **clearly disclose** policies governing the use of **automated software agents (“bots”)** on their platforms, products and services, and how they enforce such



policies-

Elements:

1. Does the company **clearly disclose** rules governing the use of **bots** on its platform?
2. Does the company **clearly disclose** that it requires **users** to clearly label all **content** and **accounts** that are produced, disseminated or operated with the assistance of a **bot**?
3. Does the company **clearly disclose** its process for enforcing its **bot policy**?
4. Does the company **clearly disclose** data on the volume and nature of user **content** and **accounts restricted** for violating the company's **bot policy**?

Indicator guidance: Social media platforms often allow users to create automated software agents, or “bots,” that automate various actions a user account can take, such as posting or boosting content (re-tweeting, for example). There are many innocuous or even positive uses of bots—for instance, artists use Twitter bots for the purpose of parody.²⁵ There are also more problematic uses that many companies forbid or discourage, such as when political parties or their surrogates use botnets to promote certain messages or to artificially inflate a candidate’s reach in order to manipulate public discourse and outcomes. On some social media platforms, bots or coordinated networks of bots (“botnets”) can be used to harass users (“brigading”), artificially amplify certain pieces of content (mass retweeting, etc), and otherwise distort public discourse on the platform. Some experts have called for companies to require users who use bots to explicitly label them as bots, in order to help detect such distortions.²⁶

Companies that allow bots therefore should have clear policies governing the use of bots on their platforms. They should disclose whether they require content and accounts that are produced, disseminated or operated with the assistance of a bot to be labelled as such. They should also clarify their process for enforcing their bot policies, including by publishing data on the volume and nature of content and accounts that are restricted for violating these rules.

Potential sources:

- Platform policies for developers
- Automation or bot rules
- Transparency reports

²⁵ *Thinkpiece Bot*, Twitter, <https://twitter.com/thinkpiecebot>, last accessed April 2, 2020.

²⁶ Engler, A. (2020, January 22). The case for AI transparency requirements. Brookings Institution. <https://www.brookings.edu/research/the-case-for-ai-transparency-requirements/>, last accessed April 2, 2020.



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,²⁷ the International Covenant on Civil and Political Rights,²⁸ 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 policies affecting users' privacy

P1(a). 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 primary language(s) spoken by users in the company's home jurisdiction?
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**?
5. (For **personal digital assistant ecosystems**): Does the company disclose that it requires **skills** made available through its **skill 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 this policy and to make an effort to

²⁷ "Universal Declaration of Human Rights," *United Nations*, <https://www.un.org/en/universal-declaration-human-rights/>, last accessed April 2, 2020.

²⁸ "International Covenant on Civil and Political Rights," *UN Human Rights Office of the High Commissioner*, <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>, last accessed April 2, 2020.



help users understand what they mean. This indicator expects companies to publish privacy policies that are easy to find, are available in the primary languages spoken in the company's home market, and easy to understand. If the company offers multiple products and services, it should be clear to what products and services the privacy policies applies.

A document that is “easy to find” should be easily accessible from the company's homepage or service website. It should be located a few clicks away from the homepage, or otherwise accessible in a logical place where users are likely to find it. The terms should also be available in the major language(s) of the home market. In addition, we expect a company to take steps to help users understand the information presented in their policies. 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 graphical features to help users understand the document, or writing the terms using readable syntax.

Potential sources:

- Company privacy policy
- Company data use policy

P1(b). Access to algorithmic system development policies

The company should offer **algorithmic system development policies** that are **easy to find** and **easy to understand**.

Elements:

1. Are the company's **algorithmic system development policies easy to find** ?
2. Are the **algorithmic system development policies** available in the primary language(s) spoken by users?
3. Are the **algorithmic system development policies** presented in an **understandable manner**?

Indicator guidance: The development and testing of algorithmic systems can pose significant risks to privacy, particularly when companies then use the information collected about users to develop, train, and test these systems without the data subject's informed consent.²⁹ Companies should clearly disclose policies describing the development

²⁹ Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY, USA: PublicAffairs; Nathalie Maréchal. Targeted Advertising Is Ruining the Internet and Breaking the World, https://www.vice.com/en_us/article/xwjden/targeted-advertising-is-ruining-the-internet-and-breaking-the-world, *Vice Motherboard*, November 16, 2018; “Human Rights Risk Scenarios: Algorithms, machine learning and automated decision-making,” *Ranking Digital Rights*, July 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-algorithms-machine-learning-automated-decision-making.pdf.



and testing of algorithmic systems in a way that users can access, read and understand, so that users can make informed decisions about whether to use a company's products and services.

Potential sources:

- Algorithmic system use policies
- Guidelines for developing algorithmic systems
- Privacy policy or data policy

P2: Notification of changes

P2(a). Changes to privacy policies

The company should **clearly disclose** that it **directly notifies** users when it changes its **privacy policies**, prior to these changes coming into effect.

Elements:

1. Does the company **clearly disclose** that it **directly notifies users** about all 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 timeframe within which it **directly notifies users** of changes prior to these 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**?
6. (For **personal digital assistant ecosystems**): Does the company **clearly disclose** that it requires **skills** sold through its **skill store** to notify **users** when the **skill** changes its **privacy policy**?

Indicator guidance: Companies frequently change their privacy policies as their business evolves. However, these changes can affect a user's privacy rights by changing what user information companies can collect, share, and store. We therefore expect companies to commit to notifying users when they change these policies and to providing 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 require a user



account, direct notification may involve sending an email or an SMS. For services that do not require a user account, direct notification should involve posting a prominent notice on the main webpage or platform where users access the service. This indicator 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

P2(b). Changes to algorithmic system development policies

The company should **clearly disclose** that it **directly notifies users** when it changes its **algorithmic system development policies**, prior to these changes coming into effect.

Elements:

1. Does the company **clearly disclose** that it **directly notifies users** about all changes to its **algorithmic system development 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 **directly notifies users** of changes prior to these changes coming into effect?
4. Does the company maintain a **public archive** or **change log**?

Indicator guidance: Companies may change their algorithmic system development policies as their business evolves. However, these changes can have a significant impact on users' right to privacy. We therefore expect companies to commit to notifying users when they change these policies and to providing users with information that helps them understand what these changes mean, as the Council of Europe recommends in its [Recommendation on the human rights impacts of algorithmic systems](#) (2020).

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 require a user account, direct notification may involve sending an email or an SMS. For services that do not require a user account, direct notification should involve posting a prominent notice on the main webpage or platform where users access the service. This indicator 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 algorithmic use policy
- Privacy policy or data policy

P3: User information collection and inference

P3(a). 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?
6. (For **personal digital assistant ecosystems**): Does the company **clearly disclose** that it evaluates whether the **privacy policies** of third-party **skills** made available through its **skill store** disclose what **user information** the skills **collect**?
7. (For **personal digital assistant ecosystems**): Does the company **clearly disclose** that it evaluates whether third-party **skills** made available through its **skill store limit collection** of **user information** to what is directly relevant and necessary to accomplish the purpose of the skill?

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 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 details on how they handle each type of information. For mobile ecosystems and personal digital assistant (PDA) ecosystems, we expect the company to clearly disclose whether the privacy policies of the



apps or PDA skills that are available in its mobile app store or PDA skill store specify what user information the apps or skills collect and whether those policies comply with data minimization principles.

Potential sources:

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

P3(b). Inference of user information

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

Elements:

1. Does the company **clearly disclose** all the types of **user information** it **infers** on the basis of **collected user information**?
2. For each type of **user information** the company **infers**, does the company **clearly disclose** how it **infers** that **user information**?
3. Does the company **clearly disclose** that it limits **inference** of **user information** to what is directly relevant and necessary to accomplish the purpose of its service?

Indicator guidance: In addition to collecting information about users, companies also perform big data analytics to make inferences, or predictions, about users on the basis of the collected information. These methods might be used to make inferences about user preferences or attributes (such as race, gender, sexual orientation), and opinions (including political opinions), or to predict consumer behaviors. Without sufficient transparency and user control over data inference, privacy-invasive and non-verifiable inferences cannot be predicted, understood, or refuted by users.³⁰

In addition to disclosing the information that they collect, companies should disclose what information they infer and how they infer it. They should also commit to only infer information that is relevant and necessary to provide the service. For example, companies should not try to infer their users' religion, sexual orientation, or health status (such as by assigning them to an audience category based on this characteristic) unless that information is somehow directly necessary to accomplish the purpose of their service.

Potential sources:

- Company privacy policy, cookies policy

³⁰ For more see: Wachter, Sandra and Mittelstadt, Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI (October 5, 2018). Columbia Business Law Review, 2019(2), <https://ssrn.com/abstract=3248829>



- 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**?
7. (For **personal digital assistant ecosystems**): Does the company **clearly disclose** that it evaluates whether the **privacy policies** of **third party skills** made available through its **skill store** disclose what **user information** the skills **share**?
8. (For **personal digital assistant ecosystems**): Does the company **clearly disclose** that it evaluates whether the **privacy policies** of **third party skills** made available through its **skill 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 our personal details and account profiles to our browsing activities and location. Companies also often share this information with third parties, including advertisers, governments, and legal authorities. We expect companies to clearly disclose what **user information (as RDR defines it)** they share and with whom. Companies should specify if they share 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. Companies that operate personal digital assistant (PDA) ecosystems should require that third-party skills that they make available in their skill store to clearly disclose what types of user information is shared, and the types of third parties with whom they share it.

Potential sources:

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

P5. Purpose for collecting, inferring, and sharing user information

The company should **clearly disclose** why it **collects**, **infers**, 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. For each type of **user information** the company **infers**, does the company **clearly disclose** its purpose for the **inference**?
3. Does the company **clearly disclose** whether it combines **user information** from various company services and if so, why?
4. For each type of **user information** the company **shares**, does the company **clearly disclose** its purpose for **sharing**?
5. Does the company **clearly disclose** that it limits its use of **user information** to the purpose for which it was **collected** or **inferred**?

Indicator guidance: We expect companies to clearly disclose the purpose for collecting, sharing, and inferring each type of user information it collects, shares, and infers. 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. Companies should also publicly commit to the principle of use limitation—meaning they publicly state in their policies that they only use data for purposes for which it was specified—in line with [OECD privacy guidelines](#), the [GDPR](#), and other frameworks, both for the user information they collect and infer.

Potential sources:

- Company privacy policy

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**?
8. (For **personal digital assistant ecosystems**): Does the company **clearly disclose** that it evaluates whether the **privacy policies** of **third-party skills** made available through its **skill store** disclose how long they retain **user information**?
9. (For **personal digital assistant ecosystems**): Does the company **clearly disclose** that it evaluates whether the **privacy policies** of **third-party skills** made available through its **skill store** state that all **user information** is deleted when users terminate their accounts or delete the **skill**?

Indicator guidance: Just as we expect companies to disclose what information they collect and share about us, we also expect companies to clearly disclose for how long they retain it and the extent to which they remove identifiers from user information they store. In addition, users should also be able to understand what happens to their information when they delete their accounts. In some cases, laws or regulations may require companies to retain certain information for a given period of time. In these cases, companies should clearly disclose these regulations to users. Companies that choose to retain user information for extended periods of time should also 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.

In addition, if companies collect multiple types of information, we expect them to clearly disclose for how long they retain each type of information. For mobile ecosystems and personal digital assistant (PDA) ecosystems, we expect companies to disclose whether the privacy policies of the mobile apps and PDA skills that are available in their app and skill store state how long the app or skill retains user information and whether all user information is deleted if users terminate or delete the app or the skill.

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, inference, 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. For each type of **user information** the company **infers** on the basis of **collected information**, does the company **clearly disclose** whether **users** can control if the company can attempt to **infer** this **user information**?
4. For each type of **user information** the company **infers** on the basis of **collected information**, does the company **clearly disclose** whether **users** can delete this **user information**?
5. Does the company **clearly disclose** that it provides **users** with **options to control** how their **user information** is used for **targeted advertising**?
6. Does the company **clearly disclose** that **targeted advertising** is off by default?
7. Does the company **clearly disclose** that it provides **users** with **options to control** how their **user information** is used for the development of **algorithmic systems**?



8. Does the company **clearly disclose** whether it uses **user information** to develop **algorithmic systems** by default, or not?

9. (For **mobile ecosystems** and **personal digital assistant 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, retain, and infer about them. Enabling users to control what information about them that a company collects, infers, 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 and algorithmic system development. Targeted advertising requires extensive collection, retention, and inference of user information, and companies should therefore clearly disclose whether users have options to control how their information is being used for these purposes.

For mobile ecosystems and personal digital assistant (PDA) 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 and personal digital assistant ecosystems can influence how other products and services access their location information. For instance, mobile apps or PDA ecosystem skills may enable users to control location information. However, if the device on which those mobile apps or PDA skills run collects geolocation data by default and does not give users a way to turn this off, users may not be able to limit mobile apps' or PDA skills' 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, privacy dashboards
- Company help center

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. Does the company **clearly disclose** that **users** can access the list of **advertising audience categories** to which the company has assigned them?
6. Does the company **clearly disclose** that **users** can obtain all the information that a company has **inferred** about them?
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** disclose that **users** can obtain all of the **user information** about them the app holds?
8. (For **personal digital assistant ecosystems**): Does the company **clearly disclose** that it evaluates whether the **privacy policies** of **third-party skills** made available through its **skill store** disclose that **users** can obtain all of the **user information** about them the skill holds?

Indicator guidance: Users should be able to obtain all public-facing and internal information that companies hold about them, including the information that a company has used to make inferences, or predictions, 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. Companies should also enable users to access the list of advertising categories that they have been assigned to. In order to target ads, companies typically assign each user to any number of audience categories. Advertisers can then select which audience categories they want to target. Users should be able to know which audience categories the company has assigned them to, on the basis of information that the company has collected or inferred about users .

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. We expect companies that operate personal digital assistant (PDA) skill stores to set minimum standards that the third-party skills hosted on their platform must meet. Just as we expect companies themselves to disclose that users can obtain a record of their own user information from the company, PDA skill stores should require skills in their store to provide similar disclosure.

Potential sources:

- Company privacy policy
- Company account settings



- Company help center
- Company blog posts

P9. Collection of user information from third parties

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

Elements:

1. (For **digital platforms**) Does the company **clearly disclose** what **user information** it collects from third-party websites through **technical means**?
2. (For **digital platforms**) Does the company **clearly explain** how it collects **user information** from **third parties** through **technical means**?
3. (For **digital platforms**) Does the company **clearly disclose** its purpose for collecting **user information** from **third parties** through **technical means**?
4. (For **digital platforms**) Does the company **clearly disclose** how long it retains the **user information** it collects from **third parties** through **technical means**?
5. (For **digital platforms**) Does the company **clearly disclose** that it respects user-generated signals to opt out of data collection?
6. Does the company **clearly disclose** what **user information** it collects from **third parties** through **non-technical means**?
7. Does the company **clearly disclose** how it collects **user information** from **third parties** through **non-technical means**?
8. Does the company **clearly disclose** its purpose for collecting **user information** from **third parties** through **non-technical means**?
9. Does the company **clearly disclose** how long it retains the **user information** it collects from third parties through **non-technical means**?

Indicator guidance: We expect companies to disclose what information about users they collect from third parties, which can mean information collected from third-party websites or apps through technical means—for instance through cookies, plug-ins, or widgets, or through non-technical means, for instance through contractual agreements. This acquired data can become part of a “digital dossier” that companies may hold on their users, which can then form the basis for inferred and shared user information. Companies should be transparent and accountable about these practices so that users can understand if and how their activities are being tracked by companies even when they are not on a host company’s website or when the individual is not a user of a particular service or platform.

Potential sources:

- Company privacy policy
- Company policy on third parties or cookies policy

P10. Process for responding to demands for user information

P10(a). Process for responding to government demands for user information

The company should **clearly disclose** its process for responding to **governments demands** for **user information**.

Elements:

1. Does the company **clearly disclose** its process for responding to **non-judicial government demands**?
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 demands** from foreign jurisdictions?
4. Do the company's explanations **clearly disclose** the legal basis under which it may comply with **government demands**?
5. Does the company **clearly disclose** that it carries out due diligence on **government demands** before deciding how to respond?
6. Does the company commit to push back on inappropriate or overbroad **government demands**?
7. Does the company provide clear guidance or examples of implementation of its process for **government demands**?

Indicator guidance: Companies increasingly receive government demands to turn over user information. These demands can come from government agencies or courts (both domestic and foreign). We expect companies to publicly disclose their process for responding to demands from governments, along with the basis for complying with these requests. Companies should also publicly commit to pushing back on inappropriate or overbroad government demands.

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 standards for 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 sustainability report
- Company blog posts

P10(b). Process for responding to private requests for user information

The company should **clearly disclose** its process for responding to requests for **user information** that come through **private processes**.

Elements:

1. Does the company **clearly disclose** its process for responding to requests made through **private processes**?
2. Do the company's explanations **clearly disclose** the basis under which it may comply with requests made through **private processes**?
3. Does the company **clearly disclose** that it carries out due diligence on requests made through **private processes** before deciding how to respond?
4. Does the company commit to push back on inappropriate or overbroad requests made through **private processes**?
5. Does the company provide clear guidance or examples of implementation of its process of responding to requests made through **private processes**?

Indicator guidance: Companies increasingly receive private requests to turn over user information. Such requests are often informal requests for user information from a non-governmental entity that do not involve or come through any formal legal process. According to the Wikimedia Foundation—which publishes [transparency reports](#) with data on the number of these types of such requests it receives—private requests for user information include cases in which another company sends them a letter or an email requesting “non-public information” about one of its users. This could include a user's IP or email address.



This indicator expects companies to disclose their processes for handling these types of requests. Companies should explain reasons for complying with these types of requests, and commit to push back on overly broad demands.

Potential sources:

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

P11. Data about demands for user information

P11(a). Data about government demands for user information

The company should regularly publish data about **government demands** for **user information**.

Elements:

1. Does the company list the number of **government demands** it receives by country?
2. Does the company list the number of **government demands** 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 **government demands** that come from **court orders**?
7. Does the company list the number of **government demands** it complied with, broken down by category of demand?
8. Does the company list what types of **government demands** it is prohibited by law from disclosing?
9. Does the company report this data at least once per year?
10. Can the data reported by the company be exported as a **structured data** file?



Indicator guidance: Companies frequently receive demands from governments to hand over user information. These demands can come from government agencies or courts (both domestic and foreign). We expect companies to regularly publish data about the number and type of such demands they receive, and the number of such demands 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 and courts. We also expect company disclosure to indicate the number of accounts affected by these demands and to delineate by category the demands with which the company has complied. We recognize that companies are sometimes not legally allowed to disclose demands for user information made by governments. However, in these cases, we expect companies to report what types of government demands 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 as a 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,
- Company law enforcement report
- Company sustainability report

P11(b). Data about private requests for user information

The company should regularly publish data about requests for **user information** that come through **private processes**.

Elements:

1. Does the company list the number of requests it receives for **user information** that come through **private processes**?
2. Does the company list the number of requests for **user information** that come through **private processes** with which it complied?
3. Does the company report this data at least once per year?
4. Can the data reported by the company be exported as a **structured data** file?

Indicator guidance: Companies increasingly receive private requests to turn over user information. Such requests are often informal requests for user information from a non-governmental entity that do not involve or come through any formal legal process. According to the Wikimedia Foundation—which publishes [transparency reports](#) with data on the number of these types of requests it receives—private requests for user information includes cases in which another company sends them a letter or an email requesting “non-public information” about one of its users. This could include a user’s IP and email address.

Just as companies should publish data about the government demands they receive to hand over user information, companies should also publish data about requests for user information they receive (and comply with) that come through any private processes. 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 also report this data once a year and ensure the data can be exported in a structured data file.

Potential sources:

- Company transparency report
- Company sustainability report
- Corporate social responsibility 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 **demanded 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) demand** their **user information**?
2. Does the company **clearly disclose** that it **notifies** users when they receive requests for their **user information** through **private processes**?
3. Does the company **clearly disclose** situations when it might not **notify** users, including a description of the types of **government demands** 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 other third parties request data about its 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 requests they are prohibited by law from disclosing.

Potential sources:

- Company transparency report
- Company law enforcement guidelines
- Company privacy policy
- Company human rights policy

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: Because companies handle and store immense amounts of information about users, they should have clear security measures in place to ensure this information is kept secure. We 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 and **personal digital assistant 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, **personal digital assistant 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 and **personal digital assistant 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 and **personal digital assistant 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, **personal digital assistant 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?
10. (For **personal digital assistant ecosystems**): Does the company **clearly disclose** what, if any, **modifications it has made to a personal digital assistant operating system**?
11. (For **personal digital assistant ecosystems**): Does the company **clearly disclose** what, if any, effect such **modifications have on the company's ability to send security updates to users**?

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 policies 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: Companies should have clearly disclosed processes in place for addressing data breaches, including clear policies 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 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.

We expect companies to have formal policies in place regarding their handling of data breaches if and when they occur, and to make this information about these policies and commitments public prior to a breach occurring.

Potential sources:

- Company terms of service or privacy policy
- Company security guide

P16. Encryption of user communication and private content (digital platforms)



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 U.N. Special Rapporteur on freedom of expression has stated unequivocally that encryption and anonymity are essential for the exercise and protection of human rights.³¹ 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 to turn on end-to-end encryption, and whether it is enabled by default. For mobile ecosystems and personal digital assistant 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 (digital platforms)

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

Elements:

³¹ “Report on encryption, anonymity, and the human rights framework,” *UN Human Rights Office of the High Commissioner*, <https://www.ohchr.org/en/issues/freedomofopinion/pages/callforsubmission.aspx>, last accessed April 2, 2020.



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 disclose** that it **notifies users** about unusual account activity and possible unauthorized access to their accounts?

Indicator guidance: Companies should help users keep their accounts secure. They 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 **cybersecurity risks**.

Elements:

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

Indicator guidance: Because companies hold such vast amounts of data about users, they are often targets of malicious actors. We expect companies to help users protect themselves against such risks. This can include publishing materials on how to set up advanced account authentication or adjust privacy settings, how to avoid malware, phishing, and social engineering attacks, how to avoid or address bullying or harassment online, and what “safe browsing” means. Companies should present this guidance using clear language, ideally paired with visual materials, designed to help users understand the nature of the risks companies and users can face. These materials can take many forms including tips, tutorials, how-to guides, FAQs, or other resources presented in a way that users can easily understand.

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.

Advertisement — A message that an advertiser has paid a company to display to a subset of its users, consisting of both advertising content and targeting parameters.

Advertiser — A person or entity that has created and/or paid for advertising content. The advertiser typically determines the targeting parameters for each advertisement.

Advertising audience categories — Groups of users, identified for the purpose of delivering targeted advertising, who share certain characteristics and/or interests, as determined on the basis of user information that a company has either collected or inferred.

Advertising content policies — Documents that outline a company's rules governing what advertising content are permitted on the platform.

Advertising content — Any content that someone has paid a company to display to its users.

Advertising network — A company or service that connects advertisers to websites that want to host advertisements. The key function of an ad network is aggregation of ad space supply from publishers and matching it with advertiser demand.

Advertising targeting policies — Documents that outline a company's rules governing what advertising targeting parameters are permitted on the platform.

Advertising technologies — Algorithmic decision-making systems that determine which users will be shown a specific piece of advertising content. This determination may take into account the targeting parameters set by the advertiser, or it may be fully automated.

Affected user — The user who posted content that was restricted by a moderation action or the user associated with a user account that was restricted by a moderation action, and, if applicable, the user(s) who submitted the flag that led to the consideration of a piece of content or an account for a moderation action.

Algorithms: An algorithm is a set of instructions used to process information and deliver an output based on the instructions' stipulations. Algorithms can be simple pieces of code but they can also be incredibly complex, "encoding for thousands of variables across millions



of data points.” In the context of internet, mobile, and telecommunications companies, some algorithms—because of their complexity, the amounts and types of user information fed into them, and the decision-making function they serve—have significant implications for users’ human rights, including freedom of expression and privacy. See: “Algorithmic Accountability: A Primer,” Data & Society, https://datasociety.net/wp-content/uploads/2018/04/Data_Society_Algorithmic_Accountability_Primer_FINAL-4.pdf.

Algorithmic content curation, recommendation, and/or ranking system — A system that uses algorithms, machine learning and other automated decision-making technologies to manage, shape, and govern the flow of content and information on a platform, typically in a way that is personalized to each individual user.

Algorithmic system development policies — Documents that outline a company’s practices related to the development and testing of algorithms, machine learning and automated decision-making.

Algorithmic system use policies — Documents that outline a company’s practices involving the use of algorithms, machine learning and automated decision-making.

Algorithmic system — A system that uses algorithms, machine learning and/or related technologies to automate, optimize and/or personalize decision-making processes.

Automated flag — A flag that originates with an algorithmic system. See also: human-submitted flag.

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.



Appeal — For RDR’s purposes, this definition of appeals includes processes through which users request a formal change to a content moderation or account restriction decision made by a company.

Artificial intelligence — Artificial intelligence has an array of uses and meanings. For the purposes of RDR’s methodology, artificial intelligence refers to systems that resemble, carry out, or mimic functions that are typically thought of as requiring intelligence. Examples include facial recognition software, natural language processing, and others, the use of which by internet, mobile, and telecommunications companies have implications for people’s freedom of expression and privacy rights. See: “Privacy and Freedom of Expression in the Age of Artificial Intelligence,” Privacy International, <https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf>.

Automated decision-making — Technology that makes decisions without significant human oversight or input in the decision-making process, such as through the use of artificial intelligence or algorithms.

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.

Bot — An automated online account where all or substantially all of the actions or posts of that account are not the result of a person.

Botnet — A coordinated network of bots that act in concert, usually because they are under the control of the same person or entity.

Bot policy — A document that outlines a company’s rules governing the use of bots to generate content, disseminate content, or perform other actions. May be part of the company’s terms of service or other document.

Collected user information — User information that a company either obtains directly or acquires from a third party.

Curate, recommend, and/or rank — The practice of using algorithms, machine learning and other automated decision-making systems to manage, shape, and govern the flow of content and information on a platform, typically in a way that is personalized to each individual user.



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.

Cookie(s) — “Cookies are a web technology that let websites recognize your browser. Cookies were originally designed to allow sites to offer online shopping carts, save preferences or keep you logged on to a site. They also enable tracking and profiling so sites can recognize you and learn more about where you go, which devices you use, and what you are interested in – even if you don't have an account with that site, or aren't logged in.” Source: “Surveillance Self Defense: Cookies,” Electronic Frontier Foundation, <https://ssd.eff.org/en/glossary/cookies>.

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).

Content restriction — An action the company takes that renders an instance of user-generated content invisible or less visible on the platform or service. This action could involve removing the content entirely or take a less absolute form, such as hiding it from only certain users (eg inhabitants of some country or people under a certain age), limiting users' ability to interact with it (eg making it impossible to “like”), adding counterspeech to it (eg corrective information on anti-vaccine posts), or reducing the amount of amplification provided by the platform's curation systems.

Content-moderation action — Content moderation is the practice of screening user-generated content posted to internet sites, social media, and other online outlets, in order to determine the appropriateness of the content for a given site, locality, or jurisdiction. The process can result in the content being removed or restricted by a moderator, acting as an agent of the platform or site in question. Increasingly, companies in addition to human moderators rely on algorithmic systems to moderate content and information on their platforms. Source: “Content moderation,” Encyclopedia of Big Data, https://doi.org/10.1007/978-3-319-32001-4_44-1.



Core functionality — The most essential functions or affordances of a product or service. For example, a smartphone’s core functionality would include making and 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.

Cybersecurity 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 inference — Companies are able to draw inferences and predictions about the behaviors, preferences, and private lives of its users by applying “big data” analytics and algorithmic decision making technologies. These methods might be used to make inferences about user preferences or attributes (e.g., race, gender, sexual orientation), and opinions (e.g., political stances), or to predict behaviors (e.g., to serve advertisements). Without sufficient transparency and user control over data inference, privacy-invasive and non-verifiable inferences cannot be predicted, understood, or refuted by users. See: Wachter, Sandra and Mittelstadt, Brent. “A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI,” *Columbia Business Law Review*, 2019(2), <https://ssrn.com/abstract=3248829>.

Data minimization — According to the principle of data minimization, companies should limit the collection of users’ information to that which is relevant and necessary to accomplishing a clearly specified purpose. *See also: use limitation (below)*.

De-identified (user information) — 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.

Digital platforms — For the purposes of the RDR Index methodology, digital platforms refers to a category of the RDR Index that includes internet and mobile ecosystem companies as well as companies that operate e-commerce services and personal digital assistant ecosystems.

Directly notify/direct notification — By direct notification, we mean that when a company changes or updates its policy that applies to a particular service, we expect the company to notify users of these changes via the service. 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.

Discrimination — For the purpose of the RDR Index, discrimination refers to the practice of treating particular people, companies, or products differently from others, especially in an unfair way. Source: Cambridge Business English dictionary, <https://dictionary.cambridge.org/dictionary/english/discrimination>.

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 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 or files 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. See: <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.

Engagement metrics — Numbers describing the popularity of a piece of content or account on the platform, for example followers, connections, contacts, friends, comments, likes, retweets, 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.

Flag — The process of alerting a company that a piece of content or account may be in violation of the company's rules, or the signal that conveys this information to the company. This process can occur either within the platform or through an external process. Flaggers include users, algorithmic systems, company staff, governments, and other private entities.



Flagger — An individual or entity that alerts a company that a piece of content or account may be in violation of the company’s rules. This process can occur either within the platform or through an external process. Flaggers include users, algorithmic systems, company staff, governments, and other private entities.

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. 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 such 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 demands — This includes demands from government ministries or agencies, law enforcement, and court orders in criminal and civil cases.

Government-issued identification — An official document with or without a photo issued by the government that can be used to prove a person’s identity. This includes government ID or any form of documentation that identifies the person by physical location, family, or community. This also includes phone numbers, which are, in many jurisdictions, connected to a person’s offline identity

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) — HRIsAs 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.

Human-submitted flag — A flag that originates with a human being, such as a user, company employee or contractor, government employee or representative, or a human employee or representative of a private entity. See also: automated flag.

Layered policy documents — Terms of service and privacy policies that are divided into hyperlinked sections, allowing users to directly navigate to the section they are interested in viewing.

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.” See: “18 U.S. Code § 2703. Required disclosure of customer communications or records,” Cornell Law School Legal Information Institute, <https://www.law.cornell.edu/uscode/text/18/2703>. “Handbook on European data protection law,” European Court of Human Rights, https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

Non-judicial government demands — 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.

Non-technical means — Companies can acquire user information through non-technical means, such as through purchases, data-sharing agreements, and other contractual relationships with third parties. This acquired data can become part of a “digital dossier” that companies may hold on its users, which can then form the basis for inferred and shared user information



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.

Personal digital assistant ecosystem — A personal digital assistant (PDA) ecosystem consists of an artificial intelligence-powered interface installed on digital devices that can interact with users through text or voice to access information on the Internet and perform certain tasks with personal data shared by the users. Users can interact with PDA ecosystems through **skills**, which are either made available by third-party developers/providers or the PDA itself.

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.^[4] 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 processes — Requests made through a private process rather than a judicial or governmental process. Private requests to restrict content or accounts 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 pp 40-52 of 211 of “Fostering Freedom Online: The Role of Internet Intermediaries,” UNESCO, <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf>.

Private requests for user data are often informal and do not involve any formal legal process. According to the Wikimedia Foundation, which produces [transparency reports](#) that disclose data on the number of these types of requests it receives, private requests for user information includes cases in which another company sends them a letter or an email requesting “non-public information” about one of its users. This could include a user’s IP address and email.

Prioritization — Prioritization occurs when a network operator “manage[s] its network in a way that benefits particular content, applications, services, or devices.” (p. 7 of 400) 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, 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.

Public third-party archive — Ideally, companies publish information about the requests they receive so that the public has a better understanding of how content gets restricted on the platform. Companies may provide information about the requests they receive to a third-party archive, such as [Lumen](#) (formerly called Chilling Effects), which is an independent research project that manages a publicly available database of requests for removal of online content. This type of repository helps researchers and the public understand the types of content that are requested for removal, as well as gain a better understanding of legitimate and illegitimate requests. See <https://cyber.harvard.edu/research/lumen>.

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 the “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>

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.

Skills — Skills are voice-driven personal digital assistant capabilities allowing users to perform certain tasks or engage with online content using devices equipped with a personal digital assistant. Personal digital assistant ecosystem skills are similar to mobile ecosystem



apps: users can enable or disable built-in skills or install skills developed by third-parties through stores similar to app stores.

Skill store — The platform through which a company makes its own skills as well as those created by third-party developers available for download. A skill store (or skill marketplace) is a type of digital distribution platform for computer software.

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,” BSR, September 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.” Source: 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>.

Targeted advertising — Targeted advertising, also known as “interest-based advertising,” “personalized advertising,” or “programmatic advertising,” refers to the practice of delivering tailored ads to users based on their browsing history, location information, social media profiles and activities, as well as demographic characteristics and other features. Targeted advertising relies on vast data collection practices, which can involve tracking users’ activities across the internet using cookies, widgets, and other tracking tools, in order to create detailed user profiles.

Targeting parameters — The conditions, typically set by the advertiser, that determine which users will be shown the advertising content in question. This can include users’ demographics, location, behavior, interests, connections, and other user information

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.

Technical means — Companies deploy various technologies, such as cookies, widgets and buttons to track users’ activity on their services and on third-party sites and services. For example, a company may embed content on a third-party website and collect user information when a user “likes” or otherwise interacts with this content.



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: “Terms of (Ab)use”, Electronic Frontier Foundation, <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).

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: “Data throttling: Why operators slow down your connection speed,” Open Signal, <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).

Unofficial processes —Processes or channels through which the government makes demands or requests for content or account restrictions instead of official processes, such as law or regulation. For example, a local official may make an order or protest on certain content through an informal channel.

Use/purpose limitation — According to the principle of use or purpose minimization, entities that handle user information should state their purpose for doing so and should limit the use of this information for any other purpose unless they receive consent from the user. *See also the principle of data minimization (above).*

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 reset 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 signals 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. User information may be either collected or inferred. 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.

Widget — A piece of code allowing a user or company to embed applications and content from one website or service on a different third-party site or service. In some cases, companies use widgets on a third-party website and collect information about visitors to that website without their knowledge.

Zero-rating program — “Zero-rating” refers to the practice of not charging users for data used to access certain online services or platforms. Zero rating is regarded as a type of network prioritization which undermines the principle of network neutrality.

The logo consists of three white arrows pointing up and to the right, arranged in a triangular pattern. A solid red circle is positioned to the right of the top arrow.

Ranking Digital Rights

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0/>.

