Ranking Digital Rights (http://rankingdigitalrights.org)

Phase 1 discussion draft, February 28, 2014

Methodology elements for ranking Internet & Telecommunications companies on respect for users' rights to freedom of expression and privacy

Overview:

In 2014 the Ranking Digital Rights project (http://rankingdigitalrights.org) is completing a methodology to rank the world's major information and communications technology (ICT) companies on their policies and practices related to free expression and privacy.

The project's purpose in ranking companies is to point the way for all companies to improve their policies and practices related to freedom of expression and privacy through concrete, measurable steps.

An annual ranking of companies policies and practices will also help to inform the decisions of investors and consumers, advocacy strategies of civil society groups, and priorities of government policymakers and legislators around the world.

Due to the complexity of the ICT sector, we are taking a two-phase approach in developing and implementing a ranking methodology:

> **Phase 1 covers Internet and telecommunications companies**. Initial case study research and stakeholder consultation was conducted in 2013. The methodology will be finalized and tested in a pilot study in 2014. The full inaugural ranking of 40-50 Internet and telecommunications companies will be released in late 2015.
>
> **Phase 2 adds software, networking equipment, and devices.** Methodology development will take place in 2014-15, with the project's second rankings report covering all categories of ICT sector companies to be published in late 2016.

This document contains proposed methodology elements for the Phase 1 methodology for ranking Internet and telecommunications companies' policies and practices related to freedom of expression and privacy.

(The term "methodology elements" is used for this document because the methodology will not be fully formed until several outstanding questions are resolved.)

These methodology elements are informed by extensive case study research carried out by an international research team over the second half of 2013 and early 2014.[1]

[1] For more information about the case studies and the draft criteria upon which they were based see: http://rankingdigitalrights.org/project-documents/case-study-research/ and

The case studies and an overarching paper distilling the research findings will be published by mid-2014 on the project website (http://rankingdigitalrights.org). At that time we will also publish a revised and refined version of this methodology.

Building on emerging global standards

In 2008 the **Global Network Initiative (GNI)**[2]**,** a multi-stakeholder initiative of companies, NGO’s, socially responsible investors, and academics, launched a set of principles for the ICT sector on free expression and privacy based on international human rights law enshrined in the UN Declaration of Human Rights and the two UN human rights covenants. Alongside those principles, the GNI published a set of Implementation Guidelines for how companies can act on their commitments through establishing company-wide policies and procedures, conducting human rights impact assessments, and maximizing transparency with users and customers about how the company responds to government demands.

Companies that join the GNI commit not only to the Principles and Implementation Guidelines. They also agree to undergo an independent assessment by certified independent assessors who verify whether member companies have put in place adequate policies and practices to implement the principles. Assessors further verify whether those policies and practices are being carried out by the company in a manner that results in greater respect for user and customers’ rights to free expression and privacy in the face of government demands that sometimes contradict human rights law.

In 2011 the **UN Guiding Principles on Business and Human Rights** (“the GP’s”) [3] affirmed that while governments have the primary responsibility to protect human rights, companies also have a responsibility to respect human rights, including:

a) Determining specifically how their products, services, or business processes affect human rights both positively and negatively (in other words, to conduct what is called a “human rights impact assessment”);

b) Implementing policies and practices designed to mitigate human rights risks and avoid complicity in human rights abuses to the fullest extent possible;

c) Engaging with organizations and individuals whose human rights are at greatest risk of violation in relation to the company’s product or service. Addressing their concerns, understanding the risks they face, and constructing the best possible policies and practices for respecting their rights;

d) Providing remedy to aggrieved parties.

http://rankingdigitalrights.org/project-documents/draft-criteria/

[2] http://globalnetworkinitiative.org

[3] http://www.business-humanrights.org/UNGuidingPrinciplesPortal/Home

The methodology is also informed by key UN documents and related efforts to implement those documents including:

- The 2012 UN Human Rights Council resolution on The promotion, protection and enjoyment of human rights on the Internet

- European Commission ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights

- 2011 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, on the right to freedom of opinion and expression exercised through the Internet

- 2013 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression

These and other documents are listed and linked on the project website.[4]

NOTES TO KEEP IN MIND:

1. In 2015 we will publish the first annual ranking of between 40-50 Phase 1 (Internet and telecommunications) companies. See the draft list at the bottom of this document for the initial proposed list.

2. Prior to full implementation, we will conduct a pilot study focusing on approximately 10 companies selected from the full list. More details on that pilot will be released in the coming months as we undertake public consultation on the draft methodology.

3. The methodology will be based on publicly available materials and other information that can be obtained by any user or subscriber.

4. Some criteria (such as the technical measures for data security or encryption that companies are using) will require the support of a security/encryption specialist working with country-specialist researchers.

5. Prior to finalizing the methodology, we will identify available technical methods for verifying certain claims made by telecommunications companies. (M-Lab, for example, might be able to help us identify bandwidth shaping/throttling; and other projects might enable spot checks on DPI use.)

6. The methodology will need to be accompanied by two supplementary documents: a) glossary of terms and b) implementation guide with more detailed explanation of how

[4] http://rankingdigitalrights.org/resources/

researchers should interpret the questions when gathering information.

Unresolved methodological questions to be refined during the methodology consultation phase and/or pilot study phase:

- How will RDR handle scoring? Specifically,
    - How will RDR score specific companies (e.g., binary, on a scale, partial credit)?
    - How will RDR calculate sub-scores for user rights, freedom of expression, and privacy?
    - How will RDR present the companies' overall scores? (e.g., in different tiers or bands in addition to numerical scores)[5]
    - How will RDR weight the various questions in calculating the overall score?

- How will RDR handle questions that do not apply to all companies (e.g., bandwidth throttling may only apply to companies that operate network infrastructure)?

- How will RDR determine when or whether to treat a subsidiary as an entity separate from its parent company?

INDICATORS: The methodology will be structured around three issue areas:

G – General Respect for User Rights
F – Freedom of Expression
P – Privacy

There are a total of 50 questions across those three issue areas.

[5] We will likely use numerical scores to between 0 and 100, with 100 being a perfect score (which no company is expected to achieve in the first year, but should be achievable over time).

<u>GENERAL RESPECT FOR USER RIGHTS</u> – The company demonstrates a commitment to respect the human rights—particularly the rights to freedom of expression and privacy as articulated by the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights—of the users of its digital platforms, products, and services.

G1. Does the company conduct a regular **human rights impact assessment (HRIA)** that includes the freedom of expression and privacy of users?

a. 50% - if the existence of the company's HRIA is publicly reported in some way but not otherwise subject to external verification or assurance.[6]
b. 75% - if assured by a third party hired by the company (e.g., accounting or consulting firms).
c. 100% - if assured by an independent multi-stakeholder organization or third party accredited and supervised by an independent multi-stakeholder organization.[7]

G2. Is the company a member of a **multi-stakeholder organization** focused on the human rights of users including freedom of expression and privacy? *[scoring: binary yes/no with 25% for observer status]*

G3. Does the company **notify** users when it **changes its Terms**? *[scoring: 1-5 scale]*

G4. Does the company **engage with users** in explaining, changing, and getting feedback on its **Terms**? *[scoring: 1-5 scale]*

G5. Are the company's **Terms freely accessible** without having to sign up or make a purchase?[8] *[scoring: yes, partial, no]*

a. 50% if answer is yes or 25% if partial on the above.
b. 100% if the company is yes for "a" and has an archive (or other form of stored documentation) of past Terms. *[scoring: yes, partial, no for completeness]*

G6. Does the company **disclose** the fact that it **intercepts, examines, and/or filters** data packets transmitted by or to its users?

a. 50% - The fact that it does so.
b. 100% - Its purposes for doing so.[9]

[6] An HRIA whose existence is not made public does not exist for the purposes of this ranking.

[7] Such as GNI or similar organizations whose independence, rigor, and professionalism are of a high standard, with strong participation by human rights organizations that themselves have solid track records of independence from corporate and/or government control. The implementation guidelines would need to include further information about what constitutes a credible multi-stakeholder organization and process in order to prevent fly-by-night flimsily disguised government or industry orgs from being set up to fulfill this criterion.

[8] If they publish Terms for customer service or marketing websites but not for actual core services, this score would be zero.

[9] In the pilot phase we will work with technologists to establish a process for verifying companies' claims.

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?**[10] *[scoring: 1-5 scale]*

G8: Does the company's **HRIA** process include an examination of the freedom of expression and privacy implications of how its **identity policies** are implemented and enforced? *[scoring: binary yes/no or partial]*[11]

FREEDOM OF EXPRESSION - Respects the right to freedom of expression of customers and users and works to avoid contributing to actions that may interfere with this right, except where such actions are lawful, proportionate and for a justifiable purpose.[12]

F1. Does the company's **HRIA** process from G1 include government demands affecting **freedom of expression?** *[scoring: binary]*[13]

F2. Does the company's **HRIA** process include examination of how the processes and mechanisms used to enforce its **Terms** could affect the **freedom of expression** of those who use its services? *[scoring: binary]* [14]

F3. Does the company publish information about the **reasons** why users could be **disconnected** or have their accounts **deactivated**? *[scoring: 1-5 on clarity/detail]*

F4. Does the company publish information about its process for evaluating and responding to **government demands**[15] to **remove, filter,** or restrict access to **content**? *[scoring: 1-5 on clarity/detail/completeness]*

F5. Does the company publish information about its process for evaluating and responding to **requests made by non-governmental entities** or **individuals** to remove, filter, or restrict access to content? *[scoring: 1-5 on clarity/detail/completeness]*

F6. Does the company have an accessible **appeals process** for users whose **content** was **removed** or restricted, or account **deactivated**, for **violating its Terms**? *[scoring: 1-5 scale on clarity/detail]*

F7. If the company **removes, restricts access to, or filters content** does it provide any

[10] These include pen names, stage names, or *noms de guerre* persistently used by an individual who chooses to separate his or her public identity from the name printed on his or her government-issued ID.

[11] If this is not specified in publicly available information then the score for this question is zero.

[12] Adapted from assessment language formulated by the Danish Institute for Human Rights

[13] If this is not specified in publicly available information then the score for this question is zero.

[14] If this is not specified in publicly available information then the score for this question is zero.

[15] Including law enforcement, national security, regulatory bodies, courts of law, etc.

explanation to users?

a. 50% if it notifies users whose content is removed, restricted, or filtered.
b. 50% if it notifies users attempting to access the removed, restricted, or filtered content.

F8. If the company **blocks the transmission of communications between users** does it have a policy to provide notification or explanation to the sender and/or intended recipient? *[scoring: 25% for each component]*

F9. When the company complies with a request for content removal, restriction, or filtering in one jurisdiction, does it have a mechanism to ensure that the **content remains visible in other jurisdictions** where the content is not illegal or does not violate the company's Terms? *[scoring: binary yes/no]*

F10. Does the company have a policy for **how** it will inform users if it **complies with a government order** to shut down or restrict service in a particular area or for a particular group of users? *[scoring: binary yes/no]*

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.[16]

F12. Does the company **publish data** at regular intervals about the number of **government requests** it receives to remove, block, restrict, or prioritize content, plus the number or percentage complied with? *[scoring: 1-5 scale on clarity and completeness]*[17]

F13. Does the company **publish data** at regular intervals about the volume and nature of **private requests** (from non-governmental entities and individuals) for content removal or filtering that it receives, plus the number or percentage it complied with?[18] *[scoring: 1-5 scale on clarity and completeness]*

F14. Does the company **publish data** at regular intervals about the volume of **content removed or restricted for violating the company's Terms**? *[scoring: 1-5 scale on clarity and completeness]*

F15. Does the company **lobby to change laws**, regulations, or international treaties that impinge on its ability to respect users' right to **freedom of expression**, including membership in industry organizations that conduct policy advocacy**?** *[scoring: 1-5 scale]*

[16] Verification of this information would require collaboration with projects such as M-Lab

[17] Implementation guidelines for this question will be informed by GNI/Berkman/CDT/OTI process to develop best practice standards for transparency reporting.

[18] Includes copyright "notice and takedown", defamation claims, etc.

PRIVACY – Respects users' right to privacy and shows a commitment to avoid contributing to actions that may interfere with users' privacy rights, except where such actions are lawful, proportionate and for a justifiable purpose.[19]

P1. Does the company conduct a **privacy impact assessment**?[20]

a. 50% if the assessment is not assured by an independent third party.
b. 100% if the assessment has been assured by an independent third party.

P2. Does the company have a privacy policy, or policies?

a. 50% if only visible to registered users or paying customers.
b. 100% if **freely accessible** without having to sign up or make a purchase.

P3. Does the company **notify users** when it **changes** its **privacy policy**?

a. 50% only - yes but there is no public record kept of previous versions.
b. 100% - the company keeps an **archive** of past privacy policies or a **summary of changes**.

P4. Does the company **engage with users** in explaining, changing, and getting feedback on its **privacy policies**? *[scoring: 1-5 scale]*

P5. Does the company disclose what **personally identifiable information about the user** (including data and metadata) are **collected** and why?[21] *[scoring: 1-5 on clarity/detail/completeness/accuracy]*

P6. Does the company disclose **how long personally identifiable information about the user** (including data and metadata) are **retained** and why? *[scoring: 1-5 on clarity/detail/completeness/accuracy]*

P7. Does the company commit to **store user data strictly for the period that is necessary** for realizing the goals for which the data was provided, and if applicable, for the period legally required under data retention regulations and no longer? *[scoring: 1-5 scale]*

P8. Does the company disclose what data and metadata are **shared with whom** and why? *[scoring: 1-5 on clarity/detail/completeness/accuracy]*

P9. Does the company publish information about which jurisdictions user **data** is or might be **stored** in? *[scoring: 1-5 on clarity/detail/completeness/accuracy]*

[19] Adapted from assessment language formulated by the Danish Institute for Human Rights.

[20] Privacy impact assessments also include consumer privacy issues that may not be included in an HRIA; therefore this question is not tied to the G1 HRIA question, in contrast to the assessment-related questions in the Freedom of Expression section.

[21] Full score requires that this information be published accurately, completely, and in a language that is easy for its users to understand.

P10. Does the company have a published policy and process in which it commits to inform affected parties about **breaches of data security**? *[scoring: 1-5 on clarity/detail/quality]*

P11. Does the company allow users to **opt out of the collection** of personally identifiable information not essential to providing the company's services and does it clearly explain how? *[scoring: 1-5 on clarity/detail/completeness/accuracy]*

P12. Does the company allow users to **opt out of the sharing** of personally identifiable information not essential to providing the company's services and explain how? *[scoring: binary yes/no & partial]*

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?[22] *[scoring: 1-5 scale]*[23]

P14. Does the company publicly report at regular intervals the number of **private requests** (from non-governmental entities and individuals) for user data and the number (or percentage) of requests complied with?[24] *[scoring: 1-5 scale on clarity and completeness]*

P15. Does the company deploy the **highest possible industry standards** of **encryption and security technology** for its products and services? Including (as and where applicable):[25]

- Implements encryption practices that best protect the security of user data[26]
- Conceals user credentials and other non-essential information (such as IP headers) in transmission and storage.
- Enables or supports use of client-to-client encryption.

[scoring: 1-5 scale on quality of implementation and completeness]

P16. Does the company engage in industry best practices to **help users defend against hacking and phishing** attacks? Including (as and where applicable):

[22] Such requests include stored data as well as real-time intercepts from law enforcement, national security, regulatory bodies, courts of law, etc. Companies should categorize different types of data requests as and where applicable.

[23] Implementation guidelines for this question will be informed by GNI/Berkman/CDT/OTI process to develop best practice standards for transparency reporting.

[24] Includes requests made through civil subpoenas or other requests connected to civil complaints.

[25] This list includes elements of the Data Security Action Plan launched by Access in March 2014.

[26] For example, These could be deduced by up-to-date "best practices" guides. For example, see the document published by SSL Labs https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices_1.3.pdf; updated September 2013), which includes 2048-bit encryption, Perfect Forward Secrecy, etc., among its best practices. The Open Web Application Security Project also has a list of broad principles: https://www.owasp.org/index.php/Category:Principle.

- Offers two-factor verification or similar additional non-password security mechanisms to log in to its service.
- Measures to alert users to unusual account activity.
- Measures to protect users from malware and viruses that third parties may attempt to transmit to them via the company's services.

[scoring: 1-5 scale on quality of implementation and completeness]

P17. Does the company conduct a **security audit** on its technologies and practices affecting user data?

a. 50% if an audit is conducted internally or by an organization hired by the company.
b. 100% if an audit is conducted and assured by an independent third-party.

P18. When legally possible does the company **notify users** when their data has been **shared with a government authority?** *[scoring: binary yes/no & partial]*

P19. Does the company publish its process for evaluating and responding to government requests for stored user data or real-time communications? *[1-5 scale]*

P20. Does the company have a clear policy **requiring third-party agents**[27] that have access to personally identifiable information to abide by its **privacy standards?** *[scoring: 1-5 scale on clarity and completeness]*

P21. Does the company provide a **comprehensive list of third parties** with which it shares personally identifiable information relating to its users, indicating what information it shares with which specific third party and for what purpose? *[scoring: 1-5 scale on clarity and completeness]*

P22. Does the company publish clear information about when user communications may be **accessible to third parties**? (Including those with which the company may have no direct relationship.) *[scoring: 1-5 scale on clarity and completeness]*

P23. Does the company publish clear information about when and how it collects user data **from third parties**? *[scoring: 1-5 scale on clarity and completeness]*

P24. Does the company allow **account deletion** for all of its services? *[1-5 scale]*

P25. Does the company inform users what **data is retained after account deletion,** how long, and why? *[scoring: 1-5 scale on clarity and completeness]*

P26. Do users have the right to view all of the personally identifiable information about

[27] Third-party ***agents*** refer to those who carry out tasks on a company's behalf (e.g., payment processors, shippers). The term does not include "independent third parties," which partner with the company and have their own privacy policies (e.g., app developers).

them that the company holds?

a. 25% - Does the company allow users to view that data but not otherwise download or receive a copy?
b. 50% - Does the company allow users to receive a copy of that data?
c. 75% - Is that data in an interoperable format?
d. 100% - Does the company allow users to make changes to all of the personally identifiable information associated with their account?

P27. Does the company **lobby to change laws**, regulations, or international treaties that impinge on its ability to respect user **privacy**, including membership in industry organizations that conduct policy advocacy?

WHO WILL BE RANKED? The following 50 companies are candidates for Phase 1:
(Note: We will select approximately 10 of these companies for the 2014 pilot study)

16 Web/Internet:[28]

1. Google
2. Facebook
3. Yahoo
4. Baidu
5. Tencent
6. Twitter
7. Microsoft
8. LinkedIn
9. Sina
10. Amazon
11. Yandex
12. Vkontakte
13. Sohu
14. Mail.ru
15. Apple
16. Naver Corporation (parent of LINE)

Top 15 telcos from Fortune Global 500:

17. NTT Docomo
18. AT&T
19. Verizon

[28] Top Alexa Global Ranking + top Alexa ranked web or social networking service of countries with large Internet populations (see http://vincos.it/world-map-of-social-networks/ and http://geography.oii.ox.ac.uk/#age-of-internet-empires) + Apple (mobile& cloud data only; device will be evaluated in Phase 2)

20. China Mobile
21. Telefónica
22. Deutsche Telekom
23. Vodafone
24. Comcast
25. América Móvil
26. France Télécom (232.5 million)
27. China Telecom (185 million users)
28. KDDI
29. SoftBank
30. China Unicom (273 million users)
31. Telecom Italia

19 companies selected for user base & global representation

32. Bharti Airtel (485 million)
33. Axiata (215 million)
34. VimpelCom (219 million)
35. MTN Group (201.5 million)
36. Etisalat (150 million)
37. Telenor (166 million)
38. TeliaSonera (189 million)
39. Saudi Telecom Company (171 million)
40. Reliance Communications (131 million)
41. MTS (106 million)
42. Portugal Telecom/CorpCo (100 million)
43. Turkcell (71.3 million)
44. MegaFon (63 million)
45. Oredoo (89.6 million)
46. Millicom (47 million)
47. Zain (46.1 million)
48. SingTel (13.4–434 million, depending on how you count it).[29]
49. Globe Telecom (38.5 million users)
50. PCCW (11.8 million)

[29] Complicated ownership structure:

- Owns 100% of two companies, SingTel Mobile in Singapore (#1, 3.9m) and Optus in Australia (#2, 9.5m).
- Owns 47% of the Philippines’ Globe Telecom (#2, 37m)
- Owns 45% of CityCell (Bangladesh)
- Owns 35% of Indonesia's Telkomsel (#1, 128m)
- Owns shares in Airtel (32%) and Thailand's AIS (23%)