Summary of proposed revisions to the 2017 Corporate Accountability Index research methodology (consultation draft)

July 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

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

In November 2015, Ranking Digital Rights launched its inaugural Corporate Accountability Index, which evaluated 16 Internet and telecommunications companies according to 31 indicators focused on corporate disclosure of policies and practices that affect users' freedom of expression and privacy. Companies' scores and accompanying analysis were generated through a rigorous process including peer review, company feedback, and quality control. The data produced by the Index informs the work of human rights advocates, policymakers, and responsible investors and helps companies improve their own policies and practices.

About the revised methodology

Ranking Digital Rights has developed the Index as an annual ranking, and we plan to publish new editions in 2017 and 2018. For 2017, RDR will expand the Index to cover companies that produce software and devices. Subsequent iterations may include companies that produce networking equipment. As a result, we have added 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.

In some cases, the revisions alter the scope of what a particular indicator or element evaluates. In other cases, the revisions represent new elements or indicators. Given that the 2015 Index was the first time the methodology and research process were fully implemented, and after consulting with key stakeholders, we decided that it was appropriate to use the first half of 2016 strengthen the Index based on what we learned from producing the first edition.

Considering the fast-changing nature of the sector, we do anticipate making further adjustments to the methodology in future years. However, to preserve year-on-year comparability of results, it is likely that 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.

This document summarizes the structural and substantive revisions that we have made to the methodology. Three additional documents provide further detail on these revisions; they are available for download here: https://rankingdigitalrights.org/2016/07/05/new-draft-methodology/.

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

The revised methodology is a draft, and we invite feedback on the proposed revisions. **The deadline to submit comments is Friday, August 5, 2016.** Comments should be sent via email to feedback@rankingdigitalrights.org.

This document first explains the types of companies, products, and services that will be evaluated in the next Index. The process for deciding which companies to add to the Index is currently underway. The names of those companies will be announced around the same time that the methodology for the new Index is finalized.

The document then presents the major structural revisions to the Index, followed by a list of substantive changes to existing indicators and brief descriptions of the newly added indicators.

Expanding the Scope of the Index

The 2015 Index included Internet and telecommunications companies. RDR has always intended to expand the Index to cover various types of companies, including those who produce software, devices, and networking equipment. The 2017 Index will rank the same 16 Internet and telecommunications companies as the 2015 Index. It will also include up to six new companies, which will be a mix of Internet and telecommunications companies as well as new types of companies, products, and services. While networking equipment companies will not be included in the 2017 Index, it will include companies that produce software and devices.

Therefore, the draft revised methodology presented in this document will be applied to four types of companies: Internet, telecommunications, software, and device makers. Some companies offer products and services from more than one category: indeed, this type of convergence is a trend across the ICT sector.

As a reminder, the RDR Index research includes the following parameters:

1. We only assess publicly traded companies in the ICT sector—not privately-owned or fully state-owned companies.
2. Scores are based on publicly available information—we do not conduct technical testing or account for company practices that are not publicly disclosed by the companies themselves.
3. We focus specifically on the human rights of freedom of expression and privacy. For more information, please see our theory and strategy document here: https://rankingdigitalrights.org/project-documents/theory-and-strategy/

When evaluating device makers, we have decided to focus on mobile devices. People around the world increasingly access the Internet primarily, or even exclusively, through the handheld

devices, or "smartphones." For millions of human rights defenders, political dissidents, journalists, religious minorities, LGBTQ individuals, and ordinary people around the world, leading a safe and satisfying life in the 21st century requires secure, reliable mobile access to the free and open Internet. For this reason, the 2017 methodology emphasizes the threats to free 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.

The RDR team conducted extensive research, including consultations with expert technologists, into this sector and concluded that the core products offered by leading smartphone manufacturers are better understood as *mobile ecosystems*. When users choose a smartphone provider, they must create an account with that company, must select from a limited choice of hardware, must commit to a particular operating system, and will generally install new software (apps) through the app store associated with that company. Crucially, users can't mix and match, for example, by pairing hardware from one company with an operating system from another company and installing apps from a variety of app stores. Rather, users must commit to one set of products and services, which are linked through the user account. We refer to this indivisible set of goods and services (hardware, operating system, app store, and user account) as the *mobile ecosystem*.

Companies that produce these mobile ecosystems also offer a variety of other services, including email, cloud storage, office software, web browsers, music subscription services, and messaging apps. What distinguishes these products and services from the mobile ecosystem is that people can opt out of using them, and in some cases can "mix and match" services from different companies. Such services are evaluated separately, and indeed several were included in the 2015 Index.

Rather than creating a new set of indicators for software and devices (including mobile ecosystems), we incorporated concerns that are specific to this sector into the existing methodology, either by clarifying how existing elements apply or by drafting new elements.

List of Indicators

G: Governance
G1. Policy commitment
G2. Governance and management oversight
G3. Internal implementation
G4. Impact assessment
G5. Stakeholder engagement
G6. Remedy

F: Freedom of Expression
F1. Access to terms of service
F2. Changes to terms of service
F3. Content and account restriction
(Merger of F3 and F4 from 2015 Index)
F4. User notification about content and account restriction
(F5 from 2015 Index)
F5. Data about terms of service enforcement
(F9 from 2015 Index)
F6. Process for responding to government requests
(Split of F6 from 2015 Index)
F7. Data about government requests
F8. Process for responding to requests from private parties
(Split of F6 from 2015 Index)
F9. Data about private requests
(F8 from 2015 Index)
F10. Network management (telecommunications companies)
F11. Network shutdown (telecommunications companies)
(New indicator)
F12. Identity policy (Internet companies)
(F11 from 2015 Index)

P: Privacy
P1. Access to privacy policies
P2. Changes to privacy policies
P3. Collection of user information
P4. Sharing of user information
P5. Purpose for collecting and sharing user information
(New indicator based on existing elements from 2015 Index.)
P6. Users' control over information
(P5 from 2015 Index)

P7. Users' access to their own information
(P6 from 2015 Index)
P8. Retention of user information
(P7 from 2015 Index)
P9. Collection of user information from third parties (Internet companies)
(P8 from 2015 Index)
P10. Process for responding to third-party requests for user information
(P9 from 2015 Index)
P11. User notification about third-party requests for user information
(P10 from 2015 Index)
P12. Data about third-party requests for user information
(P11 from 2015 Index)
P13. Security oversight
(Split of P12 from 2015 Index)
P14. Addressing security vulnerabilities
(Split of P12 from 2015 Index)
P15. Encryption of user communication and private content (Internet, software, and device companies)
P16. Account security (Internet, software, and device companies)
(Split of P14 from 2015 Index)
P17. Inform and educate users about potential threats
(Split of P14 from 2015 Index)

Structural Revisions

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…?") This way, the indicators explicitly state what standards the Index expects companies to meet, and the elements convey how the Index measures whether companies meet those standards. For example, indicator C5 in the 2015 methodology asked, "Does the company engage with a range of stakeholders on freedom of expression and privacy issues?" In the revised methodology, this reads, "The company should engage with a range of stakeholders on freedom of expression and privacy issues."

Uniform Question Type and Scoring

The 2015 methodology primarily used a "checklist element" question structure. Under this structure, one indicator had several elements, and a company would earn full credit on the indicator only if it received full credit on each checklist element. Otherwise, indicator scores were proportional. (i.e., If a company met three of four elements for a particular indicator, its score on that indicator would be 75 percent). The 2015 methodology also included a few single-choice indicators, in which the indicator question had a list of answer options that corresponded to a particular score. Researchers selected the answer that best fit the company's disclosure, and the company received the score associated with that answer on the indicator. Finally, a few indicators used an If/Then scoring approach, where 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.

The revised methodology standardizes the "checklist element" question structure and scoring across all indicators. This revision brings consistency to the methodology, which will help stakeholders better understand how companies are evaluated and scored.

Substantive Revisions

Changed title of "Commitment" section to "Governance"

In the 2015 Index, the first six indicators were grouped into a section titled, "Commitment." However, 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. Consequently, we have revised the title of this section from "Commitment" to "Governance." The notation for the indicators in this section has been updated to use "G" instead of "C" (e.g., G1, G2, etc.).

Revised scope of G1: Policy commitment

In the 2015 Index, this indicator sought disclosure of a company's policy commitment to respect human rights and privacy as well as evidence that senior executives publicly discuss such commitments. Question B of the 2015 indicator, which asked whether senior executives made public statements related to users' freedom of expression and privacy in a prominent venue, required a significant amount of subjective analysis on the part of researchers. Given that the question required researchers to look for disclosure beyond the company's own documents, it was also difficult to determine the extent to which companies were evaluated consistently. The revised G1 no longer includes Question B as a means of focusing this indicator solely on the company's policy commitment.

Summary of changes in the Freedom of Expression section

The indicators in the F section have been reorganized so that indicators focused on similar topics are next to each other. Indicators F3, F4, and F5 focus on a company's rules for using its product or services and enforcement of those rules. Indicators F6 and F7 focus on government requests for content restriction. Indicators F8 and F9 focus on private requests for content restriction.

To summarize the substantive revisions in the F indicators, we have:

- Merged F3 and F4 from the 2015 Index into one indicator (F3)
- Split F6 from the 2015 Index into two indicators (F6 and F8)
- Added a new indicator focused on disclosure from telecommunications companies about network shutdowns (F11)
- Added elements to the revised F3 and F5 related to terms of service enforcement

A brief explanation of each change follows.

Merged indicators on content and account restriction

In the 2015 Index, indicator F3 focused on a company's reasons for content restriction and indicator F4 focused on a company's reasons for account or service restriction. The 2015 version of F4 sought disclosure related to restricting an individual account as well as shutting down service for all users in a particular region. However, the 2015 research found that disclosure about content restriction and individual account restriction were quite related and that it made sense to evaluate these issues together in one indicator. Disclosure about shutting down service for all users in a particular region (which was evaluated in indicator F4 element 2 in the 2015 Index) has been moved into a new indicator focused on network shutdowns (F11 in the revised methodology) that is only applicable to telecommunications companies.

Split the indicator 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). Elements 1-4 of the 2015 indicator F6 sought disclosure related to specific types of requests. Elements 5-8 sought disclosure related to what the company's process encompassed. On elements 5 and 7, researchers looked for company disclosure related to government requests. On elements 6 and 8, researchers looked for company disclosure that encompassed government and private requests. This meant that companies could score partial 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 F6 into two indicators. The revised indicator F6 from the list above focuses on company disclosure related to the process for responding to government requests, and the revised indicator F8 from the list above focuses on the company's process for responding to private 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.

We especially welcome stakeholder feedback on this change.

Added an indicator for telecommunications companies focused on network shutdowns

In the 2015 Index, indicator F4 element 2 focused on disclosure by telecommunications about network shutdowns. Considering that network shutdowns are a growing human rights risk, we have added an indicator, F11 in the revised methodology, 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. These elements are similar to elements that are included in other indicators for other types of company processes.

We especially welcome stakeholder feedback on this new indicator and its elements.

Added elements focused on terms of service enforcement

In the revised version of indicator F3, focused on content and account restriction, we have added elements on how a company identifies content or accounts that violate its terms of service (element 3) and whether any non-governmental/non-judicial entities have priority in identifying content that violates the terms of service (element 4). In the revised version of F5, focused on data about terms of service enforcement, we have removed several elements that prescribed how companies should report data on terms of service enforcement and replaced them with an element about whether the company has a public reporting reporting framework that provides such data.

In the 2015 Index, indicator F9 focused on terms of service enforcement. In the revised methodology, indicator F5 focuses on terms of service enforcement. We moved it so it would be closer to the indicators that relate to company rules about content and account restriction (F3) and user notification when content or accounts have been restricted (F4).

However, we welcome stakeholder feedback as to whether we should consider including all elements related to terms of service enforcement under one indicator (as we have done with F11 on network shutdowns.)

Summary of changes in the Privacy section

The indicators in the P section have been reorganized to accommodate the addition of a new indicator (based primarily on existing elements) and the splitting of two indicators.

To summarize the substantive revisions in the P indicators, we have:

- Reframed the question structure and several elements in indicators related to company processes related to user information (P3-P8 from the 2015 Index, P3-P9 in the revised methodology)
- Pulled several existing elements into a separate indicator (P5 in the revised methodology) focused on why companies collect and share user information
- Added elements to the indicator on users' control over information (P6 in the revised methodology).
- Split indicator P12 from the 2015 Index into separate indicators focused on security oversight (P13 in the revised methodology) and addressing security vulnerabilities (P14 in the revised methodology)
- Split indicator P14 from the 2015 Index into separate indicators focused on account security (P16 in the revised methodology) and materials to educate users about threats (P17 in the revised methodology)

A brief explanation of each change follows.

Re-framed indicators focused on company handling of user information

In the 2015 Index, indicators P3, P4, P7, and P8 included an A/B structure, where companies that disclosed they did not collect, share, or retain user information would receive full credit (criteria A). Otherwise, companies were evaluated on a list of elements under criteria B, and their maximum score on that indicator was capped at 80 percent. In an effort to streamline the methodology and ensure that each indicator sets clear standards, we have removed the A/B criteria. These indicators are now structured with the checklist element format that is present in the rest of the revised methodology. To further clarify our expectations regarding company processes to handle user information, we have re-framed 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. We welcome feedback on this approach.

Added a new indicator on purpose for collecting and sharing user information

The lifecycle of user information encompasses collection, use, sharing, and retention.
The 2015 Index addresses all of these components, but only collection, sharing, and retention have dedicated indicators. In the 2015 Index, indicator P3 element 4 sought clear disclosure about why companies collect user information; indicator P4 element 2 sought clear disclosure

about why companies share user information; and indicator P4 element 5 sought information related to internal sharing of user information.

In their feedback, stakeholders discussed the importance of examining what companies do with user information. In addition, several privacy and data protection frameworks explicitly discuss use of information. Importantly, principles about 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 P3 and P4 referenced above into a separate indicator focused clearly on the purpose for such company actions (P5 in the revised methodology). This indicator also includes a new element related to purpose specification.

Added new elements focused on users' control over use of their data for targeted advertising

In the 2015 Index, indicator P5 element 2 sought 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.

Split the indicator focused on security standards

In the 2015 Index, indicator P12 included several elements related to how companies secured their products and services. We have moved elements 1 and 3 into a separate indicator on security oversight (revised P13). Element 2 has been spun out into a separate indicator focused on addressing security vulnerabilities, in part because several of the human rights concerns related to mobile ecosystems fall into this category. In the 2015 Index, indicator 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 P15) and account security (revised P16), respectively. We have also added several elements related to security updates for mobile ecosystems.

Split the 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 the indicator focused on educating users includes only one element (revised P17).

More information on the draft revised methodology

We encourage stakeholders to review the following documents for additional detail on the changes we are proposing; they are available for download here: https://rankingdigitalrights.org/2016/07/05/new-draft-methodology/.

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

We also invite feedback on the proposed revisions. **The deadline to submit comments is Friday, August 5, 2016.** Comments should be sent via email to feedback@rankingdigitalrights.org.