RDR Corporate Accountability Index:

Draft Indicators

Transparency and accountability standards for targeted advertising and algorithmic decision-making systems

October 2019

Acknowledgements

The following Ranking Digital Rights (RDR) team members worked on the preparation and development of the draft indicators presented in this document:

- Nathalie Maréchal, Senior Research Analyst
- Zak Rogoff, Research Analyst
- Veszna Wessenauer, Research Analyst
- Afef Abrougui, Corporate Accountability Editor
- Amy Brouillette, Research Director
- Rebecca MacKinnon, Director
- Jessica Dheere, Deputy Director

We also wish to thank former RDR research team members Laura Reed and Andrea Hackl for their significant work and contribution to this methodology development process.

About Ranking Digital Rights

Ranking Digital Rights is a non-profit research initiative housed at the New America Foundation's Open Technology Institute. We work 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 ranking the world's most powerful internet, mobile ecosystem, 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.

For more about our vision, impact, and strategy: www.rankingdigitalrights.org/about/.

For more about the RDR Corporate Accountability Index: www.rankingdigitalrights.org.

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

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

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

Contents

Introduction

This document presents new and revised indicators for the Ranking Digital Rights (RDR) Corporate Accountability Index aimed at setting corporate transparency and accountability standards for targeted advertising and algorithmic decision-making systems. These draft indicators have been developed by the RDR research team, in consultation with more than 90 experts, as part of an open consultation process launched in February 2019.[1]

The draft indicators will be pilot tested by the RDR team starting in late October 2019 and will be further revised based on the results of this pilot and continued feedback by stakeholders. We welcome your feedback about these draft indicators at: methodology@rankingdigitalrights.org.

Methodology development background

The RDR Corporate Accountability Index provides an effective roadmap for companies to improve policies and disclosures in order to prevent and mitigate a range of threats to users' rights to privacy and to freedom of expression. Since its inaugural launch in 2015, the RDR Index has contributed to improved company disclosure of policy and practice across a number of areas, including transparency reporting, content removals, account restrictions and shutdowns, and handling and securing user information. However, given geopolitical and technological developments with clear human rights implications in the years since the RDR Index methodology was first developed, it has become clear that the methodology needs to be updated if companies are to be held fully accountable for the range of potential online threats to human rights.

In early 2019, we began a process of expanding the RDR Index methodology to include benchmarks that hold companies accountable for their targeted advertising policies and practices, and for their use and development of algorithms, machine learning and automated decision-making. Our goal is to set global accountability and transparency standards, grounded in the Universal Declaration of Human Rights (UDHR), for how major, publicly traded internet, mobile, and telecommunications companies can demonstrate respect for human rights online as they develop and deploy these new technologies. A description of the process we followed can be found on our website.

[1] "RDR seeks feedback on standards for algorithms and machine learning, adding new companies," *Ranking Digital Rights*, July 2019; "RDR Seeks Input on New Standards for Targeted Advertising and Human Rights," *Ranking Digital Rights*, February 2019.

Targeted advertising and algorithmic decision-making systems: Why we are adding new indicators

Companies that derive revenue from targeted advertising have an incentive to manage, shape, and govern the flow of content and information on their platforms in a manner that maximizes advertising revenue—and they do so with the assistance of algorithms, machine learning, and other forms of automated decision-making. We see many of today's most vexing policy issues (including the rise of extremist ideologies, hate speech, incitement to violence, disinformation, and other forms of media manipulation) as negative externalities of a business model whose cornerstone is the nonconsensual collection of personal information at a planetary scale. This corporate surveillance allows advertisers to micro-target individuals with messages tailored to their specific attributes, traits and preferences. Without clear constraints on what data can be collected and how it can be used—and without strong transparency and clear mechanisms for obtaining user consent—violations of users' rights are all but inevitable. Responsible parties include those who collect the data, those with whom it is shared, and those who take advantage of targeted advertising's potential to influence behavior. The Facebook/Cambridge Analytica data sharing scandal that erupted in 2018 demonstrated how data collected for targeted advertising purposes can be used by malicious actors to manipulate users without their knowledge, but it is only one example out of many.

In order to boost user exposure to and engagement with paid content, platforms have an incentive to design and optimize user interfaces to prioritize the most controversial and inflammatory content. The results can even be deadly, such as when hateful content is shared by one group of people seeking to encourage violence against another group, as happened in Myanmar in 2017. Furthermore, human rights violations can result from unclear rules and enforcement or poor transparency about who is allowed to advertise, to whom, and with what content. These issues can also lead to the dissemination of content that incites human rights violations, or is intended to intimidate or mislead in ways that discourage or prevent people from exercising their human rights.

Due to resource limitations, the scope of this methodology expansion is limited to ranked companies' use of such tools within their consumer-facing products and services and to their use of user information for developing algorithms and machine learning systems. We focused our research on four main types of human rights risks: algorithmic curation, recommendation and ranking systems; the use of algorithmic systems for content moderation and other content restrictions; violations of the purpose limitation principle; and algorithmic systems' vulnerability to automated manipulation efforts and tendency towards bias and discrimination (whether deliberate or not).

Human rights scope

Following a rigorous research process that involved identifying human rights risk scenarios[2] and company best practices,[3] and after consulting with a wide range of stakeholders, we concluded that addressing the human rights risks posed by targeted advertising and algorithmic decision-making systems required an expansion of the RDR Index's scope.

Until now, the RDR Index has focused on two fundamental human rights: freedom of expression (UDHR art. 19) and privacy (UDHR art. 12). RDR focuses on freedom of expression and privacy for two reasons: first, because these rights are the most directly affected by the companies ranked in the RDR Index, and second, because these fundamental rights ensure the ability to exercise many other rights. If people's expression and privacy rights are not protected and respected, they cannot use technology effectively to exercise and defend political, religious, economic, and social rights. Indeed, the human rights risk scenarios published earlier this year revealed that companies' failure to respect privacy and freedom of expression causes or contributes to the violation of other human rights, specifically: the right to life, liberty and security of person (UDHR art.3); the right to non-discrimination (UDHR art. 7, art. 23); freedom of thought (UDHR art. 18); freedom of association (UDHR art. 20); and the right to take part in the government of one's country, directly or through freely chosen representatives (UDHR art. 21). While the RDR Index cannot address the full range of human rights harms associated with the companies it ranks (for example, labor and environmental rights remain beyond the scope of the RDR Index), we identified two areas where we can and must expand our scope: freedom of information (UDHR art. 19) and freedom from discrimination (UDHR art. 7, art. 23).

Freedom of expression *and information*

Internet users' rights are affected not only when their online expression is restricted, but also when companies fail to enact and enforce rules against harmful expression, and when their use of content-shaping technologies boosts harmful expression (such as hate speech, incitement to violence, and disinformation), thus infringing on the right to freedom of information and opinion. Indeed, human rights experts and many courts therefore refer to freedom of expression *and information*, emphasizing the importance of the right to receive information as being fundamental to the ability to exercise freedom of

---

[2] See CONSULTATION DRAFT: Human Rights Risk Scenarios:Targeted Advertising and CONSULTATION DRAFT:Human rights risk scenarios: Algorithms, machine learning and automated decision-making, *Ranking Digital Rights* (2019).

[3] *"*CONSULTATION DRAFT Best Practices for Business and Human Rights: Targeted Advertising.*"* *Ranking Digital Rights*, Feb 2019*; "CONSULTATION DRAFT Best practices for business and human rights: Algorithms, machine learning, and automated decision-making," Ranking Digital Rights,* July 2019.

expression rights. In this area of our methodology work, we found it necessary to expand the scope of our Freedom of Expression category to include "Freedom of Expression and Information."

Freedom from discrimination

Targeted advertising business models and algorithmic decision-making systems are two closely related phenomena that carry high risks of discrimination harms. In addition to posing critical risks to privacy and freedom of expression and information, these technologies also can threaten the right to non-discrimination. In both cases, "big data" analytics and automation are used to personalize users' experiences on the basis of collected and inferred user information. This constitutes discrimination in the most basic sense of the definition: "the practice of treating particular people, companies, or products differently from others, especially in an unfair way."[4] Such distinctions need not be illegal or individually harmful to result in harmful effects at scale, such as at the population level or over the course of an individual's lifetime. Personalization is discrimination, with the potential to do great harm to individuals and to entire communities and countries.

These discrimination harms are enabled by the massive, nonconsensual, and opaque data collection efforts undertaken by companies in service of targeted advertising business models, and enacted through algorithmic decision-making systems whose design tends to replicate and reinforce existing patterns of structural oppression. These "upstream" privacy violations, which are incentivized by the targeted advertising business model, thus enable discrimination harms, which in turn contribute to "downstream" expression and information harms such as deliberate media manipulation, viral hate speech and incitement to violence, and the erosion of the public sphere that is the cornerstone of deliberative democracies.

Because discrimination harms are tightly interwoven with freedom of expression and information and privacy harms, we opted to integrate indicators and elements that assess companies' respect for freedom from discrimination within the RDR Index's existing categories (Governance, Freedom of Expression and Information, and Privacy) rather than creating a new category focused on discrimination.

Stakeholder engagement process

Feedback and input from stakeholders is essential to developing a credible, rigorous, and effective methodology—and this feedback has been integral to our methodology work since RDR's inception in 2013. The new and revised indicators presented in this document are a result of extensive in-person and remote consultations with a broad range of civil society, academic, industry, and policy experts since early 2019. This process began with the release of consultation documents for targeted advertising and algorithmic decision-making issue areas. These documents outlined key human rights risks scenarios and proposed best

[4] Discrimination (n.d.). In Cambridge Business English dictionary. Accessed October 16, 2019. Received from https://dictionary.cambridge.org/dictionary/english/discrimination.

practices to mitigate the identified risks.[5] These best practices helped form the basis of the draft indicators presented in this document.

How to read this document

The new and revised indicators presented in this document have been integrated into the existing RDR Index methodology to the extent possible. Indicators to which we made no changes are not presented in this document.

A key structural change is the introduction of "families" of indicators: groups of indicators that apply to similar issue areas. For example, Indicator G4 (see below) has been expanded into four indicators addressing different aspects of a company's human rights due diligence policies and practices. We have also developed similar indicator "families" in the Freedom of Expression and Information and Privacy categories.

Revisions to the existing methodology are presented in red; new indicators and elements are presented in blue.

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

1. Governance

The Governance category of the RDR Index evaluates if companies have strong governance and oversight over privacy and freedom of expression and information issues. It includes six indicators evaluating disclosure of commitments to freedom of expression and privacy principles along with measures taken to implement those commitments across a company's global operations.

The draft indicators presented below includes: the addition of one new element to Indicator G1; a group of revised and new risk assessment indicators, building off of the existing Indicator G4 and addressing due diligence best practices for companies' use of targeted advertising and algorithmic decision-making systems; and a new indicator aimed at defining standards for appeals of content moderation decisions (G6(b)).

A description of changes or additions is further elaborated below. Note that we have made no proposed revisions to Indicators G2, G3, or G5 at this stage.

[5] See: Human Rights Risk Scenarios:Targeted Advertising and Human rights risk scenarios: Algorithms, machine learning and automated decision-making, *Ranking Digital Rights* (2019).

G1. Policy Commitments

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

Element:

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

2. Does the company make an **explicit**, clearly articulated **policy commitment** to human rights, including privacy?

3. Does the company disclose an **explicit**, clearly articulated **policy document** outlining their human rights commitments governing the development and use of **algorithmic decision-making systems**?

Rationale: Algorithmic decision-making systems can pose complex and rapidly-evolving threats to human rights.[6] New Element 3 asks companies to publish a formal policy articulating their human rights commitments governing the development and use of these systems. According to best practices put forth in the Council of Europe's *Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems* (2019), companies' development and use of these systems should be governed by a comprehensive, detailed policy framework, explicitly grounded in international human rights norms.

Revisions made to Element 1 and 2 clarify the basis of our evaluation by breaking out freedom of expression and privacy into separate elements. This change would have no impact on companies' scores, while clarifying our data.

1.1 Human rights due diligence

The RDR Index evaluates whether companies conduct human rights due diligence in order to identify and mitigate human rights harms posed by their business, products, or services (Indicator G4). The draft indicators below restructure and expand Indicator G4 into a broader family of indicators that address additional areas and issues: G4(a) focuses on due diligence practices pertaining to governments and regulations; G4(b) focuses on risk assessments of the company's own policy enforcement; G4(c) and G4(d) evaluate company due diligence of targeted advertising and algorithmic decision-making systems, respectively.

[6] Human rights risk scenarios: Algorithms, machine learning and automated decision-making, *Ranking Digital Rights* (2019).

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

Rationale: This indicator has been revised to focus on human rights due diligence practices related to government regulations and policies. It removes three elements, which were evaluated as part of this indicator in the 2019 RDR Index, related to terms of service enforcement, targeted advertising, and the use of algorithms, which are now presented

separately in new indicators below. Additional revisions (in red) were introduced in order to clarify the basis of our evaluation.

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 disclose that it assesses freedom of expression and information risks associated with its processes for enforcing its terms of service?

2. Does the company assess how effectively it enforces 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 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: 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.

G4(c) Impact assessment: Targeted advertising

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

Elements:

1. Does the company 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: Targeted advertising can have adverse affects on human rights, specifically freedom of information, freedom of opinion, and freedom from discrimination. 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.

G4(d). Impact assessment: Algorithmic decision-making 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 decision-making 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 decision-making systems**?

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

3. Does the company disclose that it assesses discrimination risks associated with its development and use of **algorithmic decision-making 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: There are a variety of ways in which algorithmic decision-making systems may harm human rights. 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, as discussed in the introduction. 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 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).

1.2. Appeals

The RDR Index methodology evaluates whether companies offer clear and accessible mechanisms for users to seek remedy when they feel their freedom of expression or privacy has been violated as a result of company actions (Indicator G6). This indicator, however, does not capture the developing expert consensus and standards for appeals for companies that perform content moderation, as outlined in the *The Santa Clara Principles on Transparency and Accountability in Content Moderation (2018)*. To address this gap, we developed a new draft indicator, G6(b), which aims to set standards for services that moderate user-generated content, evaluating their specialized mechanisms for users to appeal content moderation decisions.

G6(b). Process for content moderation appeals

Companies that host user-generated **content** and take any actions to moderate content on their platforms should offer users a robust mechanism to appeal **content moderation actions**.

Elements:

1. Does the company disclose a policy that outlines its processes for offering and processing appeals of **content moderation actions**?
2. Does the company **clearly disclose** that, when it takes a **content moderation action**, it immediately offers the affected user a chance to appeal the action?
3. Does the company **clearly disclose** that such appeals are reviewed by at least one human not involved in the original **content moderation action**?
4. Does the company **clearly disclose** that its appeals process gives the affected **user** an opportunity to present additional information that will be considered in the review?
5. Does the company **clearly disclose** that, upon conclusion of an appeal, it provides the affected user a statement of the reasoning behind its decision?
6. Does the company **clearly disclose** the timeframe within which it seeks to review appeals?
7. Does the company **clearly disclose** whether there are any conditions under which its mechanism for appealing **content moderation actions** is not available?

Rationale: 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 human rights, companies should provide a robust appeals system. They should clearly disclose their process for appealing content moderation actions, including enabling affected users to immediately 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 when appeals are not possible.

2. Freedom of expression and information

The draft and revised indicators presented below expand several indicators in the Freedom of Expression and Information category in order to address how transparent companies are about the rules that govern information ecosystems more broady, as well as the processes for enforcing these rules. In addition to our existing indicators (F1, F2, F3, F4) that ask companies to clearly disclose terms of service policies governing speech and activities and how those rules are enforced, we have developed new indicators that ask companies to disclose their advertising content policies, advertising targeting policies, and algorithmic system use policies, respectively.

In addition, we developed three new indicators evaluating company transparency about algorithmic content curation, recommendation and ranking systems (F12); company policies governing the use of automated software agents ("bots") on their platforms, and the enforcement of such policies (F13); and company efforts to advance media literacy by educating users on how to protect themselves from advertisers' attempts to mislead them and from risks associated with the use of algorithms, machine learning and automated decision-making (F14).

A description of changes or additions is further elaborated below. Note that we made no proposed revisions to the current RDR Index Indicators F5, F6, F7, F8, F9, F10, F11 at this stage.

Revisions to the existing methodology are presented in red; new indicators and elements are presented in blue. A glossary of terms is also appended below. The terms defined in the Glossary are **bolded i**n the indicator text.

2.1 Access to key policy documents affecting freedom of expression and information

The RDR Index evaluates whether companies make their terms of service easy to find and easy to understand (Indicator F1). The draft indicators presented here call for companies to disclose policies specifying rules governing advertising content, advertising targeting, and the use of algorithmic decision-making systems, respectively. Taken as a whole, this family of F1 indicators evaluates transparency by companies about key rules impacting freedom of expression and information.

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 language(s) most commonly spoken by the company's users?

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

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 language(s) most commonly spoken by the company's users?

3. Are the company's **advertising content policies** presented in an **understandable manner**?

4. (For **mobile ecosystems**): Does the company 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**?

Rationale: This draft indicator evaluates how transparent companies are about the rules governing what advertising content is prohibited. These rules should be easy to find and easy to understand, and available in the main languages of the company's home market.

For mobile ecosystems, many third-party apps that can be downloaded through an app store (such as the Apple App Store, Google Play Store, Samsung Galaxy Store, etc) serve users with targeted advertising. Very few apps maintain their own targeted advertising infrastructure and associated policies, with most relying instead on a third-party advertising network. Mobile ecosystems should enable users to choose which apps to download on the basis of their participation (or not) in advertising networks, and to register their privacy preferences with the advertising networks used by apps. Therefore, Element 4 asks whether the company discloses that it requires apps made available through its app store to provide users with the link to a content policy for advertising, which we expect would belong to the advertising network(s) the app participates in.

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 language(s) most commonly spoken by the company's **users**?

3. Are the **advertising targeting policies** presented in an **understandable manner**?

4. (For **mobile ecosystems**): Does the company 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**?

Rationale: Targeted advertising can have adverse affects on human rights, specifically the rights to freedom of information, freedom of opinion, and freedom from discrimination.[7] Companies that do engage in targeted advertising—or that rely on advertising-based business models—should take clear steps to ensure that they respect and protect human rights. This includes disclosing and implementing rules that protect users and their communities from the most serious harms associated with targeted advertising. Companies should clearly disclose to users how they are being targeted and what targeting parameters are available to advertisers. Users should be able to access, read and understand these rules in order to make an informed decision about whether to use a company's products and services. For mobile ecosystems (Element 4), companies should disclose that they require apps made available through their app stores to provide users with the link to an advertising targeting policy.

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**?

---

[7] 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. *Vice Motherboard,* November 16 2018. "CONSULTATION DRAFT Human Rights Risk Scenarios: Algorithms, Machine Learning and Automated Decision-Making," *Ranking Digital Rights* (2019),

2. Are the **algorithmic system use policies** available in the language(s) most commonly spoken by the company's users?

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

Rationale: Algorithmic decision-making systems can have adverse affects on freedom of expression and information, freedom of opinion, and freedom from discrimination.[8] Companies should have clear policies outlining its practices involving the use of these systems, and ensure that these policies are easy to find, understand, and available in the main languages of the company's home market. These standards are derived from the Council of Europe's *Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems* (2019).

2.2. Notification of changes

The RDR Index evaluates whether companies notify users of changes to their terms of service (Indicator F2). The draft indicators presented below expands this standard to ask companies to commit to notify users of changes to policies governing advertising content, advertising targeting, and the use of algorithmic decision-making systems, respectively. Taken as a whole, the F2 family of indicators evaluates company transparency about changes to key rules impacting freedom of expression and information.

F2(a). Changes to terms of service

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

Elements:

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

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

3. Does the company **clearly disclose** the timeframe within which it provides **notification** prior to changes coming into effect?

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

[8] "CONSULTATION DRAFT Human Rights Risk Scenarios: Algorithms, Machine Learning and Automated Decision-Making," *Ranking Digital Rights* (2019),

F2(b). Changes to advertising content policies

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

Elements:

1. Does the company **clearly disclose** that it **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 **notification** prior to changes coming into effect?

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

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

F2(c). Changes to advertising targeting policies

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

Elements:

1. Does the company **clearly disclose** that it **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 time frame within which it provides **notification** prior to changes coming into effect?

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

5. (For **mobile ecosystems**): Does the company **clearly disclose** that it requires **apps** made available through its **app store** to **notify users** when the **apps** change their **advertising targeting policies**?

Rationale: 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 therefore

should commit to notify users when they change these terms and to provide users with information that helps them understand what these changes mean.

F2(d). Changes to algorithmic system use policies

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

Elements:

1. Does the company **clearly disclose** that it **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 **notification** prior to changes coming into effect?

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

Rationale: Companies may change their algorithm use policies. However these changes can affect users' freedom of expression and information as well as their right to non-discrimination. Companies therefore should commit to notify users when they change these policies and to provide users with information that helps them understand what these changes mean. This standard is endorsed 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).

2.3 Rules and processes for enforcement

The RDR Index evaluates whether companies clearly disclose their rules for what types of content and activities are allowed on their service or platform, and if they disclose their process for enforcing these rules (Indicator F3). The draft indicators presented below expand on our existing F3 by also asking companies to disclose the rules and processes for enforcement related to advertising content policies (F3(b)), advertising targeting policies (F3(c)), and algorithmic system use policies (F3(d)), respectively.

Note that across all three draft indicators in this family we have clarified that Element 3 includes disclosures about the technologies used to enforce company rules, as well as the processes. Companies are increasingly using algorithms, machine learning and other forms of automated decision-making to enforce their rules. The use of such tools for content moderation can pose risks to users' freedom of expression and information rights, as automation can lead to over-censoring content and to unaccountable content moderation. It is therefore particularly important for companies to be transparent about their use of such technologies.

F3(a). Terms of service and 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 and technologies it uses to identify **content** or **accounts** that violate the company's rules?

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

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

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

F3(b). Advertising content rules and enforcement

The company should **clearly disclose** its content policies governing **third parties'** use of advertising technologies on the platform.

Elements:

1. Does the company **clearly disclose** what types of **advertising content** are prohibited?

2. Does the company **clearly disclose** that all **advertising content** 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: Companies should clearly disclose policies for what types of advertising content are prohibited on a platform or service. Specifically, this new 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).

F3(c). Advertising targeting rules and enforcement

The company should **clearly disclose** its targeting policies governing **third parties'** use of **advertising technologies** on its products and services.

Elements:

1. Does the company **clearly disclose** whether users 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. 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: This draft indicator evaluates the content of the rules governing targeted advertising to assess whether they adhere to certain best practices that are central to respecting human rights. Specifically, whether companies that engage in targeted advertising prohibit advertisers from targeting specific individuals (Element 3), whether algorithmically generated advertising audience categories are evaluated by human reviewers before they can be used (Element 4), and whether companies discloses the guidelines against which these audience categories are evaluated (Element 5).

2.4 Data about policy enforcement

The RDR Index evaluates whether companies published data about the volume and nature of actions taken to restrict content and accounts that violate the company's terms of service or community standards (Indicator F4). The draft indicators presented below split this Indicator F4 in order to evaluate transparency about content restrictions and account restrictions separately (F4(a) and F4(b)), and draw on draw on standards outlined in the

Santa Clara Principles On Transparency and Accountability in Content Moderation (2018), which specify that companies should publish this data on a quarterly basis.

In addition, F4 has been expanded to evaluate data about the enforcement of policies governing the content and targeting of advertisements (F4(c) and F4(d)), respectively. Such transparency reporting is necessary for users to understand the factors that shape their information ecosystems, and to hold companies accountable for the actions companies take and the role they play in shaping these ecosystems. Companies should demonstrate fair and consistent enforcement of their advertising policies to prevent advertisers from using their platforms' advertising infrastructure to incite violence, manipulate public discourse, or engage in harmful discrimination (whether willfully or not). Taken as a whole, this family of indicators evaluates company transparency about the volume and nature of actions it takes to enforce its policies.

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

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

Elements:

1. Does the company list the total number of pieces of **content** it **restricted** to enforce its **terms of service**?
2. Does the company break down the number of pieces of **content** it **restricted** based on which rule was violated?
3. Does the company break down the number of pieces of **content** it **restricted** based on the nature of the **restriction**?
4. Does the company disclose the number of times **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 **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 **content** it **restricted** based on the format of content? (e.g. text, image, video, live video)
7. Does the company publish this data at least four times a year?
8. Can the data be accessed through a **robust programmatic interface** or exported as a **structured data file**?

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 list the total number of **accounts** it restricted to enforce its **terms of service**?
2. Does the company break down the number of **accounts** it **restricted** based on which rule was violated?
3. Does the company break down the number of **accounts** it **restricted** based on the nature of the restriction?
4. Does the company disclose the number of times **accounts** were **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 **accounts** it **restricted** in an entirely automated manner, without a **human-submitted flag** or any other direct human input?
6. Does the company publish this data at least four times a year?
7. Can the data be accessed through a robust programmatic interface or exported as a **structured data file**?

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 list the total number of pieces of **advertising content** it **restricted** to enforce its **advertising content policies**?
2. Does the company break down the number of pieces of **advertising content** it **restricted** based on which rule was violated?

3. Does the company break down the number of pieces of **advertising content** it **restricted** based on 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)

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

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

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 list the total number of pieces of **advertising content** it **restricted** to enforce its **advertising targeting policies**?

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

3. Does the company break down the number of pieces of **advertising content** it **restricted** based on 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)

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

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

2.5 Additional draft indicators (Freedom of expression and information)

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

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

Elements:

1. Does the company disclose whether it uses **algorithmic** decision-making 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 content curation, recommendation, and/or ranking** system works, including the variables that influence it?

3. Does the company 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 disclose whether automated content **curation, recommendation, and/or ranking** systems is *on* or *off* by default?

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

Rationale: 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 on or off by default (Element 4), with "opt-in" as the preferred default option (Element 5).

F13. Automated software agents ("bots")

Companies should clearly disclose policies governing the use of automated software agents (**"bots"**) on their platforms, products and services, disclose how they enforce such policies, and engage in transparency reporting around the enforcement of such policies.

Elements:

1. Does the company **clearly disclose** a definition of a "bot" ?
2. Does the company clearly disclose guidelines governing the use of **bots** 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 it enforces its **bot policy**?
5. Does the company **clearly disclose** data 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: 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. There are also more problematic uses that many companies forbid or discourage, such as when political parties or their surrogates use botnets to promote certain messages or to artificially inflate a candidate's reach in order to manipulate public discourse and outcomes. On some social media platforms, bots or coordinated networks of bots ("botnets") can be used to harass users ("brigading"), artificially amplify certain pieces of content (mass retweeting, etc), and otherwise distort public discourse on the platform. Such distortions represent a violation of freedom of information, particularly when the result of those political outcomes includes empowerment of the winning group to violate the rights of other people. 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. The requirement has also been written into California law, going into effect on July 1, 2019.

Companies therefore should be clear about what rules they have in place to prevent this type of harm. They should specify how they define a bot or bot activities. For example, there is a debate about whether human control of large numbers of coordinated accounts using a combination of automation and human labor constitutes "bots" or "sock puppets." Companies should clarify their definitions and rules so that users can understand how bots might be influencing and shaping the content they are being delivered (Elements 1 and 2). Companies should clearly disclose when an account is a bot and how they detect this (Elements 3 and 4). Finally, companies should also be transparent about how they enforce their bot policies (Elements 5, 6, 7 and 8).

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: This draft indicator calls on companies to advance media literacy by educating users on how to protect themselves from advertisers' attempts to mislead them (Element 1) and from risks associated with the use of algorithms, machine learning and automated decision-making (Element 2). These risks include the amplification of inflammatory content and filter bubbles leading to political polarization, which may jeopardize users' freedom of information and freedom to participate in their country's government. Standards established in this indicator derived from the Council of Europe's *Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems* (2019).

3. Privacy

As in the Freedom of expression and information category, we expanded several existing Privacy indicators into "families" of indicators. The indicator families *Access to key policy documents* (P1) and *Notification of changes to key policies* (P2) evaluate company transparency about their privacy policies and their algorithmic system development policies. The Indicator P3 family assesses company transparency about how it acquires information about users by evaluating the collection of user information and the inference of user information on the basis of collected information (P3(a) and P3(b), respectively).

Revisions to Indicators P5, P6, and P8 below incorporate this new focus on inferred user information and assess whether companies disclose the default setting for the display of targeted advertising and for the use of user information to develop algorithmic systems. They also set the expectation that such features—which benefit the company at the expense of user privacy—should be *off* by default (with narrow, clearly disclosed exceptions). We also expanded the scope of Indicator P9, which focuses on the widespread practice of collecting information about internet users' online behavior through technical means, to also include data that is acquired through other means, such as purchases, data-sharing agreements, and other contractual relationships with third parties.

Finally, revisions to Indicator P18 clarify that the indicator assesses whether the company publishes educational materials to help users protect themselves from cybersecurity and privacy risks, including risks that arise from the company's targeted advertising practices and from the inclusion of user information in the development and optimization of algorithmic systems.

A description of changes or additions is further elaborated below. Note that we have made no proposed revisions to Indicators P4, P6, P10, P11, P12, P13, P14, P15, P16, or P17 at this stage.

Revisions to the existing methodology are presented in red; new indicators and elements are presented in blue. A glossary of terms is also appended below. The terms defined in the Glossary are **bolded i**n the indicator text.

3.1 Access to key policy documents

The RDR Index evaluates whether companies make their privacy policies easy to access and understand (Indicator P1). The draft indicators presented below also ask companies to make their policy documents governing the use of user information to develop or train algorithmic

decision-making systems easy to access and understand. Taken as a whole, this family of P1 indicators evaluates company transparency about key rules impacting user 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 language(s) most commonly spoken by the company's **users**?
3. Are the policies presented in an **understandable manner**?
4. (For **mobile ecosystems**): Does the company disclose that it requires **apps** made available through its **app store** to provide users with a **privacy policy**?

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 language(s) most commonly spoken by the company's **users**?
3. Are the **algorithmic system development policies** presented in an **understandable manner**?

Rationale: 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.[9] 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.

[9] 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. *Vice Motherboard,* November 16 2018. "CONSULTATION DRAFT Human Rights Risk Scenarios: Algorithms, Machine Learning and Automated Decision-Making," *Ranking Digital Rights* (2019),

3.2. Notification of changes

The RDR Index expects companies to notify users of changes to their privacy policies (Indicator P2). The draft indicators presented below expand this standard to cover changes to algorithmic system development policies. Taken as a whole, this family of P2 indicators evaluates company transparency about changes to key rules affecting privacy.

P2(a). Changes to privacy policies

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

Elements:

1. Does the company **clearly disclose** that it notifies **users** about changes to its **privacy policies**?

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

3. Does the company **clearly disclose** the time frame within which it provides **notification** prior to changes coming into effect?

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

5. (For **mobile ecosystems**): Does the company **clearly disclose** that it requires apps made available through its **app store** to notify **users** when the **apps** change their **privacy policies**?

P2(b). Changes to algorithmic system development policies

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

Elements:

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

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

Rationale: 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 notify users when they change these policies and to provide 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).

3.3 Collection and inference of user information

The RDR Index evaluates whether companies clearly disclose each type of user information they collect (Indicator P3). The draft indicator below further evaluates whether companies clearly disclose what user information they infer and how (P3(b)).

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?

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?

Rationale: 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.

P5. Purpose for collecting, inferring and sharing user information

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

Elements:

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

2. For each type of **user information** the company **infers**, does the company **clearly disclose** its purpose for the **inference**?

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

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

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

Rationale: This indicator asks companies to clearly disclose the purpose for collecting and sharing user information. New Element 2 asks companies to disclose the purpose for inferring user information on the basis of collected information. We have clarified the language of Element 5 to specify that the purpose limitation principle applies to both collected and inferred user information.

P7. Users' control over their own user information

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

Elements:

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

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

3. For each type of **user information** the company **infers** on the basis of **collected information**, does the company **clearly disclose** whether **users** can control if the company can attempt to **infer** this **user information**?

4. For each type of **user information** the company **infers** on the basis of **collected information**, does the company **clearly disclose** whether **users** can delete this user information?

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

6. Does the company **clearly disclose** whether the display of **targeted advertising** is on or off by default?

7. Does the company **clearly disclose** that users can opt in to being shown **targeted advertising**?

8. 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**?

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

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

Rationale: This indicator evaluates whether companies clearly disclose options allowing users to control what information the company collects and retains, and how it is used. The revisions presented above includes new elements that further 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).

New Elements 6 and 7 assess whether the company discloses the default setting for the display of targeted advertising, and whether the default option for targeted advertising is off, respectively. Similarly, new Elements 8 and 9 for this indicator 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 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.[10]

P8. Users' access to their own user information

Companies should allow **users** to obtain all of the **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?

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**

[10] For example, users of social media platforms should not be able to opt out of having their collected user information used to develop algorithmic systems for content moderation. In the context of social media platforms, protection of human rights requires some form of content moderation. In order to operate at a global scale, and to better respect the labor rights of their human content moderators, companies need to use algorithmic tools to support and augment human moderation. Developing these tools requires using user information. This is a "conflict of rights" situation where the content moderation imperative may override users' individual privacy rights. Another example might be the use of user information to develop algorithmic systems for fraud prevention. There may be other examples as well. In any case, companies should specify what these exceptions are in order to receive credit on this element.

store disclose that users can obtain all of the **user information** about them the app holds?

Rationale: This indicator asks whether companies provide clear options for users to obtain all of the information that companies hold about them. New Element 5 asks if companies also enable users to obtain all of the information 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.

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**, including through technical means.

Elements:

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

Rationale: The RDR Index expects companies to be transparent about the collection of information about internet users' online activities outside of the companies' own websites and applications, such as through the use of tracking beacons and Super Pixels. However, this is

not the only way that companies acquire user information from third parties. The new elements presented above (Elements 1 to 4) expand the scope of this indicator to also look at user information that is acquired from a third party through non-technical means, including as part of a contractual agreement. Such contractually acquired data can become an integral part of the "digital dossier" that a company holds on its users and form the basis for inferred user information.

3.4 Additional draft indicators (Privacy)

P18. Inform and educate users about potential risks

The company should publish information to help **users** defend themselves against **cybersecurity and privacy 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: The revised P18 indicator above clarifies the language of the existing element, specifying that it addresses cyber*security* risks, and includes new elements that look at user education about the privacy risks associated with targeted advertising (Element 2) and the inclusion of user information in the development and optimization of algorithmic systems (Element 3). According to the Council of Europe's *Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems* (2019), media, digital and information literacy efforts are central to the protection and promotion of human rights, particularly in the context of algorithmic systems.

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: 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 presented below calls on companies to clearly explain, in a manner that is accessible without creating a user account, 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 (Facebook calls them "affinity groups"). 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). Full disclosure on these elements would enable users to know why they are seeing each ad that they see while using a company's services and around the internet.

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.

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.

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.

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 *(from CA SB 1001 language - however, note that we are asking each company to provide a definition of what it means by "bot")*

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).

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

Court orders — Orders issued by a court, including in both criminal and civil cases.

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

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 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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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

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.

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).

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

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

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.