RANKING DIGITAL RIGHTS

2020 Ranking Digital Rights Corporate Accountability Index Draft Indicators

FOR PUBLIC CONSULTATION

April 2020

Acknowledgements

The following Ranking Digital Rights (RDR) research team members were involved in producing this draft of the 2020 RDR Corporate Accountability Index methodology:

- Amy Brouillette, Research Director
- Veszna Wessenauer, Research 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/

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

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, plus disclosed policies affecting users' freedom of expression and privacy.

The RDR Index methodology

The standards the RDR Index uses to measure companies build on more than a decade of work by the human rights, privacy, and security communities. These standards include the UN Guiding Principles on Business and Human Rights, which affirm that just as governments have a duty to protect human rights, companies also have a responsibility to respect human rights. The 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.

About the 2020 RDR Index methodology revision

In January 2019, RDR began a process of expanding and revising the methodology to include new issue areas and new company types.[2] This work has focused on three main areas:

- **Improving current methodology:** This has involved reviewing the 2019 RDR Index methodology to identify key areas for revision and improvement.

[1] 2019 RDR Index, May 2019, https://rankingdigitalrights.org/index2019/.
[2] 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/

- **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 which 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.

This draft version of the 2020 RDR Index methodology incorporates our work in these three areas. Note that this draft includes new indicators on targeted advertising and algorithmic systems that were introduced in October 2019[3] and then pilot-tested by RDR as part of our ongoing methodology development work.[4] Revisions to these draft indicators are clearly marked in this document.

Revisions are presented in further detail in the following documents:

- **A summary of revisions** to the draft 2020 RDR Index methodology

- **A table comparing** the 2019 RDR Index indicators to the draft 2020 RDR Index indicators.

We invite feedback on the proposed revisions through **Friday, May 15, 2020**. Comments should be sent via email to methodology@rankingdigitalrights.org.

How to read this document

The new and revised indicators presented in this document have been integrated into the current RDR Index methodology.

- Revisions to the existing methodology are presented in red.

[3] "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.
[4] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020 https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

- Draft indicators and elements are presented in blue. Revisions made to draft indicators as a result of the pilot test are also marked.

Short explanations for revisions and draft additions are provided after each indicator. A glossary of terms is also appended below. The terms defined in the Glossary are **bolded** in the indicator text.

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,[5] and are enshrined in the International Covenant on Civil and Political Rights.[6] They apply online as well as offline. In order for a company to perform well in this category, the company's disclosure should at least follow, and ideally surpass, the UN Guiding Principles on Business and Human Rights[7] and other industry-specific human rights standards focused on freedom of expression and privacy such as those adopted by the Global Network Initiative.[8]

G1. Policy Commitment

The company should publish a formal **policy commitment** ~~publicly commit~~ 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 ~~and privacy~~?

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**?

Rationale for revisions: Revisions (in red) are structural only. RDR has renamed the "freedom of expression" category to "freedom of expression and information." Previously, the methodology combined the evaluation of company oversight over freedom of expression and privacy at each governance level in one element. This proposed revision breaks out freedom

[5] "Universal Declaration of Human Rights," https://www.un.org/en/universal-declaration-human-rights/
[6] "International Covenant on Civil and Political Rights," *UN Human Rights Office of the High Commissioner*, https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.
[7] "Guiding Principles on Business and Human Rights," *UN Human Rights Office of the High Commissioner*, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.
[8] "The GNI Principles," *Global Network Initiative*, https://globalnetworkinitiative.org/gni-principles/.

of expression and privacy into separate element questions. No score changes will result from these revisions.

Rationale for adding draft Element 3: Draft Element 3 was introduced in October 2019[9] and then pilot-tested by RDR as part of our ongoing methodology development work.[10] Based on our pilot test, RDR has opted to include this element in this draft of the 2020 RDR Index methodology.

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 UN Guiding Principles on Business and Human Rights' Operational Principle 16, which states that companies should adopt formal policies publicly affirming their commitments to international human rights principles and standards.[11] 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 *Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems* (2019).[12] 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:

[9] "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."

[10] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020 https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

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

[12] "Addressing the impacts of Algorithms on Human Rights: Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems," *Council of Europe*, Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (2019), https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eecf.

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

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 ~~and privacy~~?

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 ~~and privacy~~?

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

Rationale for revisions: Revisions (in red) are structural only. RDR has renamed the "freedom of expression" category to "freedom of expression and information." Previously, the methodology combined the evaluation of company oversight over freedom of expression and privacy at each governance level in one element. This proposed revision breaks out freedom of expression and privacy into separate elements, which will better surface this data. No score changes will result from these revisions.

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 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 ~~and privacy~~ 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 ~~and privacy~~ 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?

Rationale for revision: These revisions (in red) are structural only. RDR has renamed the "freedom of expression" category to "freedom of expression and information." Previously, the methodology evaluated both freedom of expression and privacy in one element. This proposed revision breaks out freedom of expression and privacy into separate elements, which will better surface this data. No score changes will result from these revisions.

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

The company should conduct regular, comprehensive, and credible due diligence, through robust **human rights impact assessments**, to identify how government regulations and policies ~~all aspects of its business~~ 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. ~~As part of its decision-making, d~~Does the company consider how laws affect freedom of expression and information ~~and privacy~~ in jurisdictions where it operates?

2. Does the company consider how laws affect privacy in jurisdictions where it operates?

3. Does the company ~~regularly~~ **assess** freedom of expression and information ~~and privacy~~ 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 ~~and privacy~~ risks associated with a new activity, including the launch and/or acquisition of new products, services, or companies, or entry into new markets 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 assess freedom of expression and privacy risks associated with the processes and mechanisms used to enforce its terms of service (ToS)?~~

~~8. Does the company assess freedom of expression and privacy risks associated with its targeted advertising policies and practices?~~

~~9. Does the company disclose that it assesses freedom of expression and privacy risks associated with its use of automated decision-making, such as through the use of algorithms and/or artificial intelligence?~~

10. Does the company disclose that it conducts additional evaluation whenever the company's **risk assessments** identify concerns?

11. Does the company disclose that **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?

12. Does the company conduct **assessments** on a regular schedule?

13. Are the company's **assessments** assured by an external **third party**?

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

Rationale for revisions: This indicator has been revised to focus on human rights due diligence practices related to government regulations and policies. The revisions remove three elements, which were evaluated as part of this Indicator G4 in the 2019 RDR Index,[13] related to terms of service enforcement, targeted advertising, and the use of algorithms, which are now presented separately in new G4 indicators below. Additional revisions (in red) were introduced in order to clarify this draft indicator's focus on jurisdictional issues.

Indicator guidance: People face human rights risks when they use digital tools. Human rights impact assessments (HRIAs) are a way for companies to learn about and to address those risks, or at the very least try to mitigate them, especially when introducing new products and services or entering new markets, or when incorporating the use of automated decision-making.

This indicator examines whether companies disclose if they conduct regular, robust, and accountable due diligence to identify human rights risks in the jurisdictions in which they operate as well as those they are planning to enter. These assessments are aimed both at identifying possible risks to users' freedom of expression and privacy rights, and taking 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 can include sensitive information. Rather, companies should disclose that they conduct HRIAs and provide information on what their

[13] "G4. Impact assessment," https://rankingdigitalrights.org/2019-indicators/#G4.

HRIA process encompasses. If a company conducts HRIAs but does not publicly disclose the fact that it does so, the company will not receive credit.

Potential sources:

- Company CSR/sustainability reports
- Company human rights policy
- Reports from third-party assessors or accreditors
- 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 **clearly disclose** that it assesses freedom of expression and information risks of ~~associated with its processes for~~ enforcing its terms of service?

2. Does the company **clearly disclose** it conducts risk assessments of ~~on assesses how effectively it enforces~~ its enforcement of its privacy policies?

3. Does the company disclose that it **assesses** discrimination risks associated with its processes for enforcing its **terms of service**?

4. Does the company **clearly disclose** that it **assesses 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?

Rationale for adding draft Indicator G4b: Draft Indicator G4b was introduced in October 2019[14] and then pilot-tested by RDR as part of our ongoing methodology development work. [15] Based on our pilot test, RDR has opted to include this indicator in this draft of the 2020 RDR Index methodology. This draft indicator breaks out one element question (Element 7) from the current Indicator G4 into several elements related to company human rights due diligence practices associated with their own policy enforcement. This indicator encourages companies to conduct risk assessments to help identify and mitigate possible harms as a result of their rule-enforcement processes. The elements are meant to capture both the risk of a process being inadequate, leading to underenforcement, and the risk of a process creating other harms, such as overenforcement or discrimination.

Rationale for revisions to draft Elements 1 and 2: Elements 1 and 2 of this indicator are adapted from Element 7 of the current Indicator G4 (which asks: "Does the company assess freedom of expression and privacy risks associated with the processes and mechanisms used to enforce its terms of service (ToS)?"). The element language has been revised as a result of internal testing by RDR.

Indicator guidance: This indicator examines whether companies disclose if they conduct formal risk assesments on 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 processes that are aimed at ensuring that a company's decisions and practices align with its human rights obligations and commitments.

Note that this indicator does not expect companies to publish detailed results of their human rights impact assessments, since a thorough assessment may include sensitive information. Rather, it expects that companies disclose that they conduct HRIAs and provide information on what their HRIA process encompasses. If a company conducts HRIAs but does not publicly disclose the fact that it does so, the company will not receive credit.

Potential sources:

- Company CSR/sustainability reports
- Company human rights policy
- Reports from third-party assessors or accreditors
- 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

[14] "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.

[15] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020 https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

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 disclose that it **assesses** freedom of expression and information risks associated with its **targeted advertising** policies and practices?

2. Does the company disclose that it **assesses** privacy risks associated with its **targeted advertising** policies and practices?

3. Does the company disclose that it **assesses** 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?

Rationale for adding draft Indicator G4c: Draft Indicator G4b was introduced in October 2019[16] and then pilot-tested by RDR as part of our ongoing methodology development work. [17] Based on our pilot test, RDR has opted to include this indicator in this draft of the 2020 RDR Index methodology. Elements 1 and 2 of this indicator are based on the current Element 8 from Indicator G4 which asks: "Does the company assess freedom of expression and privacy risks associated with its targeted advertising policies and practices?" Element 3 expands the scope of this indicator to include risk assessment of how companies' targeted advertising policies might be discriminatory.

Indicator guidance: This indicator examines whether companies disclose the existence of human rights risk assessment processes in their policies and practices relating to targeted

[16] "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.
[17] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020 https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

advertising. These assessments represent a systematic internal examination to ensure that a company's decisions and practices align with its commitment (and responsibility) to respect freedom of expression and information, privacy, and non-discrimination.

Targeted advertising can have adverse affects on human rights, specifically freedom of information, freedom of opinion, and freedom from discrimination.[18] 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.

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
- Reports from third-party assessors or accreditors
- Global Network Initiative assessment reports
- Company advertising policies

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' 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 disclose that it **assesses** freedom of expression and information risks associated with its development and use of **algorithmic systems**?

[18] "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.

2. Does the company disclose that it **assesses** privacy risks associated with its development and use of **algorithmic systems**?

3. Does the company disclose that it **assesses** **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?

Rationale for adding Indicator G4d: Draft Indicator G4b was introduced in October 2019[19] and then pilot-tested by RDR as part of our ongoing methodology development work.[20] Based on our pilot test, RDR has opted to include this indicator in this draft of the 2020 RDR Index methodology. Elements 1 and 2 of this indicator are based on the current Element 9 from Indicator G4 which asks: "Does the company disclose that it assesses freedom of expression and privacy risks associated with its use of automated decision-making, such as through the use of algorithms and/or artificial intelligence?" Element 3 expands the scope of this indicator to include risk assessment of how companies' development and use of algorithmic systems might lead to or exacerbate discrimination.

Indicator guidance: There are a variety of ways in which algorithmic systems may pose harms to human rights.[21] 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 risks leading to discrimination. Companies should therefore conduct human rights risk assessments related to their development and use of algorithms, as

[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.
[20] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020 https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.
[21] "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.

recommended by the Council of Europe's *Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems* (2019).[22]

Note that this indicator does not expect companies to publish detailed results of their human rights impact assessments, since a thorough assessment may include sensitive information. Rather, it expects that companies should disclose that they conduct HRIAs and provide information on what their HRIA process encompasses. If a company conducts HRIAs but does not publicly disclose the fact that it does so, the company will not receive credit.

Potential sources:

- Company CSR/sustainability reports
- Company human rights policy
- Regulatory documents (e.g., U.S. Federal Trade Commission)
- Reports from third-party assessors or accreditors
- Global Network Initiative assessment reports
- Company artificial intelligence policies, including AI principles, frameworks, and use guidelines

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 **clearly disclose** that it assesses freedom of expression and information risks associated with its **zero-rating** programs?

2. Does the company **clearly disclose** that it assesses privacy risks associated with its **zero-rating** programs?

3. Does the company **clearly disclose** that it assesses discrimination risks associated with its **zero-rating** programs?

4. Does the company conduct additional evaluation wherever the company's **risk assessments** identify concerns?

[22] "Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems,'' *Council of Europe*, https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eecf.

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?

Rationale for adding Indicator G4e: "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.

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, ~~and~~ 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 initiative~~s~~** that address the full range of ways in which freedom of expression and information, privacy, and related human rights may be affected in the course of the company's operations? ~~based on international human rights principles?~~

2. If the company is not a member of one or more such **multi-stakeholder initiative~~s~~**, is the company a member of any organizations that engage~~s~~ systematically and on a regular basis with non-industry and non-governmental stakeholders on freedom of expression and privacy?

3. If the company is not a member of one of these organizations, does the company disclose that it initiates or participates in meetings with **stakeholders** that represent, advocate on behalf of, or are people whose freedom of expression and privacy are directly impacted by the company's business?

Rationale for revisions: Suggested revisions (in red) address the expanded scope of the RDR Index methodology to include multistakeholder engagement standards and accountability mechanisms that extend beyond just government demands. Indicator G5 sets standards for companies to engage with a range of stakeholders about their policies and practices affecting users' freedom of expression and privacy. In previous RDR Index cycles, companies that are members of the Global Network Initiative would automatically score full credit on this indicator since GNI is an inherently multi-stakeholder organization (with a governing board made up of human rights organizations, investors, and academics, in addition to company representatives). However, GNI focuses primarily on holding its members accountable for upholding principles of freedom of expression and privacy, primarily in relation to *government demands*. The proposed revisions reflect our broadened scope to include a wider range of issues addressed in the RDR Index methodology beyond just government demands. Stakeholder feedback on these proposed revisions is a priority for RDR.

Indicator guidance: This indicator seeks evidence that the company engages with and (for full credit) commits to being accountable by 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 encompasses solely 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 around other human rights risks will only result in 50 percent credit for 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 ~~or privacy~~ has 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- ~~or privacy~~-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 ~~and privacy~~?

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 ~~and privacy~~ **grievances**?

9. Does the company **clearly disclose** evidence that it is providing **remedy** for privacy **grievances**?

Rationale for revisions: These revisions (in red) are structural only. Previously, the methodology combined the evaluation of company grievance and remedy mechanisms regarding freedom of expression and privacy complaints in one element. This proposed revision breaks out freedom of expression and privacy into separate elements, which will better surface this data. No score changes will result from these revisions.

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.[23]

Potential sources:

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

[23] "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.

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 users the ability to **appeal content-moderation actions**?
2. Does the company **clearly disclose** that it **notifies** the user who is **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** the role of humans in reviewing **appeals**?
8. Does the company **clearly disclose** what role automation plays in reviewing **appeals**?
9. Does the company **clearly disclose** that the **affected user** has an opportunity to present additional information that will be considered in the review?
10. Does the company **clearly disclose** that it provides the **affected user** a statement outlining the reason for its decision?
11. Does the company **clearly disclose** evidence that it is addressing content moderation **appeals**?

Rationale for adding draft Indicator G6(b): 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.

Indicator guidance: Remedy is only meaningful and effective when it is implemented properly. In the case of content moderation, this means maintaining a robust and structured appeals process. We expect companies to provide information on both their mechanisms for offering appeals and processing them. 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.

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,[24] the International Covenant on Civil and Political Rights,[25] 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) ~~most commonly~~ spoken by ~~the company's~~ users in the company's home jurisdiction?

[24] "Universal Declaration of human Rights," https://www.un.org/en/universal-declaration-human-rights/.
[25] "International Covenant on Civil and Political Rights," *UN Human Rights Office of the High Commissioner*, https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx,

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

Rationale for revision: Indicator F1(a) is the same as Indicator F1 from the existing RDR Index methodology.[26] Revisions made to Element 2 clarify what RDR evaluates in this element. Element 2 evaluates if companies publish their terms of service in the primary languages of their home market. RDR does not evaluate if a company offers policies in the primary languages of every market in which it operates. The proposed revision clarifies the scope of our evaluation. No score changes would occur as a result of this revision.

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 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) ~~most commonly~~ spoken by ~~the company's~~ users in the company's home jurisdiction?

[26] "F1. Access to terms of service," https://rankingdigitalrights.org/2019-indicators/#F1

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** ~~which display **targeted advertising**~~ to provide users with ~~a link to~~ 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**?

Rationale for adding draft Indicator F1b: Draft Indicator F1b was introduced in October 2019[27] and then pilot-tested by RDR as part of our ongoing methodology development work.[28] Based on our pilot test, RDR has opted to include this indicator in this draft of the 2020 RDR Index methodology, with some revisions summarized below.

In addition, a new draft Element 5 has been added to address whether personal digital assistant ecosystems (such as Amazon's Alexa and Alibaba's AliGenie) require third-party **skills** (or voice-driven applications) to provide users with ad content policies. Skills are voice-driven personal digital assistant capabilities that allow users to perform certain tasks or engage with online content. Personal digital assistant ecosystem "skills" are similar to mobile ecosystem apps: users can enable or disable these built-in skills or install skills developed by third parties through "**skill stores**," similar to app stores.

Rationale for revisions: Revisions (in red) made to Element 2 clarify what RDR evaluates in this element. Element 2 evaluates if companies publish advertising policies in the primary languages of their home market. RDR does not evaluate if a company offers policies in the primary languages of every market in which it operates. The proposed revision clarifies the scope of our evaluation. No score changes would occur as a result of this revision. Draft Element 4 has been revised to clarify what we are looking for in that element, based on learnings from the pilot test.

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.

---

[27] "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.

[28] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020 https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

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) ~~most commonly~~ spoken by ~~the company's~~ **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** ~~which display **targeted advertising**~~ to provide users with ~~a link to~~ 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**?

Rationale for adding draft Indicator F1c: Draft Indicator F1c was introduced in October 2019[29] and then pilot-tested by RDR as part of our ongoing methodology development work.[30] Based on our pilot test, RDR has opted to include this indicator in this draft of the 2020 RDR Index methodology, with some revisions, which are summarized below.

[29] "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.

[30] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

In addition, a new draft Element 5 has been added to address whether personal digital assistant ecosystems (such as Amazon's Alexa and Alibaba's AliGenie) require third-party **skills** (or voice-driven applications) to provide users with ad targeting policies. Skills are voice-driven personal digital assistant capabilities that allow users to perform certain tasks or engage with online content. Personal digital assistant ecosystem "skills" are similar to mobile ecosystem apps: users can enable or disable these built-in skills or install skills developed by third-parties through "**skill stores**," similar to app stores.

Rationale for revisions: Revisions (in red) made to Element 2 clarify what RDR evaluates in this element. Element 2 evaluates if companies publish ad targeting policies in the primary languages of their home market. RDR does not evaluate if a company offers policies in the primary languages of every market in which it operates. The proposed revision clarifies the scope of our evaluation. No score changes would occur as a result of this revision. Draft Element 4 has been revised to clarify what we are looking for in that element, based on learnings from the pilot test.

Indicator guidance: In addition to providing accessible ad content policies (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 them[31]—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.[32]

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 (Element 1) and understand (Element 3), and that are available in the main languages of the company's home market (Element 2). For mobile ecosystems (Element 4) and personal digital assistant ecosystems (Element 5), 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.

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.

Note that ad targeting policies can often be found in a company's broader ad content policy. This indicator does not require companies to have a discrete policy specifically on ad targeting. It does, however, expect companies to have clearly accessible and understandable policies governing ad targeting on its platform or service.

---

[31] 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.
[32] "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.

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) ~~most commonly~~ spoken by ~~the company's~~ users in the company's home jurisdiction?

3. Are the **algorithmic system use policies** presented in an **understandable manner**?

Rationale for adding draft Indicator F1d: Draft indicator F1d was introduced in October 2019[33] and then pilot-tested by RDR as part of our ongoing methodology development work.[34] Based on our pilot test, RDR has opted to include this indicator in this draft of the 2020 RDR Index methodology, with some revisions, summarized below. While all companies we piloted use algorithmic systems in various ways in their products and services, none disclosed a discrete algorithmic use policy.[35] We have decided to retain this indicator in this draft 2020 RDR Index methodology to encourage companies to disclose clear policies describing how they use these systems.

Rationale for revisions: Revisions (in red) made to Element 2 clarify what RDR evaluates in this element. Element 2 evaluates if companies publish terms in the primary languages of their home market. RDR does not evaluate if a company offers policies in the primary languages of every market in which it operates. The proposed revision clarifies the scope of our evaluation. No score changes would occur as a result of this revision.

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 information as well as the right to non-discrimination.[36] In addition to clearly committing to

---

[33] "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.

[34] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

[35] ''2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

[36] "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.

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.[37] As recommended by the Council of Europe's *Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence*, 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 uses algorithmic systems to curate or manage digital content. We also look for companies to disclose terms that outline how companies develop and test algorithmic systems, which is addressed in the Privacy category in draft 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** ~~provides~~ ~~**notice** and **documentation to**~~ 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 ~~provides~~ **directly notifies users** of changes prior to these changes coming into effect?

4. Does the company maintain a **public archive** or **change log**?

[37] "Addressing the impacts of Algorithms on Human Rights: Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems," *Council of Europe*, Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (2019), https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eecf.

Rationale for revisions: This indicator is the same as Indicator F1 from the existing RDR Index methodology.[38] Proposed revisions (in red) clarify our evaluation standards on this indicator. In this indicator, RDR expects companies to commit to notifying users of changes to the terms of service or user agreements in a manner that the user will be sure to see and access. We therefore expect companies to *directly notify* users of changes on the platform or service. The proposed revisions bring the indicator language into alignment with the standards RDR already applies in evaluating companies on this indicator.

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 will be 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 on the main page where users access the service.

This indicator also seeks evidence that a company provides publicly available records of previous terms so that people can understand how the company's terms have evolved over time.

For companies that have two or more applicable policy documents (for example, one general terms of service and one service-specific terms), each document has to meet the element criteria in order to receive full credit.

Potential sources:

- Company terms of service

F2(b). Changes to advertising content policies

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

Elements:

[38] "2019 Indicators: F1. Access to terms of service," *Ranking Digital Rights*, https://rankingdigitalrights.org/2019-indicators/#F1

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 ~~provides~~ **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**?

Rationale for adding draft Indicator F2b: Draft indicator F2b was introduced in October 2019[39] and then pilot-tested by RDR as part of our ongoing methodology development work. [40] Based on our pilot test, RDR has opted to include this indicator in this draft of the 2020 RDR Index methodology, with some revisions, summarized below.

In addition, a new draft Element 6 has been added to address whether personal digital assistant ecosystems (such as Amazon's Alexa and Alibaba's AliGenie) require third-party **skills** (or voice-driven applications) to notify users when these skills change their advertising content policies. Skills are voice-driven personal digital assistant capabilities that allow users to perform certain tasks or engage with online content. Personal digital assistant ecosystem "skills" are similar to mobile ecosystem apps: users can enable or disable these built-in skills or install skills developed by third parties through "**skill stores**," similar to app stores.

Rationale for revisions: Proposed revisions (in red) clarify our evaluation standards on this indicator. In this indicator, RDR expects companies to commit to notifying users of changes to the terms of service or user agreements in a manner that the user will be sure to see and access. We therefore expect companies to *directly notify* users of changes on the platform or service. The proposed revisions bring the indicator language into alignment with the standards RDR already applies in evaluating companies on this indicator.

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

[39] "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.
[40] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

to notifying users when they change these terms and to providing users with information that helps them understand what these changes mean.

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** ~~provides **notice** and **documentation** to~~ **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 ~~provides~~ **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**?

Rationale for adding draft Indicator F2c: Draft indicator F2c was introduced in October 2019[41] and then pilot-tested by RDR as part of our ongoing methodology development work. [42] Based on our pilot test, RDR has opted to include this indicator in this draft of the 2020 RDR Index methodology, with some revisions, summarized below.

In addition, a new draft Element 6 has been added to address whether personal digital assistant ecosystems (such as Amazon's Alexa and Alibaba's AliGenie) require third-party **skills** (or voice-driven applications) to notify users when these skills change their ad targeting policies. Skills are voice-driven personal digital assistant capabilities that allow users to perform certain tasks or engage with online content. Personal digital assistant

[41] "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.
[42] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

ecosystem "skills" are similar to mobile ecosystem apps: users can enable or disable these built-in skills or install skills developed by third parties through "**skill stores**," similar to app stores.

Rationale for revisions: Proposed revisions (in red) clarify our evaluation standards on this indicator. In this indicator, RDR expects companies to commit to notifying users of changes to the terms of service or user agreements in a manner that the user will be sure to see and access. We therefore expect companies to *directly notify* users of changes on the platform or service. The proposed revisions bring the indicator language into alignment with the standards RDR already applies in evaluating companies on this indicator.

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.

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** ~~provides notice and documentation to~~ **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 ~~provides~~ **directly notifies users** of changes prior to these changes coming into effect?
4. Does the company maintain a **public archive** or **change log**?

Rationale for addition of draft Indicator F2d: Draft indicator F2d was introduced in October 2019[43] and then pilot-tested by RDR as part of our ongoing methodology development work. Based on our pilot test, RDR has opted to include this indicator in this draft of the 2020 RDR Index methodology, with some revisions, summarized below. While all companies we piloted use algorithmic systems in various ways in their products and

[43] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

services, none disclosed a discrete algorithmic use policy.[44] We have decided to retain this indicator in this draft 2020 RDR Index methodology to encourage companies to disclose clear policies describing how they use these systems.

Rationale for revisions: Proposed revisions (in red) clarify our evaluation standards on this indicator. In this indicator, RDR expects companies to commit to notifying users of changes to the terms of service or user agreements in a manner that the user will be sure to see and access. We therefore expect companies to *directly notify* users of changes on the platform or service. The proposed revisions bring the indicator language into alignment with the standards RDR already applies in evaluating companies on this indicator.

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 Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (2019).[45]

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?

[44] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

[45] "Addressing the impacts of Algorithms on Human Rights: Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems," *Council of Europe*, Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (2019), https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eecf.

4. Does the company **clearly disclose** whether 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?

~~8. Does the company provide clear examples to help the user understand what the rules are and how they are enforced?~~

Rationale for revisions: Indicator F3(a) is adapted from Indicator F3 in the existing RDR Index methodology.[46] Revisions (in red) to Element 7 clarify the evaluation standard. Element 8 has been removed, since the standard for this element is unclear.

Rationale for adding draft Element 4: New draft Element 4 is aimed at ensuring this indicator clearly evaluates whether companies disclose if they use algorithmic systems to flag terms of service violations. Note that RDR previously captured this information in Element 3, which asks if companies clearly disclose the processes they use to identify content or accounts that violate the company's rules. However, given our new focus on how companies use automation in the context of content moderation, we opted to create a separate element specifically asking about the use of algorithmic systems.

Indicator guidance: Companies can set rules for what content users can post on a service as well as what activities users can engage in on the service. Companies can also restrict a user's account, meaning that the user is unable to access the service, for violating these rules.

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. 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

[46] "2019 Indicators: F3. Process for terms of service enforcement," *Ranking Digital Rights*, https://rankingdigitalrights.org/2019-indicators/#F3

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 ~~content~~ policies governing what types of advertising content is prohibited ~~**third parties'** use of advertising technologies on the platform.~~

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** ~~that~~ all **advertising content** to ~~must~~ be clearly labelled as such?

3. 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?

Rationale for adding draft Indicator F3b: Draft indicator F3b was introduced in October 2019[47] and then pilot-tested by RDR as part of our ongoing methodology development work.[48] Based on the pilot test, we are opting to include this indicator in this draft of the 2020 RDR Index methodology, with some minor revisions to the wording, summarized below.

Rationale for revisions: Revisions (in red) clarify and improve the indicator and element language.

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 (Element 1), whether the company discloses a requirement that all advertising content be clearly labeled as such (Element 2), and whether the company discloses its processes for enforcing these rules (Element 3).

[47] "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.
[48] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

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 ~~its targeting policies governing **third parties'** use of **advertising technologies** on its products and services~~.

Elements:

1. Does the company **clearly disclose** whether it enables **third parties** to target its **users** with ~~will be shown~~ **advertising content** ~~based on their browsing history, location information, social media use, demographic characteristics, or other **user information**~~?

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** its guidelines for evaluating algorithmically generated **advertising audience categories** to ensure they do not contribute to human rights harms?~~

6. ~~5.~~ 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?

Rationale for adding draft Indicator F3c: Draft indicator F3c was introduced in October 2019[49] and then pilot-tested by RDR as part of our ongoing methodology development work.[50] Based on the pilot test, we are opting to include this indicator in this draft of the 2020 RDR Index methodology, with some minor revisions, summarized below.

[49] "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.
[50] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

Rationale for revisions: Revisions (in red) are primarily made to clarify and strengthen the indicator and element language. Suggested revisions to Element 1 clarify this baseline element, which asks companies to disclose that they enable third parties to target their users with advertising or other types of tailored content. Element 5 has been deleted, since assessing human rights risks associated with developing algorithmic systems is addressed in draft Indicator G4d.

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 them[51]—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.[52]

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 (non-paid) content (Element 1), and clearly disclose what targeting parameters—like using certain types of audience categories, like age, location, or other user characteristics—are not permitted (Element 2). Companies should also disclose their processes for identifying breaches to targeting rules (Element 5).

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** ~~or accounts~~ that violates the company's rules.

Elements:

[51] 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

[52] "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.

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

2. Does the company publish ~~clearly disclose~~ data on the number of pieces of **content restricted** based on which rule was violated?

3. Does the company publish ~~clearly disclose~~ data on the number of pieces of **content** it **restricted** based on the method used to identify the violation?

~~2.~~ 4. Does the company publish this data at least four times ~~once~~ a year?

~~3.~~ 5. Can the data be exported as a **structured data** file?

Rationale for revisions: This indicator is a revision of Indicator F4 from the existing RDR Index.[53] Indicator F4 is now broken out into two indicators (F4a and F4b), examining company disclosure of data about terms of service enforcement. F4a examines company disclosure of data about *content* restrictions as a result of terms of service violations; F4b examines company disclosure of data about *account* restrictions as a result of terms of service violations.

Revisions (in red) reflect the evolution of standards for company disclosure of the actions they take to enforce their own terms of service. Since introducing this indicator in 2015,[54] RDR has tracked progressive improvements by companies in this area. At the same time, there has been a growing consensus among digital rights experts about the types of data companies should be publishing about the actions they take to enforce their own rules. Revised Element 1 asks companies to publish data about the number of pieces of content companies remove, block, or otherwise restrict access to for breaches to terms of service or community standards. This proposed revision also removes account restrictions from this element, as we have broken out account restrictions into a new draft indicator below (F4b). Revised Element 4 asks companies to publish data about their terms of service enforcement at least four times a year, as opposed to once a year, in line with the Santa Clara Principles.[55]

Rationale for adding draft Elements 2 and 3: New draft Elements 2 and 3 are aimed at setting clear disclosure standards about the decisions companies make to restrict content. Element 2 asks companies to disclose data about content restrictions based on the rule that was violated. Element 3 asks companies to publish data about how the rules violation was identified. In this element, we expect companies to clearly disclose data clarifying the role of human flaggers and/or algorithmic systems in flagging content that breaches community standards or terms of service policies.

[53] "2019 Indicators: F4. Data about terms of service enforcement," *Ranking Digital Rights*, https://rankingdigitalrights.org/2019-indicators/#F4
[54] "2019 Indicators: F9. Network management (telecommunications companies)," *Ranking Digital Rights*, https://rankingdigitalrights.org/2019-indicators/#F9
[55] "The Santa Clara Principles On Transparency and Accountability in Content Moderation," https://santaclaraprinciples.org, last accessed April 1, 2020.

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 (Element 1). They should also break out this data by violation (Element 2) and by the method—such as a community flagger program or automation—through which the rules violation was detected (Element 3). Companies should also publish this data at least four times a year (Element 4) and in a structured data file (Element 5).

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 pieces of **content 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?

Rationale for revisions: This indicator is a revision of Indicator F4 from the previous three RDR Indexes (see 2019 RDR Index).[56] Indicator F4 is now broken out into two indicators (F4a and F4b), examining company disclosure of data about terms of service enforcement. F4a examines company disclosure of data about content restrictions as a result of terms of

[56] "2019 Indicators: F4. Data about terms of service enforcement," *Ranking Digital Rights*, https://rankingdigitalrights.org/2019-indicators/#F4

service violations; this indicator (F4b) examines company disclosure of data about account restrictions as a result of terms of service violations.

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 (Element 1). They should also break out this data by violation (Element 2) and by the method—such as a community flagger program or automation—through which the rules violation was detected (Element 3). Companies should also publish this data at least four times a year (Element 4) and in a structured data file (Element 5).

F4(c). Data about advertising content 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**.

Elements

1. Does the company publish ~~list~~ the total number of ~~pieces of~~ **advertisements** ~~content~~ it **restricted** to enforce its **advertising content policies**?

2. Does the company publish ~~break down~~ the number of ~~pieces of~~ **advertisements** ~~content~~ it **restricted** based on which rule was violated?

3. Does the company publish ~~break down~~ the number of ~~pieces of~~ **advertisements** ~~content~~ it **restricted** based on the method used to identify the violation ~~the nature of the restriction~~?

~~4. Does the company disclose the number of times **advertising content** was **flagged**, broken down by which type of entity submitted the flag (such as company staff, artificial intelligence, or users)?~~

~~5. Does the company disclose the number of pieces of **advertising content** it restricted in an entirely automated manner, without a **human-submitted flag** or any other direct human input?~~

~~6. Does the company break down the number of pieces of **advertising content** it restricted based on the format of **content**? (e.g. text, image, video, live video)~~

4. Does the company publish this data at least four times a year?

5. Can the data be ~~accessed through a **robust programmatic interface** or~~ exported as a **structured data file**?

Rationale for adding draft Indicator F4c: Draft Indicator F4c was introduced in October 2019 and then pilot-tested by RDR as part of our ongoing methodology development work.[57] Based on the pilot test, we are opting to include this indicator in this draft of the 2020 RDR Index methodology, with some revisions, summarized below.

Rationale for revisions: Revisions (in red) bring elements in this indicator in line with proposed revisions to F4(a) and F4(b). Elements 4 and 5 have been removed, as the method of flagging is covered under revised Element 3. Element 6 has been deleted because RDR wishes to prioritize baseline standards for transparency in this indicator.

Indicator guidance: Indicator F3c expects companies to clearly disclose policies for what types of advertising content are prohibited on a platform or service, and its processes for enforcing these rules. This indicator 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. 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 and in a structured data file.

Potential sources:
- Company transparency report
- Company community standards enforcement report

F4(d). Data about 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 targeting policies**.

Elements

1. Does the company publish ~~list the~~ total number of pieces of **advertising content** it **restricted** to enforce its **advertising targeting policies**?

2. Does the company publish ~~break down~~ the number of pieces of **advertising content** it **restricted** based on which rule was violated?

[57] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

3. Does the company publish ~~break down~~ the number of pieces of **advertising content** it **restricted** based on the method used to identify the violation ~~the nature of the restriction~~?

4. ~~Does the company disclose the number of times **advertising content** was **flagged**, broken down by which type of entity submitted the flag (such as company staff, artificial intelligence, or users)?~~

5. ~~Does the company disclose the number of pieces of **advertising content** it **restricted** in an entirely automated manner, without a **human-submitted flag** or any other direct human input?~~

6. ~~Does the company break down the number of pieces of **advertising content** it **restricted** based on the format of content? (e.g. text, image, video, live video)~~

4. Does the company publish this data at least four times a year?

5. Can the data be ~~accessed through a **robust programmatic interface** or~~ exported as a **structured data file**?

Rationale for adding draft Indicator F4d: Draft Indicator F4d was introduced in October 2019 and then pilot-tested by RDR as part of our ongoing methodology development work.[58] Based on the pilot test, we are opting to include this indicator in this draft of the 2020 RDR Index methodology, with some revisions, summarized below.

Rationale for revisions: Revisions (in red) bring elements in this indicator in line with proposed revisions to F4(a), F4(b), and F4(c). Elements 4 and 5 have been removed, as the method of flagging is covered under revised Element 3. Element 6 has been deleted because RDR wishes to prioritize more baseline standards for transparency in this indicator.

Indicator guidance: Indicator F3c expects companies to clearly disclose policies for what types of advertising content are prohibited on a platform or service, and its processes for enforcing these rules. This indicator asks companies to publish evidence that they are enforcing these rules. Companies should publish data on the total number of ads they remove as a result of breaches to their ad content policies. 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 and in a structured data file.

Potential sources:
- Company transparency report
- Company community standards enforcement report

[58] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

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

F5(a). Process for responding to government ~~third-party~~ demands ~~requests~~ to restrict ~~for~~ content or account~~s restriction~~

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

Elements:

1. Does the company **clearly disclose** its process for responding to **non-judicial government** demands ~~requests~~?
2. Does the company **clearly disclose** its process for responding to **court orders**?
3. Does the company **clearly disclose** its process for responding to **government** demands ~~requests~~ from foreign jurisdictions?

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

~~5.~~ 4 Do the company's explanations **clearly disclose** the legal basis under which it may comply with **government** demands ~~requests~~?

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

~~7.~~ 5. Does the company **clearly disclose** that it carries out due diligence on **government** demands ~~requests~~ before deciding how to respond?

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

~~9.~~ 6. Does the company commit to push back on inappropriate or overbroad **demands** ~~requests~~ **made by governments**?

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

~~11.~~ 7. Does the company provide clear guidance or examples of implementation of its process of responding to **government** demands ~~requests~~?

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

Rationale for revisions: The proposed revisions (in red) move five elements focused on "private requests" into a separate indicator (F5b), in order to ensure that F5a is focused

exclusively on government demands. We also revised the wording of "government requests" to "government demands" which more accurately reflects the nature of these orders.

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 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 ~~**private**~~ **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 ~~**private**~~ **requests** made through **private processes**?
3. Does the company **clearly disclose** that it carries out due diligence on ~~**private**~~ **requests** made through **private processes** before deciding how to respond?
4. Does the company commit to push back on inappropriate or overbroad ~~**private**~~ **requests** made through **private processes**?
5. Does the company provide clear guidance or examples of implementation of its process of responding to ~~**private**~~ **requests** made through **private processes**?

Rationale for revisions: These proposed revisions move five elements focused on "private requests" from F5a into this new indicator (F5b), in order to ensure that F5b is focused

exclusively on requests to remove content or accounts that come through private processes. Revisions also reflect a clarification of our definition of "private requests," which we define as requests that come through private processes, such as the U.S. Digital Millennium Copyright Act, the European Right to be Forgotten ruling. Requests made by private parties and that come through a civil court for instance would be considered under F5a in "government requests."

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 (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 ~~requests~~ to restrict for content and ~~or~~ accounts

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

Elements:

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

2. Does the company list the number of **accounts** affected?

3. Does the company list the number of pieces of **content** or URLs affected?

4. Does the company list the types of subject matter associated with the **demands** ~~requests~~ it receives?

5. Does the company list the number of **demands** ~~requests~~ that come from different legal authorities?

6. Does the company list the number of **demands** ~~requests~~ it knowingly receives from government officials to restrict **content** or **accounts** through **unofficial processes**?

7. Does the company list the number of **demands** ~~requests~~ with which it complied?

8. Does the company publish the original **demands** ~~requests~~ or disclose that it provides copies to a **public third-party archive**?

9. Does the company report this data at least once a year?

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

Rationale for revisions: This revision changes the wording of "government requests" to "government demands" which more accurately reflects the nature of these types of orders.

Indicator guidance: Companies frequently receive demands from governments to remove, filter, or restrict content or accounts. We expect a company to regularly publish data about the number and type of government 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 ~~private~~ 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** ~~it receives by country~~?
2. Does the company list the number of **accounts** affected?
3. Does the company list the number of pieces of **content** or URLs affected?
4. Does the company list the reasons for removal associated with the requests it receives?
5. Does the company **clearly disclose** the **private processes** that ~~describe the types of parties from which~~ made ~~it receives~~ the request~~s~~?
6. Does the company list the number of requests it complied with?
7. Does the company publish the original requests or disclose that it provides copies to a **public third-party archive**?
8. Does the company report this data at least once a year?
9. Can the data be exported as a **structured data** file?
10. Does the company **clearly disclose** that its reporting covers all types of ~~private~~ requests that it receives through **private processes**?

Rationale for revisions: Revisions (in red) incorporate RDR's clarified definition of "private requests," which we define as requests that come through private processes, such as the U.S. Digital Millennium Copyright Act or the European Right to be Forgotten ruling. Requests made by "private parties" and that come through a civil court for instance are not considered in this indicator. These would be considered as government requests, and evaluated in F5a and F6 respectively.

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 ~~that it does~~ not **prioritize**, block, or delay certain types of traffic, **applications**, **protocols**, or **content** for reasons beyond assuring quality of service and reliability of the network?

2. 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?

~~2.~~ 3. If the company does engage in network **prioritization** ~~these~~ practices for reasons beyond assuring quality of service and reliability of the network, does it **clearly disclose** its purpose for doing so?

Rationale for revisions: The revision in Element 1 clarifies the evaluation standards for this element. In this element, we are looking for telecommunications companies to publicly commit to upholding net neutrality principles. In evaluating this element, we have traditionally looked for a company to disclose a clear commitment to not prioritize traffic (other than for legitimate network management reasons). We have also considered whether a company offered programs—such as through zero-rating programs—which directly conflict with or otherwise undermine a company's net neutrality commitments in practice. This proposed revision breaks out Element 2, which specifically asks about whether a company engages in zero-rating programs, as a way of better surfacing this information, which RDR was already collecting. In addition, we clarified the evaluation standard for Element 3, which is aimed at capturing whether companies prioritize network traffic for any other reason, such as when complying with a government order. This revision should ensure that Element 3 is not rewarding companies for prioritization practices, like zero rating, that can undermine users' right to information.

Note that this indicator applies only to telecommunications companies. We considered expanding this indicator to platform companies, which also offer zero-rating programs (such as Facebook's Free Basics). However, we have opted to address this issue in the Governance category, and in draft Indicator G4e, which asks if companies that offer zero rating programs are conducting robust human rights due diligence on these programs. We are prioritizing feedback on our approach to zero rating both in this indicator and in draft Indicator G4e.

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. Note that this indicator does not address blocking of content; that is addressed in indicator F3. This indicator does, however, include company disclosure related to blocking of services, apps, or devices, which are considered a type of prioritization.

Potential sources:

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

F10. Network shutdown (telecommunications companies)

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

Elements:

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

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

3. Does the company **clearly disclose** ~~explain~~ n its process for responding to **government demands** ~~requests~~ 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** ~~requests~~ to **shut down a network or restrict access to a service**?

5. Does the company **clearly disclose** that it notifies users directly when it **shuts down a network or restricts access to a service**?

6. Does the company **clearly disclose** ~~list~~ the number of **network shutdown demands** ~~requests~~ it receives?

7. Does the company **clearly disclose** ~~clearly identify~~ the specific legal authority that makes the **demands** ~~requests~~?

8. Does the company **clearly disclose** ~~list~~ the number of **government demands** ~~requests~~ with which it complied?

Rationale for revisions: The revisions (in red) bring the element language into alignment with "clear disclosure" language used throughout this methodology. We also revised the wording of "requests" to "government demands" which more accurately reflects the nature of these orders.

Indicator guidance: Network shutdowns are a growing threat to human rights. The UN Human Rights Council has condemned network shutdowns as a violation of international human rights law and called on governments to refrain from taking these actions.[59] Yet governments are increasingly ordering telecommunications companies to shut down their networks,[60] 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?

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

[59] "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.
[60] "#KeepItOn", *Access Now,* https://www.accessnow.org/keepiton/, last accessed April 2, 2020.

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** ~~automated~~ are used to automatically **curate, recommend, and/or rank content** ~~systems is *on* or *off*~~ by default?

5. Does the company **clearly disclose** that users can opt in to automated **content curation, recommendation, and/or ranking system**?

Rationale for adding draft Indicator F12: Draft Indicator F12 was introduced in October

2019 and then pilot tested by RDR as part of our ongoing methodology development work.[61] Based on the pilot test, we are opting to include this indicator in this draft of the 2020 RDR Index methodology, with some revisions, summarized below.

Rationale for revisions: Based on our pilot research on this indicator, we revised Element 4 to more clearly reflect that we are looking for companies to state whether users' content is automatically curated by algorithmic systems. We also made editorial revisions to bring elements into alignment with the "clear disclosure" language used across this methodology.

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 content curation, recommendation, and ranking systems (Element 1); how they work (Element 2); and what options users have to control how their information is used by these systems (Element 3). Companies should further disclose whether such systems are automatically on by default (Element 4). They should also clearly disclose whether users can "opt-in" to have their content automatically curated by the algorithmic system (Element 5).

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~~, and engage in transparency reporting around the enforcement of such policies.~~

Elements:

[61] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

1. ~~Does the company **clearly disclose** a definition of a "bot"?~~

2. Does the company **clearly disclose** rules ~~guidelines~~ governing the use of **bots** on its platform? ~~to generate **content**, disseminate **content**, or perform other actions?~~

3. 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**?

4. Does the company **clearly disclose** ~~how~~ its process for enforcing its **bot policy**?

5. Does the company **clearly disclose** data on ~~about~~ the volume and nature of user **content** and **accounts** **restricted** for violating the company's **bot policy**?

6. ~~Does the company **clearly disclose** data about the volume and nature of **advertising content** and **accounts restricted** for violating the company's **bot policy**?~~

7. ~~Does the company clearly disclose that it removes **bots** from **engagement metrics** shown to users, such as sums of accounts that have taken a particular action?~~

8. ~~Does the company regularly publish data about the total number of **bots** on the platform?~~

Rationale for adding F13: Draft Indicator F13 was introduced in October 2019 and then pilot-tested by RDR as part of our ongoing methodology development work.[62] Based on the pilot test, we are opting to include this indicator in this draft of the 2020 RDR Index methodology, with some revisions, summarized below.

Rationale for revisions: Pilot testing showed that Elements 1, 6, 7 and 8 are not useful disclosure standards for companies' bot policies. The proposed revisions are aimed at ensuring this indicator is a more of a baseline that enables RDR to capture information about what companies are disclosing about their bot policies without being overly prescriptive or granular.

Indicator guidance: This indicator is applicable to digital platforms. Many of the services evaluated by RDR (notably social media platforms) 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.[63] 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),

[62] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.
[63] *Thinkpiece Bot*, Twitter, https://twitter.com/thinkpiecebot, last accessed April 2, 2020.

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.[64]

Companies 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 and publish 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

~~F14. Informing and educating users about risks~~

~~The company should publish information to help users understand how **targeted advertising** and the use of **algorithms**, machine learning and automated decision-making influence their experience using the company's products and services.~~

~~*Elements:*~~

1. ~~Does the company publish practical materials that educate users on how to protect themselves from **advertisers'** attempts to mislead them?~~

2. ~~Does the company publish practical materials that educate users on how to protect themselves from any potential undue psychological influence of the company's use of **algorithms**, machine learning and automated decision-making?~~

Rationale for deleting draft indicator F14: Draft Indicator F14 was introduced in October 2019 and then pilot-tested by RDR as part of our ongoing methodology development work.[65] Based on the pilot testing of this draft indicator, RDR has opted to eliminate this indicator. Pilot research showed that this indicator would need to be significantly revised in order to integrate it into the draft 2020 RDR Index methodology. Given the extensive revisions and additions across other indicators, we are opting to delete this indicator from the draft methodology.

[64] 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.
[65] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

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,[66] the International Covenant on Civil and Political Rights,[67] 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) ~~most commonly~~ spoken by ~~the company's~~ 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**?

Rationale for revisions: Indicator P1(a) is the same as Indicator P1 from the existing RDR Index methodology.[68] Revisions made to Element 2 clarify RDR's evaluation standards for this element. Element 2 evaluates if companies publish policies in the primary languages of their home market. RDR does not evaluate if a company offers policies in the primary

[66] "Universal Declaration of Human Rights," *United Nations*, https://www.un.org/en/universal-declaration-human-rights/, last accessed April 2, 2020.
[67] "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.
[68] "2019 Indicators: P1. Access to privacy policies," *Ranking Digital Rights*, https://rankingdigitalrights.org/2019-indicators/#P1

languages of every market in which it operates. The proposed revision clarifies the scope of our evaluation. No score changes would occur as a result of this revision.

Rationale for adding P1(a) Element 5: Similar to mobile ecosystem apps, companies that operate personal digital assistant ecosystems (such as Amazon's Alexa and Alibaba's AliGenie) should require third-party **skills** 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 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 to ensure that the policies are easy to understand. If the company offers multiple products and services, it should be clear to what products and services the policies apply.

A document that is "easy to find" should be easily accessible from the company's homepage or service website. A policy that is easy to find is 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 documents. This may include, but is not limited to, providing summaries, tips, or guidance that explain what the terms mean, using section headers, readable font size, or other 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) ~~most commonly~~ spoken by ~~the company's~~ users in the company's home jurisdiction?

3. Are the **algorithmic system development policies** presented in an **understandable manner**?

Rationale for adding P1b: Draft indicator P1b was introduced in October 2019[69] and then pilot tested by RDR as part of our ongoing methodology development work.[70] Based on our pilot test, RDR has opted to include this indicator in this draft of the 2020 RDR Index methodology, with some revisions summarized below. While all companies we piloted deploy algorithms in various ways in their products and services, none disclosed a discrete policy governing how they develop and train these systems.[71] We decided to retain this indicator in this draft 2020 RDR Index methodology to encourage companies to disclose clear policies describing how they develop algorithmic systems.

Rationale for revisions: Revisions (in red) made to Element 2 clarify RDR's evaluation standards for this element. Element 2 evaluates if companies publish policies in the primary languages of its home market. RDR does not evaluate if a company offers policies in the primary languages of every market in which it operates. The proposed revision clarifies the scope of our evaluation. No score changes would occur as a result of this revision.

Indicator guidance: The development and testing of algorithmic decision-making systems can pose significant risks to privacy, particularly when companies use user information to develop, train, and test these systems without the data subject's informed consent.[72] Companies should clearly disclose policies related to the development and testing of algorithmic systems that users can access, read and understand, in order to make an informed decision 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** ~~provides~~ **~~notice~~** ~~and~~ **~~documentation~~** ~~to~~ users when it changes its **privacy policies**, prior to these changes coming into effect.

---

[69] "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.

[70] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

[71] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

[72] 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.

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 ~~provides~~ **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**?

Rationale for revisions: This indicator is the same as Indicator P1 from the existing RDR Index methodology.[73] Proposed revisions (in red) clarify our evaluation standards on this indicator. In this indicator, RDR expects companies to commit to notifying users of changes to privacy policies in a manner that the user will be sure to see and access. We therefore expect companies to *directly notify* users of changes on the platform or service. The proposed revisions bring the indicator language into alignment with the standards RDR already applies in evaluating companies on this indicator.

Rationale for adding P2(a) Element 6: Similar to mobile ecosystem apps, companies that operate personal digital assistant ecosystems (such as Amazon's Alexa and Alibaba's AliGenie) should require third-party skills 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

[73] "2019 Indicators: F1. Access to terms of service," *Ranking Digital Rights*, https://rankingdigitalrights.org/2019-indicators/#F1

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** ~~provides~~ ~~**notice**~~ ~~and~~ ~~**documentation**~~ ~~to~~ **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 ~~provides~~ **directly notifies** **users** of changes prior to these changes coming into effect?

4. Does the company maintain a **public archive** or **change log**?

Rationale for adding P2b: Draft indicator P1b was introduced in October 2019[74] and then pilot-tested by RDR as part of our ongoing methodology development work.[75] Based on our pilot test, RDR has opted to include this indicator in this draft of the 2020 RDR Index methodology with some revisions, summarized below. While all companies we piloted deploy algorithms in various ways in their products and services, none disclosed a discrete policy governing how they develop and train these systems.[76] We decided to retain this indicator in this draft 2020 RDR Index methodology to encourage companies to disclose clear policies describing how they develop algorithmic systems.

Rationale for revisions: Proposed revisions clarify the basis of evaluation for this indicator. In this indicator, RDR expects companies to commit to notifying users of changes to their algorithmic system development policies in a manner that the user will be sure to see and access. We therefore expect companies to *directly notify* users of changes on the platform or service. The proposed revisions bring the indicator language into alignment with the standards RDR already applies in evaluating companies on this indicator.

---

[74] "Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems," Ranking Digital Rights, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-Targeted-advertising-algorithms.pdf

[75] "2020 Pilot Study and Lessons Learned," Ranking Digital Rights, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf

[76] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

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 *Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems* (2019).[77]

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**

[77] "Addressing the impacts of Algorithms on Human Rights: Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems," *Council of Europe*, Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (2019), https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eecf.

collection of **user information** to what is directly relevant and necessary to accomplish the purpose of the skill?

Rationale for adding draft Elements 6 and 7: This indicator is the same as Indicator P3 from the existing RDR Index methodology,[78] but with the addition of two new draft elements that expand our evaluation to include personal digital assistant ecosystems.

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. (*Note that Element 3 seeks disclosure for a company commitment to data minimization and not purpose limitation, which is addressed in P5.*) 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?

[78] "2019 Indicators: P3. Collection of user information," *Ranking Digital Rights*, https://rankingdigitalrights.org/2019-indicators/#P3

Rationale for adding P3b: Draft indicator P3b was introduced in October 2019[79] and then pilot-tested by RDR as part of our ongoing methodology development work.[80] Based on our pilot test, RDR has opted to include this indicator in this draft of the 2020 RDR Index methodology.

Indicator guidance: In addition to collecting information about users, companies also perform big data analytics to infer additional data points on the basis of the collected information. This inferred information is then used for a variety of purposes, much in the same way as collected information. In addition to disclosing the information that they collect, disclosing the purpose for which they collect it, and committing to only collect information that is relevant and necessary to provide their service, companies should also 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. Even in such cases, the company should ask the users for that information directly rather than inferring it.

Potential sources:

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

P4. Sharing of user information

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

Elements:

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

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

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

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

[79] "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.
[80] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

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**?

Rationale for adding draft elements 7 and 8: This indicator has been expanded to include two new elements that are applicable to personal digital assistant ecosystems. Companies that operate personal digital assistant ecosystems should require third-party skills that they make available on their skill store to clearly disclose what types of user information they share (Element 7) and with whom they share it (Element 8).

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**?

~~2~~ 3. Does the company **clearly disclose** whether it combines **user information** from various company services and if so, why?

~~3~~ 4. For each type of **user information** the company **shares**, does the company **clearly disclose** its purpose for **sharing**?

~~4~~ 5. Does the company **clearly disclose** that it limits its use of **user information** to the purpose for which it was **collected** or **inferred**?

Rationale for revisions: Revisions to indicator language (in red) were made to incorporate data inference policies. Specifically, we expanded the scope of language of Element 5 to specify that the purpose limitation principle applies to both collected and inferred user information. We also added one new draft element, further explained below.

Rationale for adding draft Element 2: Draft Element 2 was introduced to this indicator in October 2019[81] and then pilot-tested by RDR as part of our ongoing methodology development work.[82] Based on our pilot test, RDR has opted to retain this element in this draft of the 2020 RDR Index methodology. Element 2 asks companies to disclose the purpose for inferring the user information that the company collects.

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. Finally, companies should publicly commit to the principle of use limitation**,** which is part of the OECD privacy guidelines, among 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**.

[81] "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.
[82] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

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**?

Rationale for adding draft Elements 8 and 9: Draft Element 8 and Element 9 have been added because companies that operate personal digital assistant ecosystems should require third-party skills made available through their skill stores to provide privacy policies that clearly explain how long they retain the user information they collect, and whether they delete that information after a user terminates their account. These draft elements mirror the standards required for companies operating mobile ecosystems, outlined in Element 6 and 7.

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**?

~~3.~~ 5. Does the company **clearly disclose** that it provides **users** with **options to control** how their **user information** is used for **targeted advertising**?

~~4. Does the company clearly disclose whether targeted advertising is on or *off* by default?~~

6. Does the company **clearly disclose** that **users** can *opt in* to being ~~shown~~ served with **targeted advertising**?

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?

~~5.~~ 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?

Rationale for revisions: Revisions (in red) expand this indicator to include company disclosure of options they give users to control what data is used to make inferences about them. We deleted Element 6, which asks about whether companies clearly disclose if targeted advertising is on or off by default. This element was revised from the 2019 RDR Index methodology,[83] and then pilot-tested.[84] That pilot test revealed that Element 6, as structured, produces unclear data points that do not align with the standards RDR is attempting to encourage. Ideally, companies should provide users with the ability to *opt in* to receive targeted advertising (meaning that that users are not automatically served targeted ads by default). Therefore, we deleted this element and revised draft Element 7 to capture the opt-in standard.

We also expanded the scope of Element 10 to include personal digital assistant ecosystems because these ecosystems have features allowing users to perform tasks based on their location. Therefore, we expect companies that offer personal digital assistant ecosystems (such as Amazon's Alexa, Alibaba's AliGenie) to disclose that users can control how the personal digital assistant ecosystem collects their location information.

Rationale for adding draft Elements 3, 4, 7, 8, 9: These elements were introduced in October 2019[85] and then pilot-tested by RDR as part of our ongoing methodology development work.[86] Based on our pilot test, RDR has opted to include these elements in this draft of the 2020 RDR Index methodology. These elements assess transparency by companies about options users have to control what information the company may infer about them (Element 3) and to delete such inferred information (Element 4). Element 7 assesses whether the company enables users to opt in to receiving targeted advertising.

---

[83] "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, see also Indicator P7, Element 4: https://rankingdigitalrights.org/2019-indicators/#P7.
[84] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.
[85] "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.
[86] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

Elements 8 and 9 pertain to the practice of using user information (both collected and inferred) for the development of algorithmic systems. Companies often use the information that they collect and infer about users to develop, optimize, and train algorithmic systems (including ad targeting systems). Element 8 calls on companies to provide users with options to control how their user information is used for the development of algorithmic systems, and we expect companies not to use user information for tool development without opt-in consent (Element 9). In general, user information should not be used to develop, optimize, or train algorithmic systems without the free and informed consent of the data subject. However, in some cases, such as when the user information is needed to train an algorithmic system that is indispensable for the protection of human rights, the service may require the user to consent to such processing as a precondition for use of the service.

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 obtain all the information that a company has **inferred** about them?

~~5~~ 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 that **users** can obtain all of the **user information** about them the app holds?

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** state that all **user information** is deleted when users terminate their accounts or delete the **skill**?

Rationale for adding draft Elements 5 and 7: Draft Element 5 was introduced in October 2019[87] and then pilot-tested.[88] Based on our pilot test, RDR has opted to include Element 5 in this draft of the 2020 RDR Index methodology. Although no company disclosed any options for users to obtain a copy of the information it inferred about them (P8, Element 5),[89] we opted to retain this element because we expect companies to clearly disclose this information. Draft Element 7 has been added to expand our evaluation to include personal digital assistant (PDA) ecosystems. This element evaluates whether companies that operate PDA ecosystems disclose that they evaluate whether the privacy policies of third-party skills made available through their skill stores disclose that users can obtain all of the user information the skill holds about them.

Indicator guidance: Users should be able to obtain all information that companies hold about them, including the information that a company has inferred about them**.** We expect companies to clearly disclose what options users have to obtain this information, what data this record contains, and what formats users can obtain it in. For mobile ecosystems, we

[87] "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, see also Indicator P7, Element 4: https://rankingdigitalrights.org/2019-indicators/#P7.
[88] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.
[89] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

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 ~~(internet and mobile ecosystem companies)~~

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

Rationale for revisions to Elements 1 to 5: This revision clarifies the expanded scope of these elements to include "digital platforms," which RDR defines as internet and mobile ecosystem companies as well as companies that operate e-commerce services and personal digital assistant ecosystems. Previously, Indicator P9 applied to internet and mobile ecosystems only.

Rationale for adding draft Elements 6 to 9: These draft elements were introduced in October 2019[90] and then pilot-tested by RDR as part of our ongoing methodology development work.[91] Based on our pilot test, RDR has opted to include these elements in this draft of the 2020 RDR Index methodology. Elements 1 to 5 of Indicator P9 of the RDR Index evaluate whether companies disclose if they track users across the internet through technical means, such as by using cookies, plug-ins, and widgets. However, companies can also acquire user information through non-technical means, including as part of a contractual agreement, and 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. These elements should apply to both digital platforms and telecommunications companies.

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. Company disclosure of these practices helps users understand if and how their activities are being tracked by companies even when they are not on a host company's website 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 ~~third-party~~ demands ~~requests~~ for user information

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

Elements:

[90] "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.
[91] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

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

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

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

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

~~5.~~ 4. Do the company's explanations **clearly disclose** the legal basis under which it may comply with **government demands ~~requests~~**?

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

~~7.~~ 5. Does the company **clearly disclose** that it carries out due diligence on **government demands ~~requests~~** before deciding how to respond?

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

~~9.~~ 6. Does the company commit to push back on inappropriate or overbroad **government demands ~~requests~~**?

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

~~11.~~ 7. Does the company provide clear guidance or examples of implementation of its process for **government demands ~~requests~~**?

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

Rationale for revisions: These proposed revisions are structural only. We have moved five elements focused on "private requests" into a separate indicator (10b), in order to ensure that Indicator 10a is focused exclusively on government demands. We also revised the wording of "government requests" to "government demands" which more accurately reflects the nature of these orders. These revisions will not generate any changes to company scores.

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

Rationale for revisions: Indicator P10b collects five elements focused on "private requests" that were previously located in a larger indicator that also included government demands. These revisions, which break out indicators on government demands and private requests into separate indicators, will not generate any changes to company scores. Revisions (in red) also clarify RDR's definition of "private requests," which we define as requests that come through private processes.

Indicator guidance: Companies increasingly receive requests to turn over user information. These requests can come through private processes (i.e. non-governmental and non-judicial processes). We expect companies to publicly disclose their process for responding to

requests that come through private processes, along with the basis for complying with these requests. Companies should also publicly commit to pushing back on inappropriate or overbroad private requests.

In some cases, the law might prevent a company from disclosing information referenced in this indicator's elements. Researchers will document situations where this is the case, but a company will still lose points if it fails to meet 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 blog posts

P11. Data about demands for user information

P11(a). Data about government demands ~~third-party requests~~ for user information

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

Elements:

1. Does the company list the number of **government demands** ~~requests~~ it receives by country?

2. Does the company list the number of **government demands** ~~requests~~ it receives for stored user information and for **real-time communications access**?

3. Does the company list the number of accounts affected?

4. Does the company list whether a demand sought communications **content** or **non-content** or both?

5. Does the company identify the specific legal authority or type of legal process through which law enforcement and national security demands are made?

6. Does the company include **government demands** ~~requests~~ that come from **court orders**?

~~7. Does the company list the number of requests it receives from private parties?~~

~~8.~~ 7. Does the company list the number of **government demands** ~~requests~~ it complied with, broken down by category of demand?

~~9.~~ 8. Does the company list what types of **government demands** ~~requests~~ it is prohibited by law from disclosing?

~~10.~~ 9. Does the company report this data at least once per year?

~~11.~~10. Can the data reported by the company be exported as a **structured data** file?

Rationale for revisions: This proposed revision moves one element (Element 7) focused on "private requests" into a separate indicator (P11b), in order to ensure that P11a is focused exclusively on government demands. In addition, the term "government requests" was revised to "government demands" which more accurately reflects the nature of these orders.

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** ~~from private parties~~ 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?

Rationale for revisions: This proposed revision moves one existing element (Element 7) focused on "private requests" from P11a into a new indicator (P11b), in order to ensure that P11b is focused exclusively on requests for user information that come through private processes. Element 1 was further revised to clarify RDR's definition of "private requests," which we define as requests that come through private processes. Requests made by "private parties" and that come through a civil court, for instance, are not considered in this indicator. These would be evaluated as government requests, and addressed in Indicators F10a and F11a, respectively.

Rationale for adding draft Elements 2, 3 and 4: These draft elements call on companies to regularly publish data about requests they receive for user information that come through private processes. Draft elements mirror standards in Indicator P11a, which is focused exclusively on government demands.

Indicator guidance: Companies can receive requests from third parties to hand over user information. 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 ~~requested~~ by governments** and other **third parties**.

Elements:

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

2. Does the company **clearly disclose** that it **notifies** users when they receive ~~private parties~~ 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** ~~**request**~~ it is prohibited by law from disclosing to users?

Rationale for revisions: Element 2 was revised to clarify RDR's definition of "private requests," which we define as requests that come through private processes.

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?**

Rationale for revising Elements 4, 7, 8, 9, and 10: These elements have been expanded to include personal digital assistant (PDA) ecosystems. PDAs can run on different operating systems, depending on the device; these platforms should therefore be held accountable for addressing the security vulnerabilities of the operating systems.

Rationale for adding draft Elements 11 and 12: Draft Elements 11 and 12 address the issue of whether personal digital assistant providers are prompt in delivering updates to users' operating systems.

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

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

P15. Data breaches

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

Elements:

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

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

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

Indicator guidance: 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 ~~internet and mobile ecosystem companies~~)

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

Elements:

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

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

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

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

Rationale for revision: This revision clarifies the expanded scope of these elements to include "digital platforms," which RDR defines as internet and mobile ecosystem companies as well as companies that operate e-commerce services and personal digital assistant ecosystems. Previously, Indicator P16 applied to internet and mobile ecosystems only.[92]

Indicator guidance: Encryption is an important tool for protecting freedom of expression and privacy. The UN Special Rapporteur on freedom of expression has stated unequivocally that encryption and anonymity are essential for the exercise and protection of human rights.

[92] "2019 Indicators: P16. Encryption of user communication and private content (internet and mobile ecosystem companies)," *Ranking Digital Rights,* https://rankingdigitalrights.org/2019-indicators/#P16

[93] 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 that the company offers end-to-end encryption by default. For mobile ecosystems, we expect companies to clearly disclose that they enable full-disk encryption.

Potential sources:

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

P17. Account security (digital platforms ~~internet and mobile ecosystem companies~~)

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

Elements:

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

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

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

Rationale for revision: This revision clarifies the expanded scope of these elements to include "digital platforms," which RDR defines as internet and mobile ecosystem companies as well as companies that operate e-commerce services and personal digital assistant ecosystems. Previously, Indicator P17 applied to internet and mobile ecosystems only.[94]

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

---

[93] "Report on encryption, anonymity, and the human rights framework,'' *UN Human Rights Office of the High Commissioner,* https://www.ohchr.org/en/issues/freedomopinion/pages/callforsubmission.aspx, last accessed April 2, 2020.

[94] "2019 Indicators: Account security (internet and mobile ecosystem companies), *Ranking Digital Rights*, https://rankingdigitalrights.org/2019-indicators/#P17

- 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?

~~2. Does the company publish practical materials that educate **users** on how to protect themselves from the privacy risks associated with the company's **targeted advertising** practices?~~

~~3. Does the company publish practical materials that educate **users** on how to protect themselves from the privacy risks associated with the inclusion of their **user information** in the development and optimization of **algorithmic systems**?~~

Rationale for revisions: Elements 2 and 3 were introduced in October 2019[95] and then pilot-tested by RDR as part of our ongoing methodology development work.[96] Based on our pilot test, RDR has opted to eliminate these elements from this indicator. Pilot research showed that these elements would need to be significantly revised in order to integrate them into the 2020 RDR Index methodology. Given the extensive revisions and additions across the 2020 methodology, we are opting to delete these two elements at this stage.

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, to adjust privacy settings, tips for avoiding 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 images, designed to help users understand the nature of the risks companies and users can face. These can include tips, tutorials, how-to guides, or other resources, and should be presented in a way that users can easily understand (for instance, with visuals, graphics, bullet points, and lists).

Potential sources:
- Company security center
- Company help pages or community support page
- Company blog

[95] "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.
[96] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020. https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

P19. User access to advertising targeting metadata

The company should **clearly disclose** how **users** can access key information about the **targeted advertising** that they see.

Elements:

1. Does the company **clearly disclose** how **users** can access the list of **advertising audience categories** to which the company has assigned them?

2. Does the company **clearly disclose** how **users** can access the list of **advertising audience categories** to which each piece of **advertising content** they see while using the product or service was **targeted**?

3. Does the company **clearly disclose** how **users** can access the list of **advertisers** who have attempted to influence them through the company's on-platform **targeted advertising** technologies?

4. Does the company **clearly disclose** how **users** can access the list of **advertising audience categories** to which each piece of **advertising content** they see off-platform was **targeted** through the company's **advertising network**?

5. Does the company **clearly disclose** how **users** can access the list of **advertisers** who have attempted to influence them through the company's off-platform **advertising network**?

Rationale for adding draft Indicator P19: Draft indicator P19 was introduced in October 2019[97] and then pilot-tested by RDR as part of our ongoing methodology development work.[98] Based on our pilot test, RDR has opted to include this indicator in this draft of the 2020 RDR Index methodology. While pilot research showed that disclosure by companies in this area is low, companies nevertheless should be giving users options to access their targeted advertising metadata. We are therefore opting to retain this indicator as we continue to conduct research to help inform our final decision.

Indicator guidance: While some companies have started to enable their users to understand why they see particular advertising content, this practice is far from universal and appears to be limited to on-platform advertising only (as opposed to targeted advertising that appears on third-party websites through an advertising network). This new indicator calls on companies to clearly explain, in a manner that is accessible without creating a user account,

[97] "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.
[98] "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, March 16, 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

how users can access detailed information on all the targeted advertising that the company shows them (both on- and off-platform, as the case may be for each company).

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 (Element 1). In addition to knowing which audience categories they have been assigned to, users should be able to know which audience categories each ad they see has been targeted to, for both on-platform ads (Element 2) and off-platform ads (Element 4). Users should also be able to access a full list of all the advertisers who have attempted to influence them through on-platform targeted advertising (Element 3) and off-platform targeted advertising (Element 5).

Potential sources:

- Advertising & privacy policies
- Ad settings pages or portals
- Ads help center

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.

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 more at: "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," 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 observes 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: 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 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: 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. 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

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.

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.

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.

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

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

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

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. For more, see "Pushing for Perfect Forward Secrecy," Electronic Frontier Foundation, https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-important-web-privacy-protection.

Full-disk encryption — Comprehensive encryption of all data stored on a physical device, in 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) — HRIAs are a systematic approach to due diligence. A company carries out these assessments or reviews to see how its products, services, and business practices affect the freedom of expression and privacy of its users. For more information about Human Rights Impact Assessments and best practices in conducting them, see this special page hosted by the Business & Human Rights Resource Centre: https://business-humanrights.org/en/un-guiding-principles/implementation-tools-examples/implementation-by-companies/type-of-step-taken/human-rights-impact-assessments

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

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

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."

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.[1] In total it can be said to be the stage on which computer programs can run.

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

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

Private processes — Requests made through a private process rather than a judicial or governmental process. Private requests for content restriction can come from a self-regulatory body such as the Internet Watch Foundation, or a notice-and-takedown system, such as the U.S. Digital Millennium Copyright Act. For more information on notice-and-takedown, as well as the DMCA specifically, see the recent UNESCO report, "Fostering Freedom Online: The Role of Internet Intermediaries" at http://unesdoc.unesco.org/images/0023/002311/231162e.pdf (p. 40-52 of 211).

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

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

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

Public archive — A publicly available resource that contains previous versions of a company's policies, such as its terms of service or privacy policy, or comprehensively explains each round of changes the company makes to these policies.

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.

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, Sept. 2014 http://www.bsr.org/reports/BSR_Rights_Holder_Engagement.pdf

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

Structured data — "Data that resides in fixed fields within a record or file. Relational databases and spreadsheets are examples of structured data. Although data in XML files are not fixed in location like traditional database records, they are nevertheless structured, because the data are tagged and can be accurately identified." Conversely, unstructured data is data that "does not reside in fixed locations. The term generally refers to free-form text, which is ubiquitous. Examples are word processing documents, PDF files, e-mail messages, blogs, Web pages and social sites." Sources: PC Mag Encyclopedia: "structured data" http://www.pcmag.com/encyclopedia/term/52162/structured-data "unstructured data" http://www.pcmag.com/encyclopedia/term/53486/unstructured-data

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

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

Throttling – A blunt form of traffic shaping in which a network operator slows the flow of packets through a network. Mobile operators may throttle traffic to enforce data caps. For more information, see: Open Signal, "Data throttling: Why operators slow down your connection speed."

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.