

# Ranking Digital Rights Phase 1 Pilot Study

Report on Pilot Study Results and Lessons Learned

March 2015

Produced by



[rankingdigitalrights.org](http://rankingdigitalrights.org)



[www.sustainalytics.com](http://www.sustainalytics.com)

## Acknowledgments

Work by Ranking Digital Rights and Sustainalytics on this pilot study, conducted from August 2014 through February 2015, was supported by the following organizations:

The John S. and James L. Knight Foundation  
The John D. and Katherine T. MacArthur Foundation  
Hivos People Unlimited  
The Ford Foundation  
Open Society Foundations

For a full list of project funders please see: <https://rankingdigitalrights.org/who/funders>

## About Ranking Digital Rights

Ranking Digital Rights is a project hosted by New America's Open Technology Institute focused on developing a system to assess, compare, and publicly rank the world's most powerful ICT companies on free expression and privacy criteria. For more about the project please visit [rankingdigitalrights.org](http://rankingdigitalrights.org)

For more about New America please visit [www.newamerica.org](http://www.newamerica.org)

For more about the Open Technology Institute please visit [www.newamerica.org/oti](http://www.newamerica.org/oti)

## About Sustainalytics

Sustainalytics is a leading independent environmental, social and governance (ESG) research and analysis firm that supports investors around the world with the development and implementation of responsible investment strategies. As the research partner for the Ranking Digital Rights pilot project, Sustainalytics helped design the research methodology for the initiative and rank leading global ICT companies on policies and practices on free expression and privacy in relation to human rights standards and laws.

With 13 offices globally, Sustainalytics has over 200 staff members, including more than 100 analysts with a broad range of industry and language expertise. The firm is the primary research partner for the 2014 Access to Medicine Index, among other leading rankings and indices. For the past three years, Sustainalytics was voted best independent responsible investment research firm in Extel's IRRI survey. For more information about Sustainalytics, please visit [www.sustainalytics.com](http://www.sustainalytics.com).



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

# Table of Contents

- Part 1: Introduction..... 5**
  - 1.1 Project Goals .....5**
  - 1.2 Pilot Study Goals .....5**
  - 1.3 Methodology Development.....6**
  - 1.4 Company Selection .....6**
- Part 2: Pilot Results..... 8**
  - 2.1 Findings Based on Overall Scores .....9**
  - 2.2 Findings Based on General Human Rights, Free Expression, and Privacy ..... 10**
    - 2.2.1 General Human Rights ..... 10
    - 2.2.2 Freedom of Expression ..... 11
    - 2.2.3 Privacy ..... 12
  - 2.3 Indicator-Specific Findings ..... 13**
    - 2.3.1 Indicators with the strongest average performance ..... 13
    - 2.3.2 Other indicators of interest ..... 14
    - 2.3.3 Indicators with the poorest performance ..... 15
  - 2.4 Comparing Internet and Telecommunications Companies ..... 15**
  - 2.5 What the data does and does not tell us ..... 17**
- Part 3. Main Questions for Methodology Revision..... 18**
  - 3.1 Scope..... 18**
  - 3.2 Scoring ..... 19**
  - 3.3 Business Models ..... 20**
  - 3.4 Presentation of Results ..... 23**
- Part 4: Indicator Assessments ..... 24**
  - 4.1 The Two Most Problematic Indicators ..... 24**
    - 4.1.1 Identity Policies ..... 24
    - 4.1.2 Net Neutrality ..... 26
  - 4.2 Other Indicator-Specific Comments ..... 28**
    - 4.2.1 Human Rights Impact Assessments ..... 28
    - 4.2.2 Deep Packet Inspection ..... 29
    - 4.2.3 Terms of Service/Privacy Policies..... 29
    - 4.2.4 Freedom of Expression/Privacy Commitments ..... 30
    - 4.2.5 Government Requests ..... 31
    - 4.2.6 Requests from Private Entities ..... 31
    - 4.2.7 Other Content Restriction Requests ..... 32
    - 4.2.8 User Notification ..... 32
    - 4.2.9 Data Collection and Retention ..... 33
    - 4.2.10 Data Location ..... 34
    - 4.2.11 Third-Party Access to Data ..... 34
    - 4.2.12 User Controls ..... 35
    - 4.2.13 Security ..... 36

|  |           |
|--|-----------|
| <b>Part 5: Company Engagement.....</b>   | <b>37</b> |
| 5.1 Company willingness to engage.....   | 37        |
| 5.2 Variations in disclosure and reporting style.....                          | 38        |
| 5.3 Views on independent assessment.....                                       | 38        |
| 5.4 Regulatory and political context.....                                      | 39        |
| <b>Part 6: Civil society adoption .....</b>                                    | <b>40</b> |
| 6.1 Presentation and data .....  | 40        |
| 6.2 Language.....  | 40        |
| 6.3 Target audiences .....   | 40        |
| 6.4 Outreach and advocacy.....   | 41        |
| <b>Part 7: Investor feedback.....</b>  | <b>43</b> |
| 7.1 Disclosure vs. performance .....   | 43        |
| 7.2 Materiality.....   | 43        |
| <b>Part 8: Stakeholder Consultation Outcomes .....</b>                         | <b>44</b> |
| 8.1 Simplify the ranking .....   | 44        |
| 8.2 Name and frame the project differently.....                                | 44        |
| 8.3 Emphasize standards.....   | 45        |
| 8.4 Reward good practice in addition to disclosure .....                       | 45        |
| 8.5 Sharpen geographical focus .....   | 45        |
| 8.6 Separate Internet companies and telecoms .....                             | 45        |
| 8.7 Represent the results visually.....  | 45        |
| <b>Part 9: Conclusions and next steps.....</b>                                 | <b>48</b> |
| <b>Annex 1: Methodology and Research Process.....</b>                          | <b>50</b> |
| A1.1 Indicators Selected for Local and Language Review .....                   | 50        |
| A1.2 Selection of Subsidiaries, Services, and Languages for Local Review ..... | 51        |
| A1.3 Answer Categories .....   | 52        |
| A1.4 Pilot Research Steps .....  | 53        |
| A1.5 Scoring and Weighting.....  | 54        |
| <b>Annex 2: Research process: critical analysis.....</b>                       | <b>56</b> |
| A2.1 Pilot Study Workflow .....  | 56        |
| A2.2 Researcher Guidance .....   | 57        |

## Part 1: Introduction

The Ranking Digital Rights project is developing a system to rank the world's most powerful information and communications technology (ICT) companies on their respect for users' free expression and privacy rights. The data we generate will equip advocates, policymakers, and investors with the facts they need to hold companies accountable. It will also help companies improve their own policies and practices, and inform technology users about which companies are better equipped to respect their rights.

The project includes two phases. Phase 1 ranks Internet and telecommunications companies based and operating in countries around the world. This pilot study focused on 12 Phase 1 companies. The names of the companies examined in the pilot will not be disclosed. We plan to release a full, public ranking of 10-15 Phase 1 companies in Fall 2015. (Note: the number of companies to be ranked in Phase 1 has been reduced due to funding constraints.) Phase 2 will incorporate software, device, and equipment manufacturers into the ranking in 2016, and may increase the overall number of companies ranked, funds permitting.

### 1.1 Project Goals

- Encourage companies to develop, deliver and manage products and services in a manner consistent with international human rights norms;
- Inform companies, individual users, civil society, academics, investors, governments, and the public about the relationship between the ICT sector and human rights.
- Identify what specific legal and political factors prevent or hinder companies from respecting users' and customers' human rights;

### 1.2 Pilot Study Goals

In Fall 2014, Ranking Digital Rights partnered with the investment research firm Sustainalytics to refine the ranking methodology developed by the RDR team in consultation with a wide range of stakeholders, design a research process, and then test it on 12 companies in a pilot study.

This report presents the pilot study results with company names redacted, because the methodology was experimental and requires further revision before being applied publicly. The report also discusses lessons learned about what aspects of the methodology and research process worked well or less well, and poses some questions about how to revise the ranking methodology and research process before embarking on the full public ranking. Many of these points were discussed at meetings with stakeholders who reviewed a draft version of this report. In these meetings, held in February and March 2015, we sought input on how to revise the methodology in a way that fits our resource constraints and provides a meaningful ranking.

## 1.3 Methodology Development

The Phase 1 pilot study tested RDR’s ranking methodology on 12 Internet and telecommunications companies with headquarters and operations around the world. This methodology is the product of extensive research and stakeholder consultation. The first version of the methodology emerged out of case studies in which RDR and an international team of researchers examined dozens of Internet and telecommunications companies based in eight countries. We then collected two rounds of feedback on the methodology. Descriptions of how RDR developed the methodology and all relevant documents can be found at: <https://rankingdigitalrights.org/methodology-development>.

The Phase 1 pilot study described in this report tested the third version (v3) of the methodology.<sup>1</sup> This methodology examines information that is publicly disclosed by companies. The research process did not involve company surveys or interviews that would provide information not otherwise available in the public domain. The decision to define the methodology’s scope in this way was based on what our team learned from extensive case study research described in a separate paper titled “Case Study Research Overview,” which is downloadable from the project website: <https://rankingdigitalrights.org/project-documents/phase-1-case-study-research>.

The final pilot methodology contained 46 indicators divided into three sections: General Human Rights (12 indicators), Freedom of Expression (9 indicators), and Privacy (25 indicators). The methodology document containing all indicators, their associated “answer categories”, lists of elements to be evaluated in scoring, plus explanatory footnotes can be viewed online or downloaded from the project website at: <https://rankingdigitalrights.org/project-documents/phase-1-pilot-methodology>.

## 1.4 Company Selection

Four Internet companies and eight telecommunications companies were chosen for the pilot. We considered the following factors when selecting companies. Note that not all factors applied to all companies selected.

- **User base:** The companies selected have a significant footprint in the areas where they operate; meaning a substantial user base for telecommunication companies in the countries selected, and a large number of global users for Internet companies (based on Alexa ranking). The policies and practices of selected companies, and their potential to improve, thus affects a large number of people.
- **Geographic diversity:** The companies selected for the pilot collectively have users in many regions around the world. Though none of these companies are based in the Middle East, we included in our review Middle Eastern operating companies of some of

---

<sup>1</sup> <https://rankingdigitalrights.org/project-documents/phase-1-pilot-methodology/>

the telecommunications groups, and also examined Arabic language disclosure for several of the Internet companies.

- **Human rights risks:** The companies selected are operating in or have a significant user base in countries where human rights are not universally respected, based on relevant research of organizations including Freedom House, the Web Foundation and Reporters Without Borders; as well as stakeholder feedback.
- **Stakeholder relationships:** As part of the pilot study, we asked representatives from civil society organizations based in six countries in different parts of the world to fill out an extensive questionnaire exploring the ranking's relevance to stakeholders in their country and how the ranking results could support their advocacy efforts. To the extent possible, we included companies that operate in, or whose services are used heavily by, people in those organizations' home countries.

**More information about the methodology and research process:** Please see Appendix A for a detailed description of how the indicators were evaluated, how we approached challenges of linguistic and geographic diversity across companies' global operations, scoring and weighting, etc.

## Part 2: Pilot Results

This section reviews the results of the pilot study, highlighting findings from overall performance as well as performance across categories of indicators and sectors. It discusses indicators on which companies fared particularly well or poorly, and some other notable results. It then describes trends that may inform the methodology revision and framing of the public ranking.

Note that most indicators in this pilot measure and compare public commitments and disclosures. Exceptions are two indicators (G3 and P25) focusing on independent third-party assurance that verifies whether companies actually implement commitments and policies. (Although the existence of such assurance must itself be disclosed). Scores do not reflect insider knowledge obtainable by company interviews or surveys.

The table below contains overall company scores as well as scores broken out by category. See section 2.2 for further examination of scores according to the three categories. Also note that the pilot methodology applied minimal weighting to the different indicators because the methodology remains experimental. See Annex 1.5 for details on scoring and weighting.

**Phase 1 Pilot Scores (numbers are scores out of 100)**

|    | <b>Company</b> | <b>Sector</b>      | <b>Average Total Score<sup>2</sup></b> | <b>Weighted for General Human Rights</b> | <b>Weighted for Freedom of Expression</b> | <b>Weighted for Privacy</b> |
|----|----------------|--------------------|--|--|---|-----------------------------|
|    |                |                    | <b>28.04</b>                           | <b>32.33</b>                             | <b>22.31</b>                              | <b>28.24</b>                |
| 1  | Company A      | Internet           | 65.14                                  | 68.10                                    | 51.56                                     | 68.84                       |
| 2  | Company B      | Telecommunications | 47.18                                  | 50.73                                    | 39.56                                     | 48.36                       |
| 3  | Company C      | Internet           | 46.93                                  | 45.70                                    | 54.33                                     | 44.76                       |
| 4  | Company D      | Internet           | 46.61                                  | 52.70                                    | 41.33                                     | 46.08                       |
| 5  | Company E      | Telecommunications | 29.51                                  | 53                                       | 14.67                                     | 24.52                       |
| 6  | Company F      | Telecommunications | 26.02                                  | 44.73                                    | 14.67                                     | 21.88                       |
| 7  | Company G      | Telecommunications | 25.38                                  | 39.09                                    | 25.78                                     | 19.20                       |
| 8  | Company H      | Internet           | 19.61                                  | 16.60                                    | 14.78                                     | 22.56                       |
| 9  | Company I      | Telecommunications | 9.93                                   | 3  | 3.67                                      | 15.24                       |
| 10 | Company J      | Telecommunications | 9.73                                   | 5.27                                     | 3.67                                      | 13.88                       |

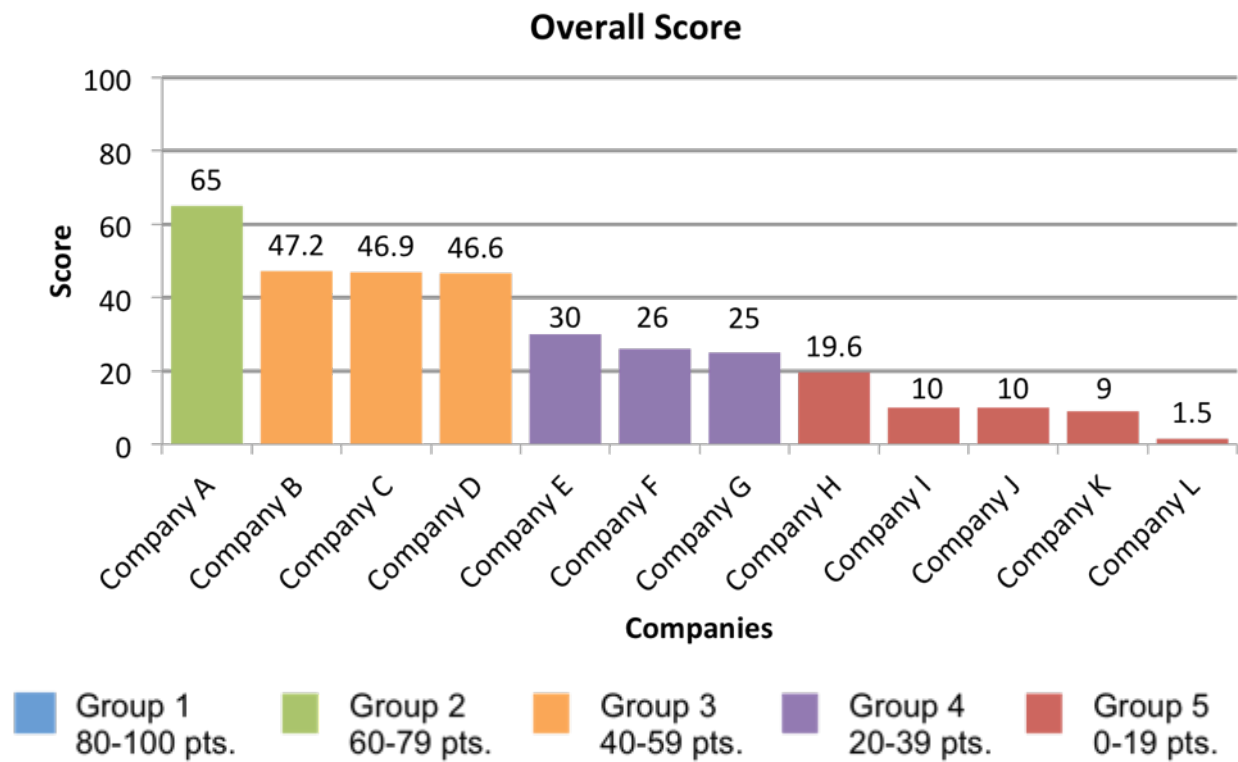
<sup>2</sup> The ‘per category’ score is the company’s total score in that category divided by the number of applicable indicators in that category; for this reason the ‘per category’ scores do not add up to the ‘total’ score, which is the average of all the company’s scores.



|    |           |                    |      |   |      |       |
|----|-----------|--------------------|------|---|------|-------|
| 11 | Company K | Telecommunications | 9.00 | 6 | 3.67 | 12.24 |
| 12 | Company L | Telecommunications | 1.47 | 3 | 0    | 1.32  |

## 2.1 Findings Based on Overall Scores

The bar graph below lists the companies and their total scores, organized into five scoring groups. (We may assign descriptive names to those groups in the full ranking, but for now we have simply given them numbers.)

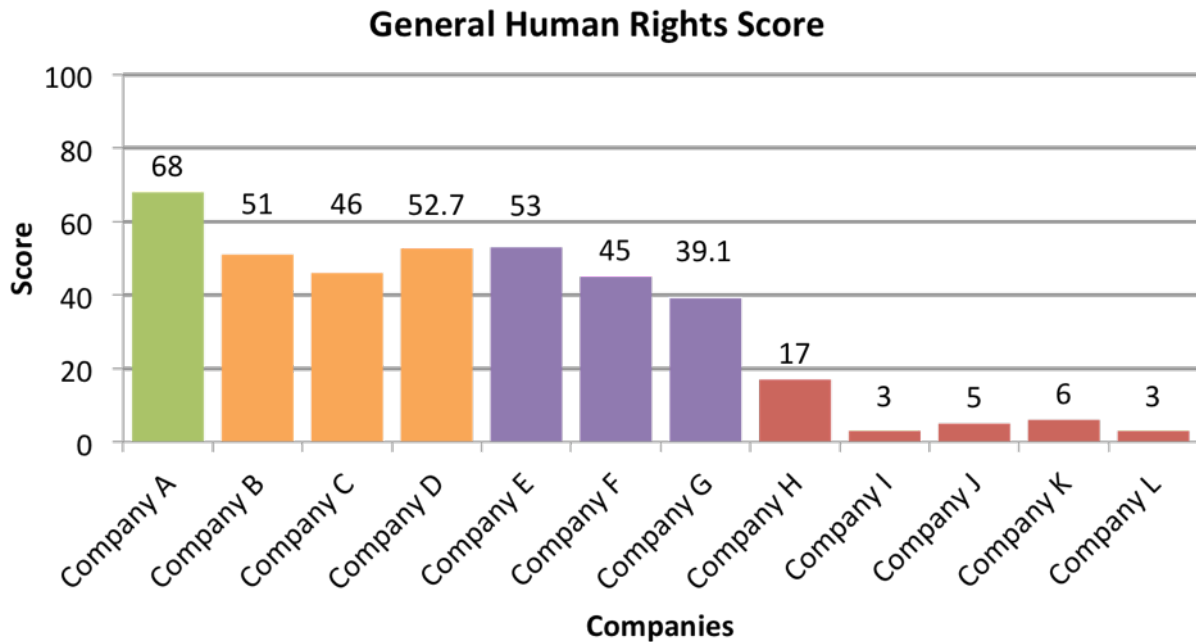


No company scored high enough to achieve Group 1, which would require a score of 80 or higher out of 100 possible. An almost equal point difference separated the next three clusters, with 18 points between Group 2 (one company) and Group 3 (three companies) and 17 points between Group 3 (three companies) and Group 4 (three companies). The final cluster of Group 5 (five companies) included a large point differential, with scores near 20, 10, and 2. These results suggest that companies have significant room to improve when it comes to their commitments and disclosures related to users' free expression and privacy rights.

## 2.2 Findings Based on General Human Rights, Free Expression, and Privacy

On average, companies scored highest in the general human rights section of the methodology, with 32.33 points, and lowest in the freedom of expression section, with 22.31 points. The average score in the privacy section was 28.24 points.

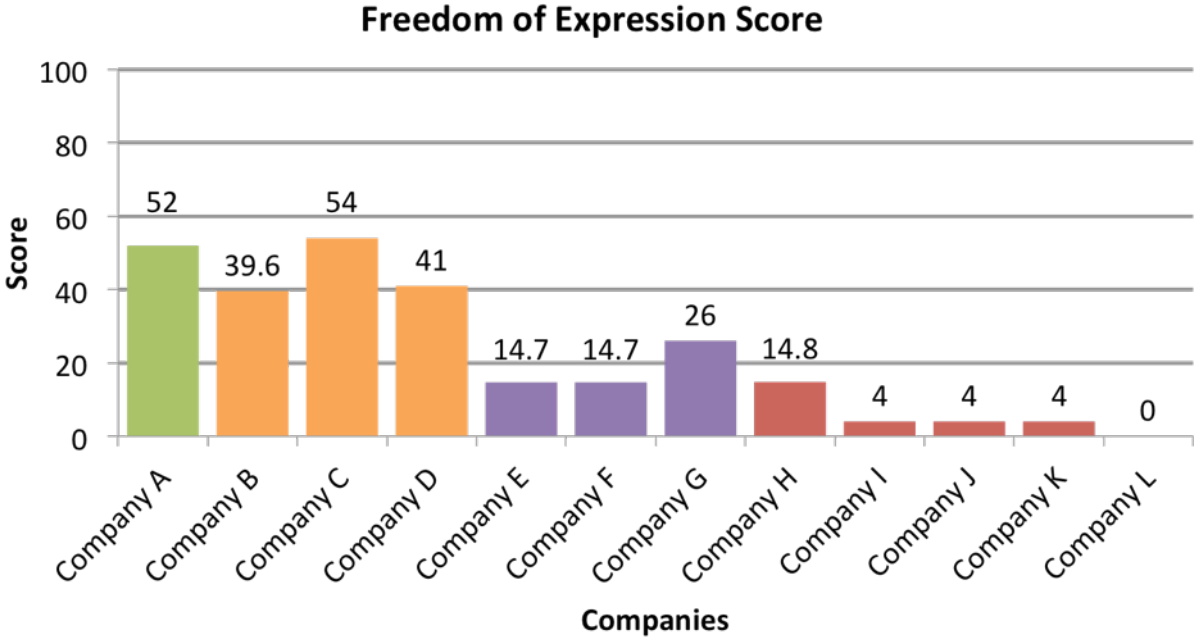
### 2.2.1 General Human Rights



Seven companies (A, B, D, E, F, G, and L) scored higher on general human rights than they did overall. Telecommunications companies E, F, and G had especially high differences between their general human rights and overall scores, with jumps of 14, 19, and 23 points. Company E, also a telecommunications company, which ranked fifth overall with a score of 29.51 jumped to second place in general human rights with a score of 53.

This jump by the three telecommunications companies appears to be related to the business models of telecommunications companies. While Internet companies have a relatively flat management structure with the head office taking responsibility for details of terms of service and privacy policies, telecommunications companies tend to delegate responsibility to subsidiaries, which are in turn less consistent about how they communicate externally. Further discussion of differences in business models can be found in section 3.3. Stakeholder feedback on the differences between company types is discussed in section 8.6.

2.2.2 Freedom of Expression

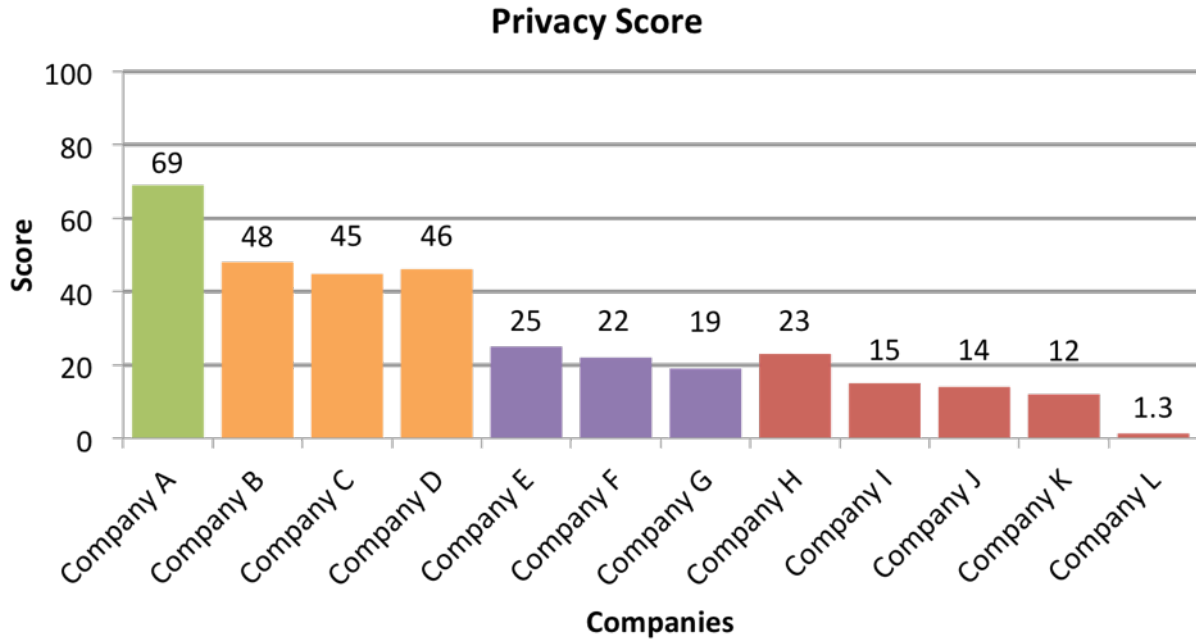


Two companies (C and G, one Internet company and one telecommunications company) scored higher on freedom of expression than they did overall. Company L (a telecommunications company) earned no points for freedom of expression.

Company C’s freedom of expression score was eight points higher than its overall score, putting it first in freedom of expression with a score of 54. Company C’s top score in this category had much to do with the thoroughness of the Internet company’s transparency reporting and clarity of disclosure on issues related to content restriction. This contrasted with its “general” score, which was lower than all but one Internet company because it discloses less information about general commitments and practices, and some of the other companies are more competitive with it on privacy-related indicators.

Company G’s freedom of expression score was substantially higher than the other telecommunications companies entirely thanks to the telecommunication company’s strong scores on F1 (implementation by staff at all levels of the company’s freedom of expression commitments) and F2 (whether it explains to users why accounts or access may be deleted, removed, deactivated etc.).

### 2.2.3 Privacy



Six companies (two Internet: A and H, and four telecoms: B, I, J, K) scored higher on privacy than they did overall. The ranking on privacy largely mirrored the overall ranking. Company H moved slightly higher, from eighth in the overall ranking to sixth in privacy.

Because the privacy indicators in this methodology include aspects of commercial data collection or sharing as well as security, privacy appears to be an area where companies that do not otherwise perform well might see some stronger scores.

## 2.3 Indicator-Specific Findings

Note that the indicators discussed below include elements to be assessed in scoring and answer categories, the full details of which can be found in the pilot methodology document.

### 2.3.1 Indicators with the strongest average performance

The following indicators showed high average performance across companies (average scores of 52 points or higher out of 100).

1. **Accessible Terms of Service (G7):** On average, companies performed best on this indicator, which asked whether a company makes its terms of service freely available in plain and accessible language. The company average for this indicator was 64 points. This was **one of only two indicators for which all companies scored above zero. Three scored “strong,” five were “partial” and four scored “weak”**. G7 was one of 16 indicators selected for a spot-check review of local operations and languages. See the Annex, A1.1 and A1.2 for details of that process. For a discussion of lessons learned on this and other indicators related to Terms of Service and privacy policies see section 4.2.3.
2. **Security and Encryption (P23):** This indicator, asking whether the company deploys strong industry standards of encryption and security, was **one of only two indicators on which all companies scored above zero. Two scored “strong,” four were “partial,” and six were “weak”**. The company average for this indicator was 55 points, tied with P1 and P2 discussed below. P23 was one of the three indicators (with P24 and P25) reviewed by technical experts. For more about that process see the Annex, A2.1. For a discussion of some of the issues that arose with this indicator see section 4.2.13.
3. **Company-wide commitment to privacy (P1):** This indicator asks whether the company provides evidence that it supports implementation by staff at all levels and throughout the company of its privacy commitments. While the company average was also 55, the standard deviation was greater. **Five scored “strong,” only one scored “partial,” three scored “weak” and three received no score due to lack of evidence**. For a discussion of questions that arose with this indicator see section 4.2.4.
4. **Availability of privacy policies (P2):** This indicator mirrors G7 on Terms of Service, asking whether the company’s privacy policy or policies are accessible to users, without needing to sign up or make a purchase. The company average was the same as the previous two indicators, but **only two companies were “strong,” five were “partial,” four were “weak”, and one showed no evidence**. P2 was also one of 16 indicators selected for a spot-check review of local operations and languages. See the Annex, A1.1 and A1.2 for details of that process. For a discussion of lessons learned on this and other indicators related to Terms of Service and privacy policies see section 4.2.3.

5. **Executive commitment (G4):** This indicator asks about efforts by the CEO and/or other top officers to advance users' rights including freedom of expression and privacy. The company average was 54 out of 100 possible points, with six companies receiving full scores (100) with "executive level commitment," one company receiving half points (50) with "management level commitment" and the remaining five companies showing no evidence.
6. **Personal information collection (P5):** This indicator asks whether the company discloses what personally identifiable information (PII) is collected, how it is collected, and why. The company average was 52, with two Internet companies receiving full points, four companies partial, five companies weak, and one company showing no evidence. This indicator was one of 16 indicators selected for a spot-check review of local operations and languages. See the Annex, A1.1 and A1.2 for details of that process.

### 2.3.2 Other indicators of interest

**Human Rights Impact Assessment:** Four of the twelve companies assessed (one Internet, three telecommunications) disclose that they undertake a human rights impact assessment process (including privacy impact assessment). Only three undergo a third-party assurance process for any part of these assessments. See section 4.2.1 for a discussion about questions that arose with indicators focused on human rights impact assessment.

**"Transparency reporting:"** The methodology contained five different indicators related to what has come to be known as "transparency reporting." Three were placed in the "freedom of expression" category broken down in terms of whether the transparency related to government requests, private requests, or companies' self-enforcement of their terms of service. Two were placed under "privacy", one pertaining to government requests for user data and the other about private requests. The results produced three general observations about the set of companies evaluated:

1. **Indicators dealing with government requests received the highest average scores for all companies.** P13, which asked whether companies report regularly on the number of **government requests for user data**, saw five companies (three Internet, two telecoms) receiving some kind of score. F5, which asked whether companies report regularly on the number of **government requests to restrict access or remove content**, had four companies (three Internet, one telecom) with partial scores.
2. **Indicators dealing with private requests** (including DMCA takedowns, requests from watchdog organizations, and private requests from individuals) **enjoy less transparency.** Three Internet companies received some kind of score on F6 which asked about private requests for content restriction or removal. Only one company scored any points on P14, which asked about private requests for user data.

3. **There is no transparency about terms of service enforcement.** This was one of two indicators for which no company received a score.

**User Security Awareness (P24):** This indicator asks whether companies publish information to help users defend against hacking and phishing attacks. It is one of three security-specific indicators, along with P23 above and P25 below. One company received full points, ten companies received weak scores, and one company showed no evidence. This indicator was one of 16 indicators selected for a spot-check review of local operations and languages. See the Annex, A1.1 and A1.2 for details of that process.

**Security Audit (P25):** This indicator asks whether companies disclose that they have undergone an independent security audit. Only five companies received any kind of score: one strong, one partial, and three weak.

P24 and P25 were reviewed by technical experts, along with P23 discussed earlier in the section on indicators with strong performance. For more about the technical review process see the Annex, A2.1. For a discussion of some of the issues that arose with this indicator see section 4.2.1.

### 2.3.3 Indicators with the poorest performance

Scores on indicators asking about private requests for user data all averaged below 10 points out of a total 100 possible.

**Questions about private requests for user data (P10, 12, and 14):** In addition to P14 mentioned above, two other indicators also deal with private data requests.

P12 asks whether companies commit to **inform users when their data has been shared** in response to requests by private parties. Like P14 it saw no score for any company.

P10 asks whether the company **publishes its process for evaluating private requests** for user data. Only one company does so, receiving 50 out of 100 points.

**Transparency about content restricted when enforcing terms of service (F7):** As mentioned in the discussion of transparency reporting indicators, this indicator was one of two for which no company received a score.

## 2.4 Comparing Internet and Telecommunications Companies

Overall, Internet companies performed better than telecommunications companies, though the pilot also included twice as many telecommunications companies than Internet companies. Their average scores in the general human rights, freedom of expression, and privacy categories were higher than the average for telecommunications companies. With 45 indicators included in the final scoring, a company could earn on average 2.22 points (100/45) per indicator. For seven indicators, the average Internet company score was more than one full

point higher than the average telecommunications score. The table below includes the seven indicators and difference between average scores by sector.

**Indicators Where Average Internet Company Score is More than One Point Higher than Average Telecommunications Company Score**

| Indicator  | Difference between Average Internet and Telecommunications Score |
|--|--|
| P22: Does the company disclose and explain whether and to what extent it allows full and permanent account deletion?   | 1.47 points  |
| P17: Does the company publish clear information about when user information may be accessed by third parties (even when not actively shared with them?)                        | 1.39 points  |
| P11: Does the company commit to notify users to the extent legally possible when their data has been or will be shared with a government authority?                            | 1.39 points  |
| P4: Does the company maintain a public archive of changes to its privacy policy(ies)?  | 1.38 points  |
| F8: If the company removes, filters, or restricts access to content, does it explain whether and how it provides explanation to affected users?                                | 1.18 points  |
| G9: Does the company maintain a public archive of changes to its ToS?  | 1.10 points  |
| P13: Does the company publicly report at regular intervals the number of government requests received for user data, and the number (or percentage) of requests complied with? | 1.01 points  |

Telecommunication companies only scored marginally better than Internet companies on a few indicators, with the largest differential (0.35 points) being on indicator **G5**: Is there board-level oversight on how the company’s practices affect human rights, including freedom of expression and privacy?



## 2.5 What the data does and does not tell us

The results surface several themes which will be useful to consider when revising the methodology and determining how to present the full ranking to the public.

**This is a story of company disclosure and represents one step in the nascent ecosystem of advancing digital rights worldwide.** Most indicators focused on company commitments and disclosure of policies and practices. These results do not measure company action, but they do highlight whether and to what degree a company has made any public commitments to respect users' rights, whether it has instituted any policies and practices to implement those commitments, and whether or how it sees fits to communicate their commitments, policies, and practices to the public.

We ranked the companies based on publicly available information. In some cases during the pilot's company feedback phase, companies shared non-public information with us in the expectation that such information would increase their score. However, we did not factor this information into the score if we could not verify it with publicly available sources. Our rationale was that if users or other stakeholders such as investors, advocacy groups, and policymakers cannot find information about how the company respects free expression and privacy rights, they have little ability to hold the company accountable.

This ranking seeks to provide information to the public about how companies are approaching digital rights, based on what is possible to measure and compare at this point in time. It is our hope that over the coming years, RDR will be able to adapt its methodology to include new sources of research and data on company practices and impact. For example, right now, while some organizations have begun to test networks around the world for bandwidth shaping, filtering, and deep packet inspection, there is insufficient global test data on the services of all the companies RDR seeks to rank in order to include such data in the ranking this year. Nor were we in a position to establish local research networks to detect communications that registered users of services receive from a company in a specific country, but which are not discoverable by a researcher not based in-country with a subscription or account on a particular service. It is our hope that in the future, in collaboration with other research projects carried out by other organizations, we will be able to build more indicators addressing company practice and impact into the methodology as more data and research becomes available.

## Part 3. Main Questions for Methodology Revision

This section describes the primary issues we want to discuss with stakeholders and evaluate when revising the methodology. These include the scope of the ranking, the need to address differences in business models between companies, the scoring system, and the presentation of results. Each section includes questions that need to be resolved before we revise the methodology and implement the full ranking.

### 3.1 Scope

**As the breadth and scope of research is extensive, what is the best way to make use of finite resources to tell a clear and credible story about a set of companies operating all over the world?**

The pilot study covered 12 companies, but the inclusion of multiple services, languages, and subsidiaries dramatically increased the amount of work necessary to examine each company. The research and scoring processes were complex. Unless these processes are managed in a much more structured and precise way, it will be difficult to scale them to include more companies in Phase 1 and Phase 2 (devices, equipment and software) of the public ranking. Improvements in the back-end data and research management system, and accompanying project-management process, will help. But these improvements alone will not be sufficient.

**A key challenge is how to adjust the methodology to make it more manageable—and more accurate, credible and thus effective—for the full ranking, without over-simplifying in a manner that can also reduce accuracy and credibility. Possible steps include reducing the total number of indicators, reducing the number of subsidiaries, services, and languages covered, and/or conducting an in-depth local review on fewer indicators.** Each of these involves tradeoffs, and we welcome input to help us determine the appropriate balance.

During the company feedback stage of the research, companies raised questions of what was being assessed, whether the indicators and answer categories adequately captured how a company addresses users' rights in general, and what specifically we were looking for companies to do in order to achieve a perfect score on a given indicator. Some indicators included a list of elements to be evaluated. The answer categories for these questions assigned scores based on how many elements the company fulfilled. Some companies expressed concerns that this "checklist" style approach did not adequately capture the degree to which they explain their practices, particularly related to government requests. Other companies suggested that the methodology needs to clarify what best practice for individual indicators should look like in a practical sense.

Questions to Resolve:

- How should we select which services, languages, or subsidiaries to research for each company, keeping in mind resource constraints and the eventual inclusion of software and device companies?

- How might the answer categories be revised so that they more fully represent the spectrum of corporate practice without adding more layers of complexity?
- Should the methodology more explicitly permit consideration of information about company practices and policies that is generally relevant but for some companies may not fit neatly into any of the answer categories?
- Should we reduce the number of indicators in the methodology, and if so, what priorities should we set?

### 3.2 Scoring

**How do we develop a scoring and weighting system that integrates scores across services, languages, subsidiaries, and methodology categories (e.g., general human rights, freedom of expression, and privacy) in a clear and meaningful way?**

(See Annex 1 for details on the pilot study’s approach to scoring.)

Since local review of all of a company’s subsidiaries or operating languages was impossible given our resources, we adopted a **spot-check approach to local subsidiary and language research for 16 selected indicators**. The 30 other indicators were only researched at the group level. (See Annex 1.2 and 1.3 for full details.) We should consider how to approach this in the full ranking and beyond. Given the realities of how many companies operate (particularly telecommunications companies, whose user-facing operations tend to be at the subsidiary level, not the parent company), some members of our team have recommended adding substantially more indicators to the local review process. This would ensure that companies that make policies available on the operational (local country) level instead of the group level are not penalized by our ranking methodology. However, this would add significantly to the time and expense of researching each company for the ranking. (See also section 3.3 on Business Models.)

Also, evaluating the same subsidiaries or languages year after year could provide a consistent look at change over time in a company’s performance, but it could also incentivize the company to focus on improving its practices for those units included in the ranking, rather than across the entire company. Selecting different languages and subsidiaries year after year could decrease the risk that companies take the latter approach and merely focus on improving their ranking rather than their conduct, but it could also make it difficult to compare a company’s year-over-year performance, as each year’s score would reflect a different set of business units.

The **pilot scoring system weighted each indicator equally**. Since the three sections of the methodology—general human rights, freedom of expression, and privacy—had different numbers of questions, these sections were not weighted equally in the overall score. The privacy section has more than half of all the indicators, so it represents more than half of the

overall score. We intend to introduce weights into the full ranking and welcome discussion from stakeholders on the best way to do so.

Questions to Resolve:

- Does a spot-check approach that evaluates some but not all of the indicators at the (local) operational level provide meaningful results?
- Does a spot-check approach that evaluates different languages and subsidiaries each year provide meaningful results? Will this approach still make it possible to compare company performance year after year?
- Should we check the same languages/subsidiaries/services each year or use some kind of rotation system?
- Do some indicators deserve more weight than others? If so, which indicators require differentiation and in what direction?

### 3.3 Business Models

**How can the methodology accommodate varied corporate structures, operating contexts, and disclosure practices of different companies, keeping in mind that the ranking will eventually expand to include software, device, and networking equipment companies?**

#### *Corporate Structures*

Companies with a flatter organizational structure fared better in this methodology, which resulted in Internet companies outperforming telecommunications companies. Internet companies can serve a global user base out of their headquarters operations. This offers a central source for company policies and disclosure. Any decision to change or disclose policy can happen immediately, without depending on operating companies to implement such decisions. Legal and political pressures that affect disclosure are mostly limited to the home country, rather than to that of all operating companies.

Conversely, telecoms maintain operating companies around the world, and local operating company governance structures can vary. For example, Company I is essentially a holding company and places responsibility on operating companies to develop and implement policies. On the other hand, Company F develops principles at the group level but expects disclosure around policies, such as data protection, at the local level. Additionally, many parent companies do not offer telecommunications services themselves; only their operating companies do.

Questions to Resolve:

- How do we address concerns that the methodology might implicitly favor one sector over another? Should we revise the indicators so that they can be consistently applied across business models? Should we consider different weight matrices to compare companies with different business models? Should we opt for different scoring models for different

sectors? Or will that be difficult given that the services offered by traditional “telecoms” and “internet companies” increasingly overlap in the era of cloud computing and the Internet of things?

- How should holding company disclosure vs. operating company disclosure be considered, and what should our expectation of best practice be?
- To what extent should we encourage disclosure related to freedom of expression and privacy to take place at the group level as opposed to the operating level?
- How do we determine which indicators should be evaluated at the group level and at the operating level, given that companies themselves take different positions on disclosure and practice at these different levels?
- At what point should the parent be considered responsible for newly acquired subsidiaries or entry into new markets? A one year grace period may be fair as that is approximately the amount of time it takes for companies to begin reporting details in other annual reporting.

#### *Operating Environments*

Due to the need for physical infrastructure and personnel at the local level in order to provide service, telecommunications companies are more regulated than Internet companies and thus face greater constraints on their actions. The reality that legal environments differ around the world and that telecom operating companies need to maintain a physical presence in their countries of operation is one (but not the only) factor that dragged down many telecom scores. Company B, which was the highest-scoring telecom in the pilot, does not operate in high-risk countries, and free expression is constitutionally protected in its home market. Conversely, most of the other telecoms operate to varying extents in higher-risk countries where users’ free expression and privacy rights receive fewer legal and constitutional protections.

#### Questions to Resolve:

- Sustainability, in its own research, holds parent companies responsible for subsidiary actions when the parent exerts control over the subsidiary. If this ranking adopts a similar approach, how can we ensure that the results are instructive for companies and other stakeholders?
- Would it be useful for the narrative report accompanying the full ranking to include contextual information about the legal conditions under which companies operate and general policy issues on which they work with governments to change/address? Our sense is that this would be important to include in the narrative even if it is impossible to factor into the ranking scores themselves.
- Companies may be limited in their disclosure due to legal restrictions; however, general comments in a narrative report accompanying the ranking results can provide an

understanding of the extent to which the company could push for improvement. What are reasonable expectations for narrative reporting?

### *Company Disclosure Practices*

Researchers observed a difference in the way telecommunications and Internet companies disclose information. Telecommunications companies tend to publish formal policy statements and disclose information according to generally accepted reporting standards (e.g., corporate social responsibility reporting using the Global Reporting Initiative framework, annual sustainability reports or annual reports to shareholders). Internet companies, on the other hand, typically describe information that resembles policy positions in blog posts that are very difficult for researchers to locate. In several cases during the company feedback stage, Internet company representatives sent links to blog posts as evidence for particular indicators. In many cases these posts were several years old, dating back to 2010 or 2007. Typically, company policy statements are decided by a formal approval process that includes executive or board oversight. It is not clear that blog posts fall into this category.

In other cases, disclosure related to a company's policies or practices existed publicly on a third-party website (e.g., government regulator, industry group, multistakeholder initiative, or media account), but was not clearly disclosed on the company's own website. For example, one Internet company directed researchers to government audits for evidence of its practices. These audits were available online on the auditors' websites and mentioned on the websites of some civil society groups and in news reports, but researchers found no mention of them on the company's own website. In another case, the fact that a company had undergone and passed a full round of Global Network Initiative assessments, verifying that the company conducts human rights impact assessments among other practices spelled out in the GNI implementation guidelines, was disclosed on the GNI website but not by the company itself. In accordance with RDR's pilot methodology, that company received no credit for G1, which asks about human rights impact assessment, because researchers could find no company disclosure about the fact that the company actually has such processes.

Finally, questions arose around how to evaluate companies when they decided not to disclose certain information. In some cases, this represents a position the company has taken. For example, feedback from telecommunications companies suggested that some disclosure around data requests should be the government's responsibility, not the company's. In other cases, best practices around disclosure are still emerging, and companies appear to default to no disclosure until best practice has been established by others. In other situations, full disclosure may be impractical or illegal (e.g., data security practices or certain types of government requests for user data in certain jurisdictions). Some companies indicated an openness to discussing non-public, confidential information with RDR researchers but said they would not want the full detail released to the public.

### Questions to Resolve:

- What types of disclosure should be considered adequate for inclusion in the methodology? When does a piece of information published in a blog, or an executive

quoted in a media report, or a media account of a legal challenge mounted by a company, properly represent a committed company position?

- Should a date range be set (e.g., not older than three years) for non-formalized policy commitments?
- What should our expectation of disclosure be where the information would not be public for valid reasons? Or where the disclosure is public, but it is very difficult to find and company representatives do not direct researchers toward it?
- Is there room in the methodology for companies to release confidential information to RDR for evaluation? Would inclusion of such information bias the results even further towards North American and European companies that tend to be more comfortable talking to researchers on issues related to freedom of expression and privacy? Is it possible to admit such information without jeopardizing the research transparency that the ranking intends to offer?

(See sections 7.1 and 8.4 for further feedback from investors and other stakeholders on these questions.)

### **3.4 Presentation of Results**

#### **How do we present the results in way that accurately conveys the scope of the ranking?**

This ranking covers a variety of nuanced issues within the sphere of digital rights. We want to ensure that the stories this data tells are accurate and informative, yet also accessible to a general audience. One key adjustment for the full ranking is to ensure the final dataset captures sub-scores for services, languages, and subsidiaries. The pilot dataset does not include sub-scores, which limits our ability to explain and fully analyze why companies scored as they did or to detect trends. If the methodology evolves to include qualitative information or narrative feedback from companies that we cannot publicly verify, we must also consider how to display it alongside the quantitative ranking data.

Questions to Resolve:

- How can we best present the quantitative ranking data along with narratives to put the data in context?
- Are bar charts an effective means of visually communicating the results? What other visualization techniques would be useful?

(See Section 8.6 for some suggestions offered during the stakeholder consultation meetings.)

## Part 4: Indicator Assessments

This section provides details on indicator-specific issues or challenges that arose during the research process, as well as issues that company representatives identified in their feedback. Answers to questionnaires about the local relevance of the pilot results, sent to civil society activists in six different countries, also helped us to identify potential incongruences between pilot results and local experience with the companies that we reviewed.

When reviewing the indicators discussed in this section, please consider the following questions:

- Are we asking the right question to elicit meaningful results about a company's disclosure?
- Does the question apply well enough to both Internet companies and telecoms?
- What indicators/answer categories should we consider deleting or revising?
- What indicators/answer categories we should consider adding?
- Should we raise the bar for all companies? Are there new standards we should be trying to set?

### 4.1 The Two Most Problematic Indicators

Two indicators in the pilot methodology proved especially difficult, and were therefore considered experimental. Both underwent dramatic changes throughout the methodology development process as we explored different approaches to these issues of high importance to stakeholders we consulted. This sub-section will discuss those two indicators in greater detail than the others given their importance for specific stakeholder groups.

#### 4.1.1 Identity Policies

The “v3” methodology<sup>3</sup> used in the pilot asked the following question about a company's identity policies:

**G10.** Is there evidence that the company's identity policy, and measures taken to enforce it, increases users' exposure to human rights violations or otherwise has a negative impact on users' freedom of expression or privacy?

Answer categories:

- No evidence – There is no evidence of controversy related to the company's identity policies.

---

<sup>3</sup> <https://rankingdigitalrights.org/project-documents/phase-1-pilot-methodology/>



- Moderate – Moderate risk/evidence of negative impacts
- Significant – Significant risk/evidence of negative impacts
- High – High risk/evidence of negative impacts
- Severe – Severe risk/evidence of negative impacts
- N/A

Throughout the methodology development process, we struggled to develop an indicator that would effectively address identity policies across a range of different types of companies and services. One challenge has been formulating the indicator in a way that fits telecoms and Internet companies. The pilot language was meant to enable researchers to draw upon Sustainalytics' in-house system for identifying and tracking public controversies that arise around particular companies. However, beyond a couple of very high profile Internet companies, there is simply not enough media coverage (or any other kind of public reporting by human rights groups or other specialized groups that generate research and reporting) about the link between identity policies or requirements of all the companies covered in the pilot and direct privacy (and free expression) harms to users. **We found that the inability of a researcher to find “evidence” was not a useful indicator of good or bad practice by the company in most cases. Therefore this indicator was removed from the pilot’s scoring.**

Earlier versions tried different approaches to identity.

The original identity-related indicator in v1 of the methodology published in February 2014<sup>4</sup> asked the following question:

G7: Does the company allow users to be anonymous or (if the service’s core function genuinely depends on some degree of identity in order to deliver value to users) use persistent pseudonyms?

The next revision published in May 2014 (v2)<sup>5</sup> took a different approach:

G8: Does the company allow anonymous or pseudonymous use of the service?

Elements to be assessed in scoring:

- If anonymous or pseudonymous usage is permitted with no account verification;
- If anonymous or pseudonymous usage is permitted after an account has been verified using another potentially anonymous service (e.g., email activation);
- If anonymous or pseudonymous usage is permitted when using a third-party identity service that allows pseudonyms;

<sup>4</sup> <https://rankingdigitalrights.org/wp-content/uploads/2014/02/rdrmmethodologyfeb28.pdf>

<sup>5</sup> [https://rankingdigitalrights.org/wp-content/uploads/2014/05/RDRmethodology\\_v2\\_May28-FINAL.pdf](https://rankingdigitalrights.org/wp-content/uploads/2014/05/RDRmethodology_v2_May28-FINAL.pdf)

- If anonymous or pseudonymous usage is permitted when using a third-party identity service that enforces a real ID policy;
- If the ToS require “real name” usage but the company does not require users to verify by submitting government issued identification to company staff;
- If users must submit a government-issued ID upon request or face account termination;
- If users are required to submit a government-issued ID at time of service registration.

A major problem with the v2 approach is that it is not applicable to telecommunications services, only to Internet platforms. Perhaps this question should be applied exclusively to Internet platforms, just as G12 (on Deep Packet Inspection) applies only to telecoms. Some stakeholders have continued to emphasize to us, throughout the methodology development process as well as during civil society questionnaires, that Internet companies’ identity policies—and how they are implemented—can have a serious impact on users, particularly in countries governed by authoritarian regimes or where sectarian violence and civil war takes place.

#### 4.1.2 Net Neutrality

Questions related to Net Neutrality evolved even more dramatically over time. In the pilot methodology:

**F9. Does the company disclose its policies and practices affecting net neutrality?**

Elements to be assessed in scoring:

1. Practices to prioritize certain content
2. Contractual agreements to prioritize content

Answer categories:

- Strong – The company states that it does not prioritize certain content or enter into contractual agreements to do so.
- Partial – The company discloses that it prioritizes some content and/or enters into contractual agreements to do so and provides justification.
- Weak – The company discloses that it prioritizes content/has contractual agreements to prioritize content, but does not explain why.
- None/no evidence
- N/A

In February 2014, v1 of the methodology did not use the term “net neutrality”, in part to avoid getting bogged down in debates about definitions of the term:

F11. If the company uses techniques to prioritize transmission or delivery of different types of content (e.g., bandwidth shaping or throttling) does it disclose:

- a. 50% the use of such techniques.
- b. 100% the purpose of their use.

In May 2014, v2 revised the question substantially and divided it into two, reflecting stakeholder feedback about how to address net neutrality issues pertaining to Internet platforms as well as telecommunications providers.

For telecommunications services:

F9. If the company prioritizes transmission or delivery of different types of content (e.g., bandwidth shaping or throttling) does it disclose the use and purpose of such techniques?

Elements to be assessed in scoring:

- If it does not carry out content prioritization;
- If it discloses that it carries out content prioritization;
- If it discloses the purpose of any content prioritization.

For Internet services:

F10. Has the company entered into agreements with mobile and/or fixed line Internet service provider(s) for prioritization or special access by subscribers, and if so does it disclose basic information about the existence and nature of such agreements?

Research experience and discussions with companies suggest that reverting to questions more along the lines of v2 might bring more clarity to researchers about what they are supposed to evaluate, as well as clarity on the part of companies about what exactly they are being evaluated on. Civil society respondents to our questionnaire about the pilot results (all based in developing countries, as described in the beginning of Part 6 and also mentioned in Part 2) flagged this indicator—and the concept of Net Neutrality generally—as challenging to explain to local audiences. For this reason one respondent suggested “rewriting this criteria to focus on the detail and clarity of disclosure of practices.”

Note that local technical testing to detect bandwidth shaping across dozens of locations and services around the world was not deemed feasible within the project’s current resources, nor within the capacity of the project’s existing research partners.

## 4.2 Other Indicator-Specific Comments

This section discusses groupings of indicator types on which further stakeholder input would be extremely helpful. Answer categories and elements for consideration are not included here due to length considerations. Please refer to the [Phase 1 Pilot Methodology document](#) for those details.

### 4.2.1 Human Rights Impact Assessments

**G1.** Does the company regularly conduct human rights impact assessments (HRIA) addressing how the company's products and services affect the freedom of expression and privacy of its users?

**G2.** Is the company's HRIA process comprehensive?

**G3.** Is the company's HRIA process assured by an external third party?

Key issues:

- Companies engage in a variety of due diligence practices, and some companies asked whether these indicators would capture those efforts (and third party assurance of them) even if they weren't explicitly called HRIAs. (Note that the researcher guide instructed researchers to include privacy impact assessments.)
- G1 asked about company practice, but the answer categories focused on disclosure. It was our position that if an internal due diligence process takes place but no public mention of it occurs, then it does not exist for the purpose of this ranking. However the question arose whether these indicators will only consider disclosure of HRIA information found on company websites, or if disclosure from other organizations is sufficient. For example, researchers found information about some company HRIAs from the website of a multi-stakeholder initiative but no disclosure by the company itself. This led to companies receiving no credit on G1 but some credit on G2.
- Respondents to the civil society questionnaires flagged low scores on G1 for certain companies as not accurately reflecting due diligence processes that they themselves had observed, or even participated in when companies reached out to them for advice on particular policies, practices, or markets. None of these engagements are disclosed by the companies or by other participants.
- Conversely, other respondents objected to scores that gave some degree of credit to companies for having an HRIA process, pointing out that while HRIAs might take place for other markets, there was no evidence that such processes exist in relation to company operations in their own country.

## 4.2.2 Deep Packet Inspection

**G12.** If the company intercepts, examines, or filters data packets transmitted by or to its users, does it disclose whether it does so?

Key issues:

- We evaluated this question only for telecoms. This indicator was meant to address whether companies disclosed use of deep packet inspection. Note the challenge is that DPI can be used for legitimate (e.g., network management) and rights-violating purposes (e.g., broad censorship and surveillance).
- This indicator focused solely on disclosure and did not take a position on best practice. For example, a company that disclosed its use of DPI to comply with government requirements for wide ranging censorship and blanket surveillance of users could earn a strong score just for disclosing that fact, based on the current wording of the question. One could argue that disclosure in and of itself is a step in the right direction in terms of addressing the fundamental problem of users' rights being violated via telecoms companies in accordance with government requirements, which might be most appropriately addressed at the legal/political level.
- The greatest problem in assessing this question was making sure that researchers had sufficient understanding of the differences between disclosure of data collection that may or may not involve DPI, and disclosure of DPI usages specifically. Civil society survey respondents also flagged this indicator as difficult to explain to their own domestic audiences.
- Along with bandwidth shaping in the net neutrality question, it is beyond the resources of this project, and the technical capacity of existing research partners, to verify the presence or absence of DPI across dozens of operating companies across the world.

## 4.2.3 Terms of Service/Privacy Policies

**G7.** Are the company's Terms of Service freely available, without having to sign up or make a purchase, in plain and accessible language?

**G8.** Does the company commit to provide meaningful notice to users when it changes its ToS?

**G9.** Does the company maintain a public archive of changes to its ToS?

**P2.** Does the company have a privacy policy or policies that are freely available, without having to sign up or make a purchase, in plain and accessible language?

**P3.** Does the company commit to provide adequate and meaningful notice to users when it changes its privacy policy(ies)?

**P4.** Does the company maintain a public archive of changes to its privacy policy(ies)?

Key issues:

- Several telecoms do not offer services at the group level, so these indicators may not be appropriate for group-level review in that sector. Internet companies reviewed in the pilot do provide services at a global level, so it would be appropriate to evaluate these indicators for them at that level.
- Regarding the existence of an archive of previous versions of policies, some companies suggested that it was more important for users to understand why aspects of the policies changed rather than simply see what changed, adding that an archive may not be the most user-friendly way to communicate policy-related information to users.
- It was also pointed out that indicators did not consider whether companies engage with users about proposed policy changes prior to making them.
- Civil society questionnaire respondents affirmed the importance of making privacy policies and terms available in local languages. One respondent whose country and predominant language were not selected for the pilot's local/language research process complained that several of the companies receiving strong marks on Tos/Privacy policy accessibility do not make them available in that country's predominant language. Due to civil society's heavy dependence on social media and mobile services, in a country where the press is not considered free by international human rights groups, the respondent felt that the global scores for those companies was inconsistent with national-level experience.
- A further challenge exists in defining what constitutes 'plain and accessible' language.

#### **4.2.4 Freedom of Expression/Privacy Commitments**

**F1.** Does the company provide evidence that it supports implementation by staff at all levels and throughout the company of its freedom of expression commitments?

**P1.** Does the company provide evidence that it supports implementation by staff at all levels and throughout the company of its privacy commitments?

Key issues:

- This question as worded assumed companies had made commitments to freedom of expression and privacy. (If they had not, the company received no score on this indicator.) The elements evaluated in this question were whether the company had an officer with managerial responsibility for freedom of expression/privacy, provided regular employee training on freedom of expression/privacy, and reported on freedom of expression/privacy issues.

- Companies rarely reported the existence of company training, and more researcher guidance is necessary to determine what constitutes reporting on issues.
- Finally, we should determine to what degree these elements sufficiently indicate company commitments, or if there are other ways to measure such commitment. Another approach could focus on how companies publicly discuss what they do to enhance free expression and privacy.

#### 4.2.5 Government Requests

**F3.** Does the company publish information in plain and accessible language in its Terms of Service, or in another prominent location, about its process for evaluating and responding to government requests to remove, filter, or restrict access to content?

**F5.** Does the company publish data at regular intervals about government requests it receives to remove, filter, or restrict access to content, plus data about the extent to which the company complies with such requests, if permissible under law?

**P9.** Does the company publish its process for evaluating and responding to government requests for stored user data or real-time communications, including the legal basis for complying with such requests?

**P13.** Does the company publicly report at regular intervals the number of government requests received for user data, and the number (or percentage) of requests complied with?

Key issues:

- We should consider how the checklists in these indicators align with company disclosure practices.
- One challenge in assessing company scores on indicators F3 and P9 was determining the level of detail that we expected from companies in explaining their processes for dealing with government requests.

#### 4.2.6 Requests from Private Entities

**F4.** Does the company publish information in plain and accessible language in its Terms of Service, or in another prominent location, about its process for evaluating and responding to requests made by private entities (including private individuals) to remove, filter, or restrict access to content?

**F6.** Does the company publish data at regular intervals about requests from private entities to remove, filter, or restrict access to content, plus data about the extent to which the company complies with such requests?

**P10.** Does the company publish its process for evaluating and responding to private requests for user data?

**P12.** Does the company commit to notify users when their data has been shared in response to requests made by private parties?

**P14.** Does the company publicly report at regular intervals the number of requests made by private entities for user data and the number (or percentage) of requests complied with?

Key issues:

- The term, “private requests” is intended to include requests made by any private entity without going through a court or government authority. In one case, the researcher guide used in the pilot was inconsistent in stating that “private requests” included civil subpoenas. Private requests include DMCA or EU E-Commerce Regulations takedown requests and requests by intellectual property rights holders to identify account holders. Private requests can also potentially include informal requests made by private parties, such as requests made by families of a deceased account holder directly to a company. However the information in the methodology document itself needed to be much clearer.
- Some telecommunication companies told us in their feedback that they do not respond to (or receive) requests from private entities, but they also did not state this explicitly in public documents. A larger question is the degree to which the methodology expects companies to state publicly what they do not do.
- Also, we need to make sure that these questions capture the need for greater company transparency around self-regulatory regimes, whereby a group of companies will agree to restrict content flagged or blacklisted by non-governmental or quasi-governmental “watchdog” organizations.

#### **4.2.7 Other Content Restriction Requests**

**F7.** Does the company publish information at regular intervals about content removed, filtered, or restricted for violating the company’s Terms of Service for reasons unrelated to government or private requests covered by F5 and F6?

Key issue:

- Some telecom companies said that this indicator is not applicable to telecommunications companies.

#### **4.2.8 User Notification**

**F8.** If the company removes, filters, or restricts access to content, does it explain whether and how it provides explanation to affected users?



Key issues:

- This indicator requires additional guidance on what constitutes acceptable disclosure.
- Civil society respondents pointed out cases in which telecoms studied do in fact provide user notification pages when content has been blocked or filtered. However these pages can only be found when a user attempts to visit a filtered website from that particular telecommunication company's local service in the country where it operates. Evidence of these notification pages tends to be collected and published by activists and researchers. The telecoms themselves do not generally release information about how they communicate with users who try to access blocked or filtered content. This example, among others, once again raises the question of what types of publicly available information should be considered by researchers.
- Due to resource constraints as well as security concerns we ruled out one solution: engaging local researchers in each country selected for local spot-checking, requiring them to have an account or subscription on the services being researched. Researchers would then test the services by attempting to access content likely to be blocked and documenting the result, or posting content likely to be removed and documenting whether they receive any kind of notification or explanation from the company.

**P11.** Does the company commit to notify users to the extent legally possible when their data has been or will be shared with a government authority?

Key issue:

- Some companies explained that employees process government requests without full knowledge of why the government seeks a user's data. Thus, even in situations where the company was legally permitted to disclose that a customer's data has been shared with the government, it likely would not since it would not want to hinder a lawful investigation.

#### **4.2.9 Data Collection and Retention**

**P5.** Does the company disclose what personally identifiable information (PII) about the user (including metadata) is collected, how it is collected, and why?

**P6.** Does the company disclose how long personally identifiable information about the user (including metadata) is retained, what data may be retained for longer periods in an anonymized form, and why?

**P8.** Does the company disclose what personally identifiable information (including metadata) may be shared with which government entities and why?

- The methodology defined PII, generally, but it may be more helpful to provide a list of specific information that we consider PII and evaluate how companies handle it. For example, companies that included disclosure on this topic described the data they collect and what they did with it, but their documentation did not typically differentiate between PII and non-PII. In cases where they do make such a distinction, it is important to understand how they define PII and consequently offer greater protection, so that we can compare with our own definition of PII. For example: we regard IP addresses as PII, but not all companies do.
- Moreover, there is an ongoing debate among experts as to whether ‘anonymized’ data truly cannot be connected back to individual users.<sup>6</sup>

#### 4.2.10 Data Location

**P7.** Does the company publish information about which legal jurisdictions user data is known, or highly likely, to be subject to while in storage and/or in transit?

Key issue:

- Some companies suggested that it would be impossible and impractical for companies, particularly telecoms, to collect and display this data. In addition, revealing the location of data in transit may be counterproductive for privacy, since governments may seek access to such information.

#### 4.2.11 Third-Party Access to Data

**P15.** Does the company publish clear privacy and data protection requirements for third parties that may have access to personally identifiable information (e.g., app and widget developers, advertisers, etc.)?

**P16.** Does the company provide a comprehensive list of third parties with which it shares users’ personally identifiable information, indicating what information it shares with which specific third party and for what purpose?

**P17.** Does the company publish clear information about when user information may be accessed by third parties (even when not actively shared with them)?

**P18.** Does the company publish clear information about whether it collects user data from third parties, and if so, how and why it does so?

Key issues:

---

<sup>6</sup> See for example <http://www.sciencemag.org/content/347/6221/468.summary>

- The similar wording in P17 and P18 is confusing, and companies may not always differentiate between these practices. Some telecommunications companies suggested these questions are not applicable to them.
- In P18, greater clarity is needed on what we mean by “how” a company collects data. For example, companies may list where they collect data from (e.g., cookies) but it is unclear whether this would satisfy as an explanation of “how.”

#### 4.2.12 User Controls

**P19.** Does the company allow users to opt in or opt out of the collection of personally identifiable information (PII) not essential to providing the company’s core services?

**P20.** Does the company allow users to opt in or opt out of the sharing of personally identifiable information not essential to providing the company’s services?

Key issues:

- These indicators are confusing given their extremely similar wording. More researcher guidance is necessary to explain the difference between collecting and sharing data and to define information that is “not essential.” It is also unclear if companies structure their user controls based on the collection and sharing of user data.
- If companies present these options to users at the time they sign up for the service, would we consider this publicly available? Moreover, can users be seen as ‘opting in’ by merely registering for a service?
- The answer categories generally did not map to how companies discuss user controls. They focused on opt-in/opt-out functions, but some companies gave users the ability to adjust their own settings for sharing personal data.

**P21.** Are users able to view, download or otherwise obtain, in user-friendly formats, all of the personally identifiable information about them that the company holds?

- We should define “user-friendly.” We can also consider explaining legal requirements that may mandate companies in some jurisdiction (e.g., EU) to do this.

**P22.** Does the company disclose and explain whether and to what extent it allows full and permanent account deletion?

- We should clarify what constitutes deletion. For example, does this include deletion of all of a user’s data (which may not be legally possible in some environments)? Moreover, for telecom companies account deletion may be less self-evident a process than it is for Internet companies, as they do not all by default have online user portals.

### 4.2.13 Security

**P23.** Does the company deploy strong industry standards of encryption and security for its products and services?

Key issues:

- How can we structure this question in a way that applies to Internet companies and telecoms while still providing meaningful results, considering that companies may not reveal all of their security/encryption practices? We want to incentivize companies to use more secure technology, but legal requirements or industry realities (e.g., telecoms that still use inferior 2G technology) may limit their ability to do so.
- How can we evaluate the validity of industry codes of practice? ISO standards are clear and reputable. Companies highlighted membership in GSMA or Trust-e certification, but it's unclear the degree to which these agreements have teeth.

**P24.** Does the company publish information to help users defend against hacking and phishing attacks?

Key issues:

- The elements evaluated for this indicator (e.g., two-factor authentication, user notification about account activity, disclosure of known security vulnerabilities, and publication of materials to educate users) may be more applicable to Internet companies than for telecoms.
- Legal requirements in some areas may require disclosure of vulnerabilities or breaches. In this case, would we look for a company to state publicly that they abide by the particular law? Companies may make a general statement that they abide by the laws in their operating environment, but would we want to see mention of specific laws? Or would we look for the mere statement affirming that vulnerabilities and breaches will be disclosed?

**P25.** Does the company regularly conduct credible and independent security audits on its technologies and practices affecting user data?

Key issues:

- In some cases, company feedback suggested that these audits occurred, but information about them was not publicly disclosed.
- Researchers sometimes found it difficult to determine which products and services fall under a particular audit.

## Part 5: Company Engagement

The previous two sections of this report have discussed in considerable detail specific company reactions to specific indicators, and comments on aspects of the research process. This section provides broader observations about themes and trends that arose in our interactions with companies. Drawing on those observations, it also offers some ideas for a company engagement strategy after the release of the ranking results.

### 5.1 Company willingness to engage

It is interesting to note that the top seven companies (in fact, all of the companies that scored above 20 points) provided at least some substantive information about their company's policies and practices during the pilot's feedback stage—either verbally on a conference call, as a written submission, or both.

The lack of engagement on the part of the poorest performers – even if just to confirm whether we located all the relevant information they have already published, and to point out any errors on our part—does not necessarily mean that non-responders will automatically score lowest in the full public ranking.

Also it is important to note that some companies that chose not to participate in the feedback stage of the pilot did communicate with us about their reasons. The company that ranked lowest over all (Company L) told us that they would be open to future communication with the project and recognized the importance of the issues covered in the ranking to their industry. Ultimately, however, the company felt it more important to address these issues within the context of their own due diligence processes and operations. The company stated that it had identified countries of risk where due diligence is needed, but did not want to make the specifics of such processes public. It made a general point that licensing restrictions and requirements may hamper company disclosure on the issues researched by RDR.

Nonetheless, it does appear that a company's willingness to engage with the Ranking Digital Rights research process is a meaningful indication of a company's broader level of capacity and comfort in engaging with stakeholders on human rights questions generally, and matters related to users' freedom of expression and privacy more specifically. One individual from a company that participated in the pilot study feedback process noted that the results would help them build an internal case for more systematic disclosure, as well as for the establishment of formal risk assessment processes.

Idea for engagement:

Work with partner organizations and academic institutions to convene invitation-only meetings to discuss best practices, making special effort to have a mix of strong and poor performers in the room. Invite companies that scored well on certain indicators to share their experience, alongside other organizations that worked with those companies to help them build policies and practices that fared well in the ranking. (Indeed, it is important to note that all of the companies

that scored above 20 points have worked with a range of civil society organizations, industry groups, consultants, policymakers, and multistakeholder initiatives in order to build the practices and policies they have in place today.) Some parts of these discussions should focus on elements of the ranking that one might describe as “low hanging fruit”: indicators on which most if not all companies should be able to improve regardless of the legal and political contexts in which they operate.

## **5.2 Variations in disclosure and reporting style**

As mentioned in previous sections, some companies we examined were more familiar than others with the expectations common to socially responsible investors (SRI) and environmental, social and corporate governance (ESG) researchers that company information disclosures take place in annual reports, sustainability reports, CSR reports, and other official company documents. Some companies habitually make revelations, policy announcements, and disclosures in blog posts or executive comments to the media. Feedback from some of those companies reflected a certain level of indignation that the research team had not found all such relevant statements and postings. Other companies, due to regulatory requirements or investor expectations in their home markets – or due to the fact that their businesses have been in operation for relatively longer periods of time – are accustomed to providing more of a “one stop shop” for researchers and other stakeholders seeking comprehensive information about their policies and practices. On the other hand, many of the companies that are less organized about certain types of disclosure and reporting more familiar to the SRI and ESG world are also leaders when it comes to a new and innovative form of disclosure: “transparency reporting”.

Idea for engagement:

The Ranking Digital Rights team could convene a joint workshop with the GNI and Industry Dialogue, and the Open Technology Institute’s transparency reporting research team, perhaps also in conjunction with the Freedom Online Coalition’s Working Group 3 which addresses questions of transparency, examining differences in company disclosure and transparency practices as identified by RDR. The goal of such a workshop would be to: 1) identify and clarify how and why different types of disclosure and transparency are meaningful and desirable; 2) identify what the current best practices are across different sub-sectors and regions; and 3) identify gaps on which all should be expected to improve; 4) identify obstacles to improvement as well as strategies for overcoming those obstacles.

## **5.3 Views on independent assessment**

The methodology places value on whether a company undergoes an independent, third-party assurance process on its internal human rights impact assessments (including internal privacy assessments) in order to verify whether the company undertakes human rights due diligence in a meaningful way. It also expects companies to disclose that they undergo third-party security audits. Some companies raised questions about what types of assurance and auditing would “count” for full credit in the RDR framework.

Idea for engagement:

Convene a workshop with the GNI, Industry Dialogue, and other experts on human rights due diligence and assurance to help clarify stakeholder expectations as well as company understanding of best practices in internal assessment, external audits, and independent assurance processes.

#### **5.4 Regulatory and political context**

A number of companies expressed concern about regulatory and political factors that they believed prevented them from performing as well on specific indicators as they might otherwise have done. We do not believe it is possible to adequately “factor in” policy and legal environments to the ranking equation. However we do believe that there is a story to tell about what types of government policies, laws, and regulations clearly prevent companies from performing well on specific indicators to which human rights risks can clearly be linked. (RDR has developed a set of human rights risk scenarios, available at <https://rankingdigitalrights.org/project-documents/risk-scenarios>, to facilitate such a discussion.)

Idea for engagement:

A workshop that brings companies, government representatives, and civil society activists together to discuss specific points of human rights “failure” identified by the ranking, might help to facilitate policy reform recommendations as well as advocacy strategies by civil society as well as companies.

## Part 6: Civil society adoption

Review by civil society stakeholders was not integrated into the research process that generated companies' scores. However as previously mentioned in earlier parts of this report, we did send questionnaires to six civil society representatives in different countries generally considered to be part of the "Global South". We felt that this was important in order to gain a sense of how the ranking results would be viewed from a local perspective and how the information might potentially be used for advocacy in different countries and regions. Responses pertaining to some of specific indicators have been incorporated into Part 4. Other responses were extremely detailed: sharing them would enable readers to identify which companies were reviewed. We will therefore use those internally to inform our methodology revision process but not share them on the record.

We also asked respondents some general questions, specifically: how the ranking results might be useful to whom in their countries and regions, and how we can maximize the ranking's usefulness to them.

### 6.1 Presentation and data

Respondents stressed the importance of providing raw data for download in open formats. Many also stressed the need for clear visual presentation of results, as well as interactive tools enabling users to drill down. One respondent suggested that animations and "white board" style YouTube videos are an effective way to reach people in their country. Others pointed out that given connectivity problems in their countries, having a downloadable PDF and even printed version is also very important. Indeed, several respondents made clear that having hard copies of the ranking results would substantially increase their impact, especially among government officials.

### 6.2 Language

Respondents stressed the importance of translating the report and data into local languages if the ranking is to be used effectively in countries where English is not widely understood. This is a natural corollary to the project's expectation that companies will communicate with users in a language they understand. Translation will be a challenge for RDR given that we do not presently have resources to pay for translation. Thus we will need to forge strategic partnerships with other organizations interested in helping with translation—and ideally, help them find funding to support the translation work.

### 6.3 Target audiences

#### *Government*

Some respondents named as target audiences for this ranking specific government ministries in charge of communications, information, press, national security and law enforcement. One respondent pointed out that their country is in the process of drafting digital security and privacy



laws, making information about best practices extremely relevant. Another respondent expressed the hope that the ranking would help to bring regulators' attention to the importance of disclosure and transparency, which have been largely absent from regulatory discourse to date.

#### *Companies / Industry associations and self-regulatory bodies*

One respondent pointed out that associations of mobile operators and ISPs "would be interested in the ranking as they work closely with companies in developing best practices and ensuring that they are in compliance with legal norms and they work closely with the government as well."

#### *Academic researchers*

Ranking results and the granular data behind those results were viewed as being valuable for research reports that can have an impact on policy discussions.

#### *Civil society advocates*

As one respondent put it, the ranking has the potential to provide raw materials for more effective "evidence based advocacy" directed at companies.

## **6.4 Outreach and advocacy**

In addition to making the ranking report and its data available in a range of languages, respondents stressed that if the ranking data is to be used effectively, local outreach strategies are also key. Ideas included:

- "Bring these companies into regional or country level dialogues with the civil society, academia and research, private sector and governments through seminars and conferences"
- "Submissions to relevant government departments and bodies with recommendations for the uptake of ranking indicators onto the national agenda."
- "Adoption of the ranking by industry bodies such as [body and country redacted] and the Cellular Operators of [country redacted]. Once adopted – key indicators could be incorporated into relevant member codes etc."
- "News items and journal articles discussing the findings of the rankings."
- "Consistent online and radio conversation around this topic would encourage subscribers to discuss the issues. Enlightenment on their legal rights should also come through publications and advertorials that will create such awareness."

One respondent was especially succinct and clear about the advocacy ecosystem that might be developed around the ranking in her country:

“The adoption of stronger company practices that protect users’ rights to privacy and freedom of expression depends on a number of actors and factors. The government needs to create enabling policy and regulation, companies need to adopt and be held accountable to these practices, industry bodies need to promote and adopt these practices, users need to demand and create a market for these practices, and civil society and academia need to research, promote, and justify the relevance of these practices.”

Given the resource constraints of this project, local outreach would likely need to be carried out by local partner organizations to which (we hope) funders could provide direct support.

## Part 7: Investor feedback

After circulating a draft pilot report, we consulted with investors as well as other stakeholders at several meetings in late February and early March 2015. (See Part 8 for a full discussion of overall outcomes from those meetings.)

### 7.1 Disclosure vs. performance

Like other stakeholders, investors told us that if the ranking is going to focus primarily on disclosure, RDR needs to be very clear about that up front. One executive with a socially responsible investment fund pointed out that investors are fundamentally interested in information about actual performance. To the extent that disclosure is a proxy for performance, information about disclosure is useful, but the connection between the two also needs to be clearly explained in the ranking's introductory materials, analysis, and related engagement.

Another executive with a different socially responsible investment fund articulated a view that the transparency and accountability fostered by strong disclosure practices is “the gateway” to improved performance. RDR's value is demonstrating to companies that they have an obligation to users and customers to disclose certain information. Investors also expect disclosure on issues they consider “material” for the business in which they are investing.

### 7.2 Materiality

For the purposes of this project, “materiality” refers to the salience of particular factors that may create risks or opportunities for a company. Disclosure on material issues relates to how companies evaluate material issues.

Investors expressed the hope that RDR can make a clear connection between the issues it focuses on— freedom of expression and privacy—and investor risk. The project can help to educate investors as well as the ICT sector more broadly about how company respect for users' freedom of expression and privacy provides business opportunity, while threats to the same rights can pose business risks. One investor suggested that wherever possible in the project's narrative reporting, it would be helpful to provide concrete examples of how threats to users' rights have hurt businesses, as well as how demonstrations of respect for users' human rights have benefitted companies.

One investor suggested that in deciding which companies to rank, the RDR team should consider companies with large market cap and large investment holdings. In addition to geography and risk factors, investors would like to see an evaluation of companies that are part of most investors' portfolios.

## Part 8: Stakeholder Consultation Outcomes

From mid-February through early March 2015 we held five stakeholder consultations in New York, Washington DC, Berlin, Budapest, and London. Invited participants included academics, technologists, human rights advocates, business and human rights experts, investors, and funders. These meetings were held separately from company consultations conducted during and after the pilot. During these consultations, we received invaluable feedback on broad questions about the project's focus and framing, research approaches, and issues related to specific indicators. All of this feedback will inform efforts in March-April 2015 to revise all aspects of the project including scope, focus, indicators, research process, and communications strategy.

During the course of the consultation period, it also became clear that fundraising targets necessary to support a ranking of 20 or more companies could not be reached. Available funds would likely only support the ranking in 2015 of 10-15 companies (the exact number depending on the extent to which the indicators and research process can also be simplified). At the final meetings in Budapest and London, stakeholders were asked for their views on what the project team should prioritize if the 2015 ranking is constrained to approximately a dozen companies. While it is impractical to provide a full summary of all suggestions, below is a summary of several key suggestions.

### 8.1 Simplify the ranking

Given the project's ambitions and limited resources, for the first year at least, various stakeholders suggested the 2015 public ranking "start simple and build from there." While the many complexities included in the pilot ranking reflect the realities of the sector, too much complexity makes it difficult for stakeholders to ascertain the reasons behind specific company scores without elaborate explanation. Simplifying the ranking may affect decisions about the extent and scope of, for example, local/language research and number of services examined.

### 8.2 Name and frame the project differently

A number of stakeholders expressed the view that calling the project "Ranking Digital Rights" may create unrealistic expectations given that the methodology focuses primarily on disclosure. Several participants suggested that it is important to describe the ranking as a measurement of companies' transparency and disclosure rather than a ranking of how companies protect their users' rights. In any case, language used to introduce the project on its website and related promotional materials should clarify what the ranking will—and will not—examine. Importantly, the relationship between company disclosure and good practices should also be explained more explicitly. Alternative names might focus more on disclosure and standard-setting. Suggestions included "Digital Rights Standards Project" or "Digital Rights Disclosure Project" – the latter inspired by the highly successful Carbon Disclosure Project.<sup>7</sup>

---

<sup>7</sup> <https://www.cdp.net>

### **8.3 Emphasize standards**

Many expressed the view that the project's most important contribution – especially in its first year or two – will be in establishing clear standards that all companies should be expected to achieve. Which companies score higher than other companies will be much less important, especially if the number of companies ranked is likely to be limited.

### **8.4 Reward good practice in addition to disclosure**

Many stakeholders made strong arguments that the indicators should be reviewed and revised to ensure that disclosure of good practice will always be ranked more highly than disclosure of poor practice. At present, the pilot methodology takes a mixed approach: some indicators merely evaluate the level of disclosure while other indicators evaluate the quality of the policy or practice disclosed in addition to whether and to what extent disclosure takes place.

### **8.5 Sharpen geographical focus**

Stakeholders from a range of backgrounds expressed a desire to see more analysis of the legal, regulatory and other jurisdictional factors that affect companies' levels of disclosure as well as their policies and practices. One participant suggested that in addition to companies' actual scores, the ranking report should provide "gap scores" reflecting an expert analysis of which indicators a company should be expected to perform well on given the legal and regulatory context of the jurisdictions in which it operates. In order to make this feasible from a research standpoint, some participants also suggested that the project should sharply limit the number of jurisdictions in which local and language research is carried out.

### **8.6 Separate Internet companies and telecoms**

Several stakeholders suggested that comparing Internet companies and telecoms produced results that were insufficiently comparable, partly for reasons outlined in sections 3.2 and 3.3 of this report. Many suggested that separating out a ranking for Internet companies and telecoms would be more meaningful than putting them on the same scale. Others argued that comparing all companies across a set of common disclosure and policy standards remained important and meaningful, but that sub-rankings of telecoms and Internet companies should be included alongside the overall ranking.

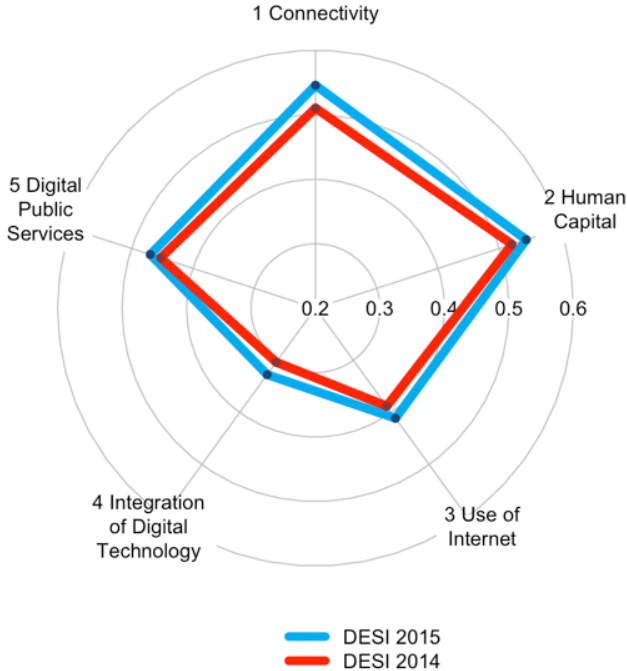
### **8.7 Represent the results visually**

Many participants felt that bar graphs, such as those displayed in Part 2, are not the most constructive way to display the project's comparative data. This is particularly true if we aim to place primary emphasis on the standards the project seeks to set, as well as on the widespread gap between these standards and actual industry practice. Examples of alternative representations of the data include:

1. A “dial” such as that used by Transparency International’s Defence Companies Anti-Corruption Index:<sup>8</sup>



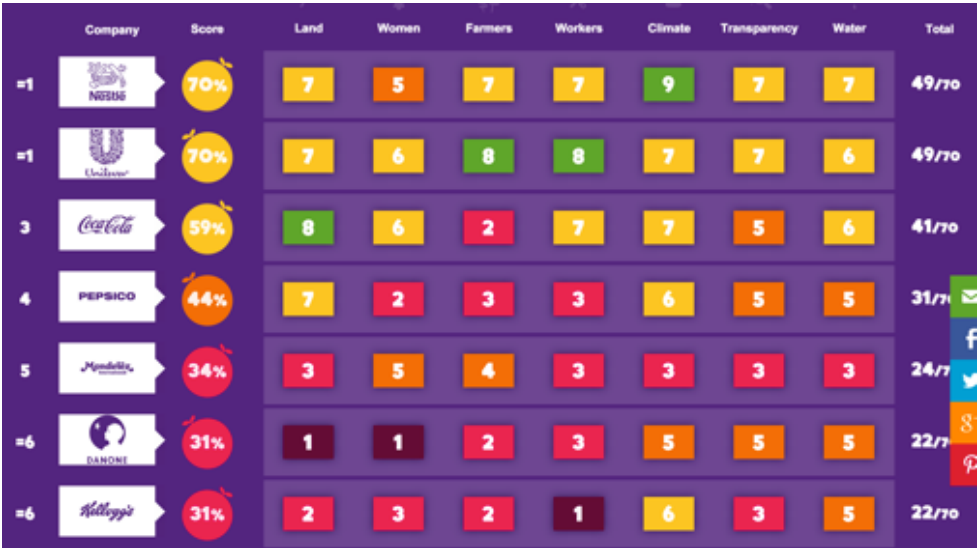
2. Radar charts, such as this one used by the EU Digital Economy and Society Index:<sup>9</sup>



<sup>8</sup> <http://companies.defenceindex.org/results/overall>

<sup>9</sup> <http://ec.europa.eu/digital-agenda/en/digital-economy-and-society-index-desi>

3. A “scorecard” approach used by Oxfam’s “Behind the Brands”:<sup>10</sup>



Other key suggestions related to the presentation of data included separating out thematic sub-scores within the broader “privacy” or “freedom of expression” categories. Others emphasized the importance of enabling individuals who visit the project website to select indicators or adjust weightings, thus generating customized scores most relevant to their particular concerns.

<sup>10</sup> <http://www.behindthebrands.org/en/company-scorecard>

## Part 9: Conclusions and next steps

This report has two main purposes:

1) To meet our commitment to be transparent and accountable with stakeholders—including companies that will be ranked or otherwise affected by the project—about how the ranking’s methodology and research process were developed, tested, and revised before full public implementation.

2) To provide the information necessary for experts, partners, and stakeholders to offer advice and recommendations for how the methodology and research process should be revised.

We hope that the information we have provided will indeed make it possible, in the context of structured conversations, conference calls, and meetings, for our partners and stakeholders to provide concrete recommendations not only for revision. We also welcome bold or even radical suggestions for how the ranking should be streamlined and focused for maximum impact.

### Timeline

In order to revise and implement a methodology and research process in time for a November release date for the full public ranking we anticipate the following timeline:

- **February/March:** Stakeholder consultations
- **April:** Complete methodology revision
- **May:** Complete revised researcher guide and set up a restructured and refined back-end research management system and database.
- **June to mid-July:** Launch research process for the full ranking.
- **mid-July to August:** **Collect** company feedback
- **September:** Incorporate company feedback and finalize dataset
- **October:** Write the report and complete web development
- **November:** Release the inaugural Phase 1 ranking



## **Serving the broader ecosystem**

This ranking is not meant to be an end in itself. It should be considered successful if it can meet the needs of a large and wide-ranging ecosystem of organizations whose own work will be better informed and enhanced by the ranking's existence.

Thus, in addition to advice on how to revise the ranking itself, we hope to hear from organizations about projects they would like to implement based on information that the ranking produces and conversations that it helps to facilitate.

We recognize that Ranking Digital Rights addresses only one slice of a very complex set of problems that are collectively causing a global deterioration of Internet users' enjoyment of their rights to freedom of expression and privacy. However we also believe that if together with many different players in the public, private and non-profit sectors around the world, we roll up our sleeves and tackle different strands of these problems, eventually the tide can be pushed in a more positive direction.

## Annex 1: Methodology and Research Process

This section briefly reviews the methodology development process and explains how the research team scoped the pilot study. It describes company selection; selection of services, languages, and subsidiaries; and selection of questions for a deeper review at the local operating level. Finally, it then describes the steps in the pilot research process and the scoring/weighting system used to calculate the final pilot results.

### **A1.1 Indicators Selected for Local and Language Review**

Time and resource constraints prevented us from evaluating company practices and policies for every indicator at the local level, which depending on company type required examination of local subsidiaries and their separate services, usually in local languages. We selected 16 indicators for which to carry out a local/language review, listed below with indicator number and description of subject. Please see the pilot methodology document for full wording, elements evaluated and answer categories.

G7 - availability/accessibility of terms of service

G10 - impact of identity policy

G11 - complaints and remedy mechanisms

F2 - information about content or access restriction in terms of service

F3 - publishes process for handling government content restriction requests

F4 - publishes process for handling private content restriction requests

P2 - availability/accessibility of privacy policies

P5 - disclosure about collection and use of personal information

P6 - disclosure about retention of personal information

P7 - disclosure about jurisdictions data is stored in or passes through

P8 - disclosure of what personal information may be shared with authorities and reason

P19 – allows users to opt in or opt out of collection of personally identifiable information not essential to core service

P20 – allows opt in /opt out of sharing of personally identifiable info not essential to core service

P21 – users can obtain/download info that the company retains on them

P22 – whether the possibility of account deletion is disclosed/explained

P24 – publishes information to help users defend against hacking/phishing

These indicators were selected because we found it especially important for companies to offer disclosure on them locally, or in the language of key user groups. If the information was not available in that selected language, even if it was available in other languages, the score here would be 'none/no evidence'. This is something that pulled down the score for many indicators for many of the companies.

## **A1.2 Selection of Subsidiaries, Services, and Languages for Local Review**

### *Subsidiaries*

For telecommunication companies we reviewed one to four operating companies or subsidiaries in addition to the parent company. The factors listed above for company selection were also used in selecting subsidiaries. This provided a broader picture of the company's performance and also widened the pilot's geographic coverage.

### *Services*

For telecommunications companies and their subsidiaries, we examined mobile, fixed voice, and fixed broadband services. For Internet companies, we examined the company's three to six most popular services, depending on company size and complexity.

In some cases the services we selected for Internet companies were technically subsidiaries, but we treated them as services and reviewed all indicators for them. Subsidiaries for telecommunications companies, which for all pilot companies operate at a national level, were only reviewed on the 16 indicators flagged for local research.

### *Languages*

Given that most users around the world do not speak English or whatever other language predominates in a company's home market, we recognized the importance of checking for company disclosure in languages that users can be expected to understand. For example, while a company operating in Tunisia might offer its services in French, the official business language, most users are more likely to understand Arabic. Thus in such a case our researchers check on whether and the extent to which the company communicates with users in Arabic in relation to selected indicators.

After identifying subsidiaries and services, we took a spot-check approach to language evaluation, selecting two to three languages for each Internet company (serving a global user base) or one language per subsidiary (for telecommunications companies that reach specific national markets primarily through subsidiaries), depending on size of user base and geographic reach.

For parent companies headquartered in non-English speaking countries, we conducted parent company research in the host country’s language.

For the 16 local-review indicators, we reviewed each service for each subsidiary or local market in the designated languages spoken by significant numbers of users in that market. For the remaining 30 indicators, researchers reviewed services at the parent company only. Consider the following example:

- Company G research included three subsidiaries. For the 16 indicators flagged for local research, researchers reviewed the three services for each subsidiary, for a total of nine potential responses per indicator.
- For the remaining 30 indicators, researchers only reviewed the services for parent Company G, for a total of three potential responses per indicator. (Some of these indicators did not require service-level review and only included one potential answer).

### A1.3 Answer Categories

For all indicators, we developed what we called “answer categories” (ACs): researchers were instructed to select one category that best describes the extent to which a given company meets the standard set by a particular indicator. For the pilot, each AC was associated with a different score: the highest AC being 100%, the lowest (usually “none/no evidence”) being 0%. The “non applicable” (N/A) category was also provided for cases where researchers determined that the indicator does not apply in any way to a given company.

Some indicators were also followed by a set of “elements to be assessed in scoring”, which were used as the basis for determining answer categories. For example:

|  |
|--|
| <p><b>G8.</b> Does the company commit to provide meaningful notice to users when it changes its Terms of Service?</p> <p>Elements to be assessed in scoring:</p> <ul style="list-style-type: none"><li>• Method of notification, e.g., email, SMS, etc.</li><li>• Timeframe within which notification is provided, e.g., two weeks prior to changes occurring</li></ul> <p>Answer categories:</p> <ul style="list-style-type: none"><li>• Meaningful notice – Meaningful notice is provided to users, including detail on method and timeframe</li></ul> |
|--|

- Some notice – Company commits to providing notice, but insufficient detail is available on method and timeframe
- None/no evidence
- N/A

Researchers collected answers to the indicator questions and related research materials through a research management interface and back-end data database system called Indaba, which is described further in Annex 2.

### **A1.4 Pilot Research Steps**

The pilot research was conducted from October 2014 to January 2015 and included seven steps.

1. Primary Data Collection: Sustainalytics carried out an extensive review and data collection analysis of publicly available information on companies, with contributions from local and technical researchers.
2. Peer Review: Sustainalytics undertook an internal peer review of research and findings.
3. RDR Review 1: The RDR team reviewed the research and provided suggestions.
4. Incorporation of Feedback: Sustainalytics incorporated feedback from RDR and prepared the data for company review.
5. Company Feedback: Sustainalytics sent preliminary results to companies and invited their feedback to address any potential gaps in our research findings, and engage their broader feedback on the ranking and its underlying methodology
6. RDR Review 2: The RDR team reviewed company feedback and provided suggestions on score adjustments and any other changes.
7. Finalizing Data: Sustainalytics incorporated any changes and finalized the dataset.

## A1.5 Scoring and Weighting

### *Scoring*

As discussed in Section 3.2, we faced many challenges with scoring. It is expected that the scoring and weighting methodology will need to be changed for the next phase. Mindful of these factors, the pilot study took the following approach to scoring:

We had to aggregate scores across services, local languages, and subsidiaries to arrive at an overall company score per indicator.

Across services, we took the average score.

Across local languages/subsidiaries, we took the lowest score (lowest common denominator). The reason we did not opt for an average, but for a lowest score, is because we recognize that even though it is relatively easy for companies to disclose policies and practices at a parent company level, it takes more effort to ensure users in other countries or of not the parent-company language can have access to key information. Moreover, averaging scores would obscure poor company performance in restrictive operating environments, where good company conduct is especially imperative for users' protection.

The one exception to the lowest common denominator approach was if the parent company or at least one of its subsidiaries received a score higher than "None/No evidence", but the lowest score was "None/No evidence". In that case, we took the next highest score above "None/No evidence", which was oftentimes "Weak". The purpose of this was to recognize the effort the company undertakes in one or more of its operations.

Consider the following example:

- A telecommunication company and its three subsidiaries included a review of three services. To calculate each company/subsidiary score, we averaged the scores of the three services. For example, the company's score for Subsidiary 1 on one specific indicator was calculated as such:

|       | Service 1 | Service 2 | Service 3 |
|-------|-----------|-----------|-----------|
| Score | 100       | 67        | 33        |

This averages out to a 'local' indicator score of 67.

- To calculate the overall score for the company on this indicator, we took the lowest common denominator of the four scores. If the lowest score was None/No evidence, we gave the company a "Weak" score.

|       | Parent company | Subsidiary 1 | Subsidiary 2 | Subsidiary 3 |
|-------|----------------|--------------|--------------|--------------|
| Score | 33             | 67           | 100          | 0            |

The lowest common denominator score here would be '0', but following the rule of exception as described above, the final company score on this specific indicator was '33'.

*Weighting*

To simplify the pilot results, given that the methodology remains experimental, we gave each indicator an equal weight. We eliminated G10 (asking about identity policies) from consideration in the final score, since the question was unclear and did not produce meaningful results. This resulted in section weights that correspond to the portion of indicators in the section. For example, the Freedom of Expression section contains 20 percent of the methodology's indicators (9/45) and comprises 20 percent of a company's overall score.

- General Human Rights: 24 percent
- Freedom of Expression: 20 percent
- Privacy: 56 percent

## Annex 2: Research process: critical analysis

This section describes aspects of the pilot study workflow and researcher guidance that need to be revised before the full ranking. It also highlights differences that researchers observed in disclosure practices across companies. It ends with several questions related to company disclosure practices that need to be resolved before the full ranking. We invite stakeholder input and discussion on these questions.

### A2.1 Pilot Study Workflow

Overall, the pilot workflow functioned well and provides a foundation for the research process for the full ranking. It nevertheless became clear through the pilot study that certain aspects of the process need to be revised, given that the full ranking will include more companies and the results will be released publicly. The main issues to be addressed are the sequence in which research occurs and the need for more robust quality controls.

#### *Research Sequence*

Company research in the pilot included three parts.

- **Primary research:** A primary researcher reviewed the parent company and its services for all 46 indicators in the methodology.
- **Language and local research:** Researchers with specific language expertise conducted research on the 16 indicators flagged for language and local review.
- **Technical research:** Technical experts performed in-depth research on the three security indicators (P23, P24, P25). These indicators focused on encryption and security practices, information that helps users protect themselves from hacking and phishing, and security audits, respectively.

Due to time constraints, primary research, language research, and technical research occurred concurrently. Ideally, we would like to complete primary research for a parent company first, followed by language/subsidiary research. If a company includes multiple languages or subsidiaries, those reviews can occur concurrently.

The technical research may require a bit more flexibility. One of the technical indicators (P24) was also included in the language and local research. We may want to ensure that any security-related materials the technical researcher finds for a company are available in the languages we are evaluating. Conversely, the technical researchers are not fluent in all the languages we examine, so we would want the language and local researchers to check if the company publishes security information that technical researchers can factor into their evaluation.



## *Quality Controls*

The pilot research process included several levels of peer review from Sustainalytics and the RDR team. However, use of multiple repositories for data, complex nature of the methodology, research process, and scoring system, and time constraints resulted in inconsistencies that must be addressed before the full ranking begins.

We used a research platform called Indaba<sup>11</sup> to enter and store most of the pilot data. However, language and subsidiary research was collected in spreadsheets. This required members of the research team to constantly reference two different sources of information. It also introduced redundancy, as researchers sometimes had to enter information from the spreadsheets into Indaba.

After the first stage of data collection was completed, we reviewed the primary, language, and technical research. However, the later stages of the workflow lacked an explicit step to re-examine the language and local and technical research. We will revise the workflow for the full ranking to include multiple reviews of all parts of the research.

## **A2.2 Researcher Guidance**

Before the pilot, we developed a research guide that provided researchers with information about the indicators and how to interpret them. The pilot process revealed that this guidance needs to be much more detailed for the full ranking. Such guidance will provide context for the researchers and help to ensure consistency in research across companies. It will also help company representatives who provide feedback on the data better understand what the indicators are measuring and how their company is being evaluated. The next version of the researcher guide should include more examples, descriptions of the activities being assessed, criteria for assessment, and information on how to select scores.

In addition to the research guide, we offered researchers an implementation guide. While not comprehensively covering all indicators, it offered very concrete examples of the type of information we were looking for specific indicators.

Definitions of key terms will also help ensure that researchers interpret information as consistently as possible. For example, one element that researchers considered in G7 and P2 was whether terms of service and privacy policies were “legalese-free.” Some researchers may have checked the layout of the text in the policy while others may have reviewed the actual language of the policy. Other terms that could be subjectively interpreted, including “meaningful effort” and “prominent location,” need additional explanation. In addition, some researchers may not be familiar with topics the methodology addresses. Researchers would benefit from background information on such topics as identity policies, remedy, net neutrality, filtering, and deep packet inspection.

---

<sup>11</sup> <http://indaba.io/> (Indaba will be discontinued in 2015 and we are in the process of identifying alternative solutions.)