# Ranking Digital Rights (rankingdigitalrights.org)

## PHASE 1 METHODOLOGY DRAFT - V2 - MAY 28, 2014

*Draft methodology for ranking Internet & telecommunications companies on respect for users' rights to freedom of expression and privacy*

**Overview:**

The Ranking Digital Rights project is completing a methodology to rank the world's major information and communications technology (ICT) companies on their policies and practices related to freedom of expression and privacy. For more information about the project's approach, goals, partners, and timeline see http://rankingdigitalrights.org.

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

> **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 the second half of 2014. The first ranking of 40-50 Internet and telecommunications companies will be released in 2015.
>
> **Phase 2 adds software, networking equipment, and devices.** Methodology development will take place in 2014-15, with Phase 2 companies integrated into the ranking cycle from 2016 onward.

This document sets forth a proposed set of indicators for the Phase 1 methodology for ranking Internet and telecommunications companies' policies and practices related to freedom of expression and privacy. For more information about how the methodology was developed, as well as next steps for public consultation and pilot testing, please see the project website.

**Core human rights standards on which this methodology is built:**

Ranking Digital Rights will rank ICT companies on their respect for 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 products and services.

The methodology builds on the **UN Guiding Principles on Business and Human Rights** ("the GP's"),[1] which affirm that while governments have a duty to protect human rights, companies have a responsibility to "respect" human rights, including:

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

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) Developing and 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 by ensuring the availability of effective grievance mechanisms.

Many of the methodology's indicators build on the **Global Network Initiative (GNI)**[2] principles addressing freedom of expression and privacy specifically for the ICT sector, based on international human rights standards enshrined in the UN Declaration of Human Rights and the two UN human rights covenants. A multi-stakeholder initiative comprised of companies, NGOs, socially responsible investors, and academics, the GNI was launched in 2008 and developed in parallel with the UN "protect, respect, and remedy" framework (also released in 2008) which laid the basis for the UN GPs.[3] The GNI developed a set of Implementation Guidelines for its principles, describing specific ways that companies can implement their commitments, including: establishing company-wide policies and procedures; conducting human rights impact assessments; and maximizing transparency with users about how the company responds to government requests. Companies that join the GNI commit 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. The results are in turn certified by GNI's multi-stakeholder board of directors.

The methodology is further informed by other key UN human rights documents and related efforts to implement those documents. A full list can be found on the project website.[4]

[2] http://globalnetworkinitiative.org
[3] See http://www.business-humanrights.org/SpecialRepPortal/Home/Protect-Respect-Remedy-Framework
[4] http://rankingdigitalrights.org/resources/

**Key aspects of the methodology:**

1. The methodology is based on publicly available materials. There are 43 indicators in three categories: General (10), Freedom of Expression (10), and Privacy (23).

2. This version of the methodology is the result of revisions made after receiving extensive feedback from companies, investors, academics, human rights groups, technologists, and specialists in business and human rights to an earlier draft published in February 2014.[5] That draft was based on case study research conducted on companies around the world in order to test out an initial set of draft criteria published in August 2013.[6] (For more about what was learned during the research and development process please see the project website.)

3. This version (V2) will be subject to one more round of public and stakeholder comment. The pilot study will be based on V3, which will reflect feedback on V2.

4. The methodology will be accompanied by two supplementary documents: a) glossary of terms and b) implementation guide with more detailed explanation of how researchers should interpret the questions when gathering information. These documents are consistent with our commitment to maximum transparency about how scores are obtained. They should also make it possible for others to apply the methodology to other companies not included in the RDR ranking.

5. Some indicators (such as the technical measures for data security or encryption that companies are using) will require the support of a security/encryption specialist. Prior to finalizing the methodology (see below), we will identify available technical methods developed by projects such as the Measurement Lab, the Open Observatory of Network Interference, and the Chokepoint Project for verifying telecommunications companies' practices related to bandwidth management and deep packet inspection.[7]

6. In the second half of 2014 we will conduct a pilot study focusing on approximately 10 companies out of 45-50 companies that we are likely to rank in 2015. More details on the pilot will be released after its design and partnership structure have been finalized.

7. In late 2015 we will publish the inaugural ranking of between 40-50 Phase 1 companies (Internet and telecommunications). Funds permitting, we intend to update the ranking online at least annually if not on a quarterly basis, starting in Q1 2016. Phase 2 companies will be added in late 2016. In addition to an annual narrative report, a regularly updated blog will track ongoing developments. The website will invite public feedback and reporting on issues related to the companies ranked.

[5] http://rankingdigitalrights.org/wp-content/uploads/2014/02/rdrmethodologyfeb28.pdf
[6] http://rankingdigitalrights.org/project-documents/draft-criteria
[7] http://www.measurementlab.net, https://ooni.torproject.org and https://chokepointproject.net

**Important points to remember when reviewing the indicators below:**

- Specifics of scoring and weighting are being developed as part of a more detailed Implementation Guide that will be tested during the pilot phase, then revised and finalized prior to implementation.

- A few indicators are followed by bullet point lists headed “elements to be assessed in scoring.” When completed, the Implementation Guide will include much more detailed lists and precise guidelines on scoring. In this draft we have included these lists only in cases where we deemed their inclusion necessary at this stage to clarify the indicator’s meaning and purpose.

- The detailed criteria for scoring most of the other indicators remain under development, to be finalized after the indicators themselves have been finalized at the end of this public consultation phase.

- The question of how scoring will take into account subsidiaries, as well as differences across different jurisdictions in company policies/practices, will also be resolved during the course of the pilot study.

# Ranking Digital Rights

## PHASE 1 DRAFT INDICATORS - V2

### GENERAL HUMAN RIGHTS

*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 products and services.*

***Human Rights Impact Assessment:***

**G1.** Does the company regularly conduct **human rights impact assessments (HRIA)**[8] addressing how the company's products and services affect the freedom of expression and privacy of its users?[9]

*Elements to be assessed in scoring:*

- *If the company publishes information about its HRIA process;*
- *If the company publishes information about its HRIA results;*
- *If the company publishes information about what progress it has made in implementing measures to mitigate negative outcomes for users' freedom of expression and privacy.*

[8] For more information about Human Rights Impact Assessments and best practices in conducting them see this special page hosted by the Business & Human Rights Resource Centre: http://www.business-humanrights.org/UNGuidingPrinciplesPortal/ToolsHub/Companies/StepTaken/ImpactAssessmentThe Danish Institute for Human Rights has developed a related Human Rights Compliance Assessment tool (https://hrca2.humanrightsbusiness.org), and BSR has developed a useful guide to conducting a HRIA (http://www.bsr.org/en/our-insights/bsr-insight-article/how-to-conduct-an-effective-human-rights-impact-assessment) For guidance specific to the ICT sector, see the excerpted book chapter by Michael Samway on the project website at http://rankingdigitalrights.org/resources/readings/samway_hria. Also see the section on assessment in the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights: http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr-sme/csr-ict-hr-business_en.pdf

[9] In including each of the below elements, does the company make a clear commitment to the rights and needs of, as well as the challenges faced by, individuals from groups or populations that may be at heightened risk of becoming vulnerable or marginalize, and with due regard to the different risks that may be faced by women and men.

**G2.** Is the company's HRIA process comprehensive?[10]

*Elements to be assessed in scoring:*

- *Engagement with stakeholders, including human rights experts and potentially affected groups;*
- *Examination of laws affecting privacy and freedom of expression in jurisdictions where the company operates to inform company policies and practices for mitigating risks to users' rights;*
- *Ongoing examination of existing products and services that may pose free expression and privacy risks;*[11]
- *Examination of free expression and privacy risks associated with the launch and/or acquisition of new products or services;*[12]
- *Examination of free expression and privacy risks associated with entry into new markets;*
- *Examination of free expression and privacy risks associated with how the processes and mechanisms used to enforce the company's Terms of Service unrelated to government requirements may affect the freedom of expression and/or privacy of those who use its products or services.*

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

*Elements to be assessed in scoring:*

- *If it is assured by an external organization hired by the company (e.g., accounting or consulting firm);*
- *If the work of that assuring organization has been accredited and supervised by an independent and credible multi-stakeholder organization.*[13]

[10] An HRIA whose existence is not made public does not exist for the purposes of this ranking. Note that this question is not seeking details or results of the HRIA. Rather, it seeks demonstrated commitment to include the listed issue areas as part of its HRIA.
[11] Including Privacy Impact Assessments (PIAs).
[12] Including PIAs.
[13] A credible multi-stakeholder organization includes and is governed by members of at least three other stakeholder groups besides industry: civil society, investors, academics, at-large user or customer representatives, technical community, and/or government. Its funding model derives from more than one type of source (corporations, governments, foundations, public donations, etc.). Its 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 for this methodology should include further information about what constitutes a credible multi-stakeholder organization, with appropriate examples.

***Policy Commitment:***

**G4**. Do/does the **CEO and/or other top officers of the company** make meaningful efforts **to advance users**' **rights**, including freedom of expression and privacy?[14]

**G5.** Does the company commit to **narrowly interpret government requests** and **seek clarification or modification** from authorized officials before complying when **government requests appear overbroad, unlawful, not required by applicable law** or inconsistent with international human rights laws and standards on privacy and freedom of expression?[15]

***Terms of Service:***[16]

**G6.** Are the company's **Terms of Service freely available in plain and accessible language** without having to sign up or make a purchase?[17]

**G7**. Does the company give **meaningful notice** when it **changes its Terms of Service**?[18]

**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;*
- *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.*

---

[14] Full points for CEO involvement plus other top officers, partial for top officers but not CEO. May include membership in industry initiatives as well as multi-stakeholder organizations and initiatives if clearly supported by top corporate officers. Scoring will require substantial and specific guidance, with examples, in the implementation guidelines.

[15] See the Global Network Initiative's Implementation Guidelines: http://globalnetworkinitiative.org/implementationguidelines/index.php

[16] For the purposes of this methodology "Terms of Service" are the same as "Terms of Use," "Terms and Conditions," etc.

[17] Including whether the ToS are in major languages understood by its users. If terms are public for customer service or marketing websites but not actual core services, this score would be zero.

[18] Meaningful notice not only relates to the visibility, format, and clarity of the notice but also the length of time between when notice is given and when the terms actually change. (For example, some companies provide notice one week in advance, others provide it two weeks in advance, etc.) Guidelines for scoring these distinctions will be spelled out in more detail in the Implementation Guide.

***Remedy:***

**G9.** Does the company have a mechanism to receive complaints and **provide remedy to users** who believe that their **rights have been violated** by the company?[19]

***Specific to telecommunications services:***

**G10.** If the company **intercepts, examines, and/or filters** data packets transmitted by or to its users does it **disclose** in plain and accessible language whether it does so?

*Elements to be assessed in scoring:*

- *If the company discloses the fact;*
- *If it also discloses the purposes for doing so.*[20]

**FREEDOM OF EXPRESSION**

*The company respects the right to freedom of expression of 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.*[21]

***Transparency: Content Restriction Policies***

**F1.** Does the company publish information in plain and accessible language in its Terms of Service, or in another prominent location, that explains to users the **reasons** their accounts or **access** to the service may be **deleted, removed, deactivated, or otherwise limited**?

**F2.** 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**[22] to **remove, filter,** or restrict access to **content**?

**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 **requests made by private entities** (including private **individuals)**[23] to **remove, filter, or restrict** access to content?

---

[19] For discussion of remedy in the ICT sector context please see Peter Micek and Jeff Landale, "The Forgotten Pillar:The Telco Remedy Plan," Access, May 2013, at: https://s3.amazonaws.com/access.3cdn.net/fd15c4d607cc2cbe39_0nm6ii982.pdf and the European Commission's "ICT Sector Guide for Implementing the UN Guiding Principles on Business and Human Rights" at: http://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf

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

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

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

[23] Businesses, non-governmental organizations, and any other entities that are not part of the government. This includes subpoenas directly from attorneys in private litigation.

***Transparency: Content restriction practices***

**F4.** Does the company **publish data** at regular intervals about the number of **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?

**F5**. Does the company **publish data** at regular intervals about the volume and nature of **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?[24]

**F6.** Does the company **publish data** at regular intervals about the volume of **content removed, filtered, or restricted for violating the company's Terms of Service** for reasons unrelated to government or private requests covered by F4 and F5?[25]

**F7.** If the company **removes, filters, or restricts access to content** does it provide **explanation to affected users**?[26]

**F8.** When the company complies with a request for content removal, filtering, or restriction in one jurisdiction, does it allow the **content to remain visible in other jurisdictions** where it is legal?

***Net Neutrality:***

**F9.** (For telecommunications services) 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?[27]

*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.*

[24] Includes copyright "notice and takedown", defamation claims, etc.
[25] For the implementation guide: Most ToS stipulate that illegal content/activity is not allowed on their service, but many companies also restrict content in their ToS that is not illegal in at least some jurisdictions where they operate. This question thus covers two types of situations: 1) content removal/restriction that companies carry out without having received a government request but based on an internal decision made by company employees that the content is illegal; 2) Removal/restriction of content that is legal but nonetheless violates the company's ToS.
[26] For this question, the implementation guide will clarify what constitutes meaningful notification.
[27] Verification of this information would require collaboration with projects such as M-Lab

**F10.** (For Internet services) 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?

## PRIVACY

*Respects users' right to privacy and shows a commitment to avoid contributing to actions that may interfere with users' privacy, except where such actions are lawful, proportionate and for a justifiable purpose.*[28]

### *Privacy Policies:*

**P1.** Does the company have a **privacy policy**, or policies, that are **freely available in plain and accessible language**?[29]

**P2.** Does the company give **meaningful notice** to users when it **changes** its **privacy policy**?[30]

### *Transparency: Data collection and retention*

**P3.** Does the company disclose what **personally identifiable information about the user** (including metadata) is **collected,** how it is collected, and why?[31]

**P4.** 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?[32]

### *Data sharing:*

**P5.** 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?

**P6.** Does the company disclose what personally identifying information (including metadata) may be **shared with which government entities** and why?

---

[28] Adapted from assessment language formulated by the Danish Institute for Human Rights.
[29] This includes whether the policies are in all the major languages understood by its users.
[30] Definition of meaningful notice (how many weeks or days) will be detailed in the implementation guide.
[31] This methodology defines PII as information connected to an identified or identifiable person. See: Schwartz, Paul M. and Solove, Daniel J., "Reconciling Personal Information in the United States and European Union" (September 6, 2013). 102 California Law Review (2014 Forthcoming); UC Berkeley Public Law Research Paper No. 2271442; GWU Legal Studies Research Paper No. 2013-77; GWU Law School Public Law Research Paper No. 2013-77. Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2271442
[32] Includes when applicable clear disclosure about what data is stored in anonymized format, under what conditions, and to what uses.

**P7.** 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?

**P8.** Does the company **publish its process** for evaluating and responding to **private requests** for user data?

**P9.** When legally possible, does the company commit to **notify users** when their data has been **shared with or accessed by a government authority**?[33]

**P10.** Does the company commit to **notify users** when their data has been **shared with private parties**?[34]

**P11.** 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?[35]

**P12.** 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?[36]

**P13.** Does the company have a clear published policy **requiring third-party agents**[37] that have access to personally identifiable information to abide by its **privacy standards**?

**P14**. 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?

**P15.** Does the company publish clear information about when user communications may be **accessible to third parties** (even when not actively shared with them)?

---

[33] One demonstration of this commitment would be if the company publishes examples of this type of notification and general circumstances under which such notices are sent to a user.
[34] One demonstration of this commitment would be if the company publishes examples of this type of notification and general circumstances under which such notices are sent to a user.
[35] 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. Implementation guidelines for this question will be informed by GNI/Berkman/CDT/OTI process to develop best practice standards for transparency reporting.
[36] Includes requests made through civil subpoenas or other requests connected to civil complaints. The implementation guide will provide more detail about the categories of private requests including: requests made through law firms, direct requests by family members
[36] of deceased persons, etc.
[37] 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).

**P16.** Does the company publish clear information about whether it **collects user data from third parties**, and if so how and why it does so?

***User control:***

**P17.** Does the company allow users to **opt in or opt out of the collection** of personally identifiable information not essential to providing the company's core services?[38]

*Elements to be assessed in scoring:*

- *If the user can opt out for some services but not all;*
- *If the user can opt out for all services;*
- *If the user is offered a mix of opt out and opt in for different services;*
- *If the user can opt in for all services.*

**P18.** 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?[39]

*Elements to be assessed in scoring:*

- *If the user can opt out for some services but not all;*
- *If the user can opt out for all services;*
- *If the user is offered a mix of opt out and opt in for different services;*
- *If the user can opt in for all services.*

**P19.** Do users have the **right to view, download, or change** all of the **personally identifiable information** about them that the company holds?

*Elements to be assessed in scoring:*

- *If the company allows users to view that data;*
- *If the company allows users to receive a copy of that data;*
- *If that data is in an interoperable format;*
- *If the company allows users to make changes to (including permanently delete all or portions of) the personally identifiable information associated with their account.*

**P20.** Does the company allow **full and permanent account deletion** for all of its services?

[38] Whether the company explains how in a clear and accessible manner is also considered.
[39] Whether the company explains how in a clear and accessible manner is also considered.

***Security:***

**P21.** Does the company deploy the **highest possible industry standards** of **encryption and security** for its products and services?[40]

*Elements to be assessed in scoring:*

- *Implements encryption and other practices that best protect the security of user data, both in transmission and in storage;*[41]
- *Protects user credentials and other non-essential information (such as IP headers) in transmission and storage;*
- *Enables or supports use of client-to-client encryption.*

**P22.** Does the company engage in industry best practices to **help users defend against hacking and phishing** attacks?[42]

*Elements to be assessed in scoring:*

- *Maintains security of credentials with robust authentication safeguards;*
- *Implements measures to alert users to unusual account activity;*
- *Has a notification and patching system to promptly address known, exploitable vulnerabilities;*
- *Educates users on improving their own digital security practices.*

**P23.** Does the company conduct a **security audit** on its technologies and practices affecting user data?

*Elements to be assessed in scoring:*

- *If the company discloses the existence of an audit conducted by an organization hired by the company;*
- *If the identity of the auditor is disclosed;*
- *If the auditor's work is publicly assured by an independent third-party.*

---

[40] This list includes elements of the Data Security Action Plan launched by Access and other organizations in March 2014. See: www.encryptallthethings.net

[41] The implementation guidelines can refer researchers to 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.

[42] This indicator like the previous one draws heavily from the Data Security Action Plan.