RANKING DIGITAL RIGHTS

Summary of revisions to the 2017 Corporate Accountability Index research methodology

September 2016

Acknowledgements

While the entire Ranking Digital Rights team provided input and conducted consultations with stakeholders, the following team members carried out the bulk of the work in researching and implementing revisions for the new draft methodology:

- Priya Kumar, Research Analyst
- Nathalie Maréchal, Open Technology Fund Information Controls Fellow
- Revati Prasad, Annenberg COMPASS Fellow
- Laura Reed, Senior Research Analyst
- Amy Brouillette, Research and Editorial Manager

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

- John D. and Catherine T. MacArthur Foundation
- Ford Foundation
- Open Society Foundations
- Open Technology Fund Information Controls Fellowship Program
- Annenberg COMPASS Fellowship Program

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

About Ranking Digital Rights

Ranking Digital Rights (RDR) is a non-profit research initiative housed at New America's Open Technology Institute that works with an international network of partners to set global standards for how companies in the information and communications technology (ICT) sector should respect freedom of expression and privacy.

For more about RDR and its Corporate Accountability Index, please visit www.rankingdigitalrights.org.

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

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

Table of Contents

About the Corporate Accountability Index

Ranking Digital Rights produces a Corporate Accountability Index that ranks the world's largest ICT companies' public commitments to users' freedom of expression and privacy rights. The Index is a standard-setting tool aimed at encouraging companies to abide by international principles and standards safeguarding freedom of expression and privacy.

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

2017 Index methodology revision

In 2015, RDR launched its inaugural Index, which ranked 16 Internet and telecommunications companies. For the 2017 Index, RDR has expanded the ranking to cover additional companies and services, including companies that produce mobile software and devices that create what RDR refers to as "mobile ecosystems." As a result, RDR expanded the methodology, adding new indicators and elements to account for the potential threats to users' freedom of expression and privacy that can arise from use of networked devices and software. The RDR team also further refined the methodology based on a detailed review of the raw data from the 2015 Index as well as consultations with stakeholders from civil society, academia, the investor community, and the companies themselves.

This document summarizes the main **structural** and **substantive** revisions we introduced to the 2017 Index methodology. We encourage stakeholders to review the following documents for additional detail on the changes we made to the methodology, available for download here:

- A table comparing the 2015 indicators to the 2017 indicators
- A clean version of the 2017 Index methodology research guidance, and glossary

Considering the fast-changing nature of the sector, we anticipate in future Index cycles we will make adjustments to the methodology to accommodate new developments. However, to preserve year-on-year comparability of results, future revisions of the Index methodology will be narrower in scope. Because an important goal of the Index is to demonstrate company change over time, we intend to provide enough context in the 2017 Index to enable companies and other stakeholders to gauge their changes from 2015 and 2017.

Structural Revisions

The following summarizes the key structural changes made to the 2017 Index methodology.

Framing of indicators and elements

In the 2015 Index methodology, indicators were written as questions, and elements were written as statements. The revised methodology reverses this. The indicators are now framed as normative statements (*"The company should…"*) and elements are now questions (*"Does the company…?*"). The indicators now explicitly state what standards the Index expects companies to meet, and the elements convey how the Index measures whether companies meet those standards.

Element structure and scoring

The 2017 Index methodology standardizes the question structure and scoring across all indicators. For companies to receive full credit on an indicator they have to receive full credit for each indicator element. The 2015 methodology primarily used a "checklist" question structure, but also included several single-choice indicators as wells as a few based on a "if/then" scoring approach, in which a company would receive full credit if it fulfilled the "A" criteria, otherwise, it could only receive a score of 80 percent if it fulfilled all the criteria under the "B" criteria. In the 2017 Index, we have revised this to make each indicator based on the checklist approach, which will help stakeholders better understand how companies are evaluated and scored.

Addition of mobile ecosystems

RDR has always intended to expand the Index to cover various types of companies, including those that produce software and devices. In addition to evaluating Internet and telecommunications companies, the 2017 Index will include companies that produce mobile software and devices. For the purposes of our project, we concluded that the core products offered by leading smartphone manufacturers (such as Apple and Samsung) and providers of smartphone operating systems (such as Google's Android) are best understood as *mobile ecosystems*. Given that people around the world increasingly access the Internet primarily, or even exclusively, through the use of handheld devices, or "smartphones," the 2017 methodology emphasizes the threats to freedom of expression and privacy that smartphones—including operating systems, third-party apps and the app stores through which users download them—pose to end-users, as well as the policies and practices that companies can put in place to mitigate these risks.

Expanded scope of indicators for telecommunication companies

In the 2015 Index, for telecommunications companies we evaluated pre- and post-paid mobile services together as one service. After an extensive review of the data from the 2015 research cycle, we found that in many cases, telecommunication companies were scoring partial credit on elements because their disclosure was adequate for one of their mobile services (for example, pre-paid mobile) but not the other (for example, post-paid mobile). In the 2017 Index methodology, we've broken out pre-paid and post-paid mobile services into two separate services.The goal here is to be able to identify differences in how company policies might impact subscribers of pre-paid mobile services and those who use post-paid mobile services.

Substantive Revisions

The following summarizes the key revisions to each of the 2017 Index methodology categories.

Commitment

In order to more accurately reflect what we seek to measure in the first section of the methodology, we have renamed this Index category from "Commitment" to "Governance." Most of these indicators and their elements go beyond seeking a commitment to respect freedom of expression and privacy. We look for company disclosure that demonstrates that the company has governance and oversight mechanisms in place to ensure that it implements its commitments in an accountable manner. For example, indicators in this section focus on disclosure of relevant oversight, due diligence, and remedy mechanisms. The "Governance" concept also more closely aligns with the terminology used by investors and company representatives; in applying this change, we seek to further engage these stakeholders in understanding the relevance of the methodology.

Freedom of Expression

The indicators in the "F" category have been expanded to capture additional information relevant to how company policies and practices might impact users' freedom of expression, such as additional elements related to a company's process for enforcing its terms of service. The element on network shutdowns that was included in the 2015 Index methodology has been expanded into its own indicator in order to better capture how companies explain their process for dealing with this growing threat to freedom of expression. In addition, several indicators have been reordered to ensure that indicators focused on similar topics are grouped together.

A brief summary of these changes are as follows:

F3: Process for terms of service enforcement

After reviewing the data from the 2015 Index, we found that company disclosure of content and account restrictions was quite related and that it made sense to evaluate these issues together in one indicator. We decided to regroup the elements from the 2015 Index indicators on content and account restrictions under the indicator heading of “process for terms of service enforcement,” which is now covered under **F3**.

We also added elements on how a company identifies content or accounts that violate its terms of service (Element 3) and whether any government or private entities receive priority consideration in identifying content that violates the terms of service (Elements 4 and 5). These additional elements seek to evaluate how well companies explain what prompts them to enforce their rules. Transparency around these processes will allow users to maintain their trust in how these platforms and services are governed.

F5: Split the elements focused on third-party requests for content restriction

In the 2015 Index, Indicator F6 focused on a company’s process to respond to third-party requests for content restriction. This covered requests from government entities (which include government ministries or agencies, law enforcement, and court orders in criminal and civil cases) as well as requests from private parties (e.g., a company, an NGO, an individual person). Researchers looked for company disclosure that may have included *both* government and private requests.This meant that companies could score partial credit for a few reasons: their disclosure encompassed government and private requests, but the disclosure itself was insufficient for full credit, or a company provided sufficient disclosure on only one type.

To provide companies with greater clarity about what we expect them to disclose and about how their disclosure is scored, we have split these elements (now housed under indicator **F5**) into separate elements focused on government requests and private party requests. By private requests, we mean requests made through some sort of defined or organized process. This can be a process established by law, (e.g., requests made under the U.S. Digital Millennium Copyright Act, the European Right to be Forgotten ruling, etc.) or a self-regulatory arrangement (e.g., company agreements to block certain types of images). The latter example does not include company actions to restrict content or accounts that violate terms of service, as that is evaluated in a separate indicator. If a company does not accept any requests from private parties, we would expect companies to publicly disclose this fact. Such disclosure would mean this indicator is N/A for that company.

F10: Added a new indicator focused on network shutdowns

Considering that network shutdowns are a growing human rights risk, we have broken out the element in the 2015 Index that addressed this issue and have created a new indicator, **F10**, focused on the issue. This indicator is only applicable for telecommunications companies.

In his report on the role of the private sector in respecting online freedom of expression, David Kaye, the UN Special Rapporteur for freedom of opinion and expression, identified network shutdowns as a "trend for concern," calling them "a particularly pernicious means of enforcing content regulations." The indicator includes elements that seek disclosure on why a company would restrict access to services, their process for responding to requests to shut down service, and their reporting on such requests. With this expanded indicator, our goal is to more clearly track company disclosure over time with regard to the specific threat of network shutdowns, separate from company disclosure regarding account or content restrictions. This information will hopefully help human rights advocates and other stakeholders engage with companies directly on this issue and the ways that companies can be more transparent about their responses to network shutdown requests.

Privacy

Several of the indicators in the "P" section related to user information have been reorganized and reframed in order to evaluate company disclosure of all aspects of the user information life cycle. These changes include adding a separate indicator focused on the purpose(s) for which companies collect and share user information, as well as adding language regarding each *type of user information* across these indicators. We also added an indicator on data breaches and revised several indicators related to security standards.

A brief summary of these changes are as follows:

P3-P7: Strengthened disclosure standards for user information

In our review of the 2015 data, we found that companies were often inconsistent in the level of detail they gave regarding user information and what they do with it. To further clarify our expectations regarding company processes to handle user information, we have reframed several elements in these indicators to specify that we expect disclosure of what happens to each *type of user information* the company collects. For example, if a company states that it collects six types of user information, we would expect the company to disclose how long it retains each of those six types of user information. This change applies to indicators **P3-P7**, which encompass company disclosure related to collection, sharing, purpose for collecting and sharing, and retention of user information, as well as users' control over their own information. In reframing these indicators, our goal is to encourage companies to be more specific and transparent in their policies regarding user information so that users can clearly understand what a company might do with each piece of information they collect.

P5: Added a new indicator on the purpose of collecting and sharing user information

The lifecycle of user information encompasses collection, use, sharing, and retention. The 2015 Index addressed all of these components, but only collection, sharing, and retention had dedicated indicators. The elements related to a company's *use* of the information they collect, share, or retain were spread across several indicators, making it difficult for stakeholders to see where the Index methodology evaluated this information.

In their feedback, stakeholders discussed the importance of clearly examining what companies do with user information and why. In addition, principles about the use of user information are explicitly stated in several privacy frameworks. The Fair Information Practice Principles (FIPPs), which provide the framework for many national and international privacy laws and guidelines, include “purpose specification,”meaning entities should state why they are collecting user information, and “use limitation,” meaning entities should not use information for purposes beyond those for which it was collected. The OECD privacy guidelines also reference these principles. The EU’s General Data Protection Regulation (GDPR) espouses the need for “purpose limitation” (Chapter 1, Article 1, paragraph 1(b), p. 33).

Consequently, we have moved the elements from the indicators referenced above into a separate indicator focused clearly on the purpose for the collection and sharing of user information (**P5** in the 2017 Index methodology). This indicator also includes a new element related to purpose limitation.

P7: Added new elements focused on users’ control over the use of their information for targeted advertising

In the 2015 Index, Indicator P5 Element 2 examined whether companies gave users the ability to control how their information was shared. The companies that received credit on this element did so based on disclosure related to users’ ability to control how their information was used for targeted advertising. We replaced this element with two elements focused specifically on the ability to control use of information for targeted advertising. We expect that companies give users the ability to control the use of their information for this purpose, and that companies clearly show users how to exercise this control.

P13, P14: Split the 2015 indicator focused on security standards

In the 2015 Index, Indicator P12 included several elements related to how companies secured their products and services. In order to strengthen the methodology as we add new types of services, we have broken this indicator into a separate indicator on security oversight **(P13)**, and a separate, more detailed indicator focused on addressing security vulnerabilities **(P14)**, in part because several of the human rights concerns related to mobile ecosystems fall into this category. In the 2015 Index, P12 Elements 5 and 6 were only applicable to Internet companies. For the sake of clarity, we have moved these elements into indicators focused on encryption (revised **P16**) and account security (revised **P17**), respectively. We have also added several elements related to security updates for mobile ecosystems.

P15: Added new indicator on data breaches

Several indicators in the 2015 Index methodology touched on the subject of company disclosure regarding security standards and approaches to security vulnerabilities. However, these indicators did not directly address how companies respond to another significant threat to users' privacy: data breaches.

Many companies collect and retain immense amounts of user information, and unauthorized access to this data by a malicious actor can result in significant threats to an individual's financial or personal security, in addition to exposing private information. Before deciding whether to hand over their personal information in order to use a company's services, users should be able to learn about the policies and procedures a company has in place to respond to data breaches. We've therefore added an indicator **(P15)** to evaluate what companies publicly disclose about their approaches to data breach incidents. This indicator seeks disclosure related to companies' processes for notifying data subjects who might be affected, notifying the relevant authorities without undue delay, and the steps a company might take to address the impact of a data breach on its users.

P18: Revised indicator focused on user education

In the 2015 Index, Indicator P14 focused on informing and educating users about potential threats. It included two elements, but Element 1 was only applicable to Internet companies. For greater clarity, we combined this element and P12, Element 6 from the 2015 Index into a separate indicator focused on account security, which is not applicable for telecommunications companies (revised **P16**). Thus, the revised version of this indicator in the 2017 Index **(P18)** includes only one element.

For more information

As noted above, we encourage stakeholders to review the following documents for additional detail on the changes we made to the project methodology; they are available for download here:

- A table comparing the 2015 indicators and the 2017 indicators
- A redline version of the 2017 Index methodology
- A clean version of the 2017 Index methodology research guidance, and glossary

For more information on the project please visit our website, where you can sign-up to receive regular project updates. Feedback on the methodology should be sent to feedback@rankingdigitalrights.org.