Ranking Digital Rights (rankingdigitalrights.org)

PHASE 1 PILOT METHODOLOGY - V3 - OCT 2, 2014

Methodology for pilot study to rank Internet & telecommunications companies on respect for users' rights to freedom of expression and privacy

Overview:

In 2015 the Ranking Digital Rights project will launch an annual ranking of 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. The inaugural public ranking of 40-50 Internet and telecommunications companies will be published in late 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 outlines the 46 indicators, plus basic scoring criteria and research guidance, for the Phase 1 methodology.

In Fall 2014 this methodology will be applied to 12 publicly listed Internet and telecommunications companies operating around the world in a pilot study carried out in partnership with Sustainalytics, a leading independent research firm with extensive experience assessing the environmental, social, and governance (ESG) performance of global companies. The methodology will then be further revised prior to full implementation of Phase 1 in 2015.

During the pilot, RDR and Sustainalytics will draft and refine a detailed research guide to help researchers determine what scores companies receive on each indicator. RDR and Sustainalytics will also decide how to calculate and present companies' overall scores.

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 at https://rankingdigitalrights.org.

Ranking Digital Rights

PHASE 1 PILOT INDICATORS

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) addressing how the company's products and services affect the freedom of expression and privacy of its users? [1]

Elements to be assessed in scoring: [2]

1. If the company publishes information about its HRIA process;
2. If the company publishes information about its HRIA results;
3. 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

Answer categories:

- Comprehensive disclosure – The company publishes information about the progress it has made in implementing measures to mitigate violations of freedom of expression and privacy AS WELL AS publishing information about the results of its HRIAs.

---

[1] 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

[2] 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.

- Strong disclosure – The company publishes information about the results of its HRIAs.
- Basic disclosure – The company says that it undergoes a human rights impact assessment.
- None/no evidence – The company does not disclose implementation of HRIAs.
- N/A

G2. Is the company's HRIA process comprehensive? [3]

Elements to be assessed in scoring:

1. Engagement with stakeholders, including human rights experts and potentially affected groups;
2. 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;
3. Ongoing examination of existing products and services that may pose free expression and privacy risks;
4. Examination of free expression and privacy risks associated with the launch and/or acquisition of new products or services;
5. Examination of free expression and privacy risks associated with entry into new markets;
6. Examination of free expression and privacy risks associated with the processes and mechanisms used to enforce the company's Terms of Service, including identity policies.

Answer categories:

- Comprehensive – Includes all 6 elements
- Strong – Includes 5 of 6 elements
- Good – Includes 4 of 6 elements
- Partial – Includes 2 or 3 of 6 elements
- Weak – Includes 1 of 6 elements
- None/no evidence – Includes 0 of 6 elements
- N/A

[3] Including Privacy Impact Assessments (PIAs).

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

Elements to be assessed in scoring:

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

Answer categories:

- Independent – Assured by an organization that was accredited, and whose work was supervised by, an independent and credible multi-stakeholder organization
- Dependent – Assured by an organization hired by the company but not accredited or supervised by an independent and credible multi-stakeholder organization
- None/no evidence
- N/A

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?

Prominent venue may include: statements or declarations (taking a public stand) made by company VIPs to a wide public audience inclusive of major public fora, such as its own media, public meetings, industry groups, comments to government, etc.

Answer categories:

- Executive-level comment – The chief executive officer, another executive officer, or a board director has commented on the issue.
- Managerial-level comment – Company managers or spokesperson(s) have addressed this issue.
- None/no-evidence – Based on available evidence, the company has not made related disclosures/statements.
- N/A

G5. Is there board-level oversight on how the company's practices affect human rights, including freedom of expression and privacy?

Answer categories:

- Board committee – A board committee has formal oversight of how company practices affect human rights, including freedom of expression and privacy.
- Executive participation on board committee – C-level participation in an executive level committee on how company practices affect human rights, including freedom of expression and privacy
- Executive-level committee – Executive-level committee on how company practices affect human rights, including freedom of expression and privacy, and details of responsibilities are disclosed
- Management committee – Management committee on how company practices affect human rights, including freedom of expression and privacy, but details of responsibilities and membership are not publicly disclosed. Or only one executive has oversight over how practices affect human rights, including freedom of expression and privacy.
- Some executive reporting – The company discloses evidence that executive management in some capacity reports back to the board on human-rights related issues, including freedom of expression and privacy, on a systematic basis, either annually or bi-annually etc.
- Committee below management level – There is a committee on human rights issues, including freedom of expression and privacy, but it is below management level.
- Some existing committee – A committee is responsible for human-rights related issues, including freedom of expression and privacy, but its composition and/or degree of authority is not disclosed.
- None/no evidence
- N/A

G6. Does the company commit to narrowly interpret government requests and seek clarification or modification from authorized officials before complying with government requests that appear overbroad, unlawful, not required by applicable law or inconsistent with international human rights laws and standards on privacy and freedom of expression?

Answer categories:

- Strong – Policy/commitment as well as evidence of follow through

- Partial – Policy/commitment
- Weak – No disclosed formal policy, but evidence of relevant action, or commitments are contained in a narrative-style source, like the website or comments to a news organisation, etc.
- None/no evidence
- N/A

Terms of Service:[4]

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

Elements to be assessed in scoring:

1. Free: **All** of the company's terms are freely available.
2. Language: It is evident that the company has made an effort to provide the ToS in most of the languages spoken by its users.
3. Legalese-free: Easy-to-understand summaries in plain language of what certain paragraphs/section mean.

Answer categories:

- Strong – 3 of 3 elements are satisfied
- Partial – 2 of 3 elements are satisfied
- Weak – 1 of 3 elements are satisfied
- None/no evidence
- N/A

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

Elements to be assessed in scoring:

- Method of notification, e.g., email, SMS, etc.

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

- Timeframe within which notification is provided, e.g., two weeks prior to changes occurring

Answer categories:

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

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

Answer categories:

- Comprehensive archive with redline – The company keeps a comprehensive archive of previous terms of service as well as a “redline” version that allows users to compare changes between old and new versions.
- Comprehensive archive without redline – The company keeps a comprehensive archive of previous terms but does not provide a “redline".
- Disclosure without archive – The company lacks an archive but discloses when the current terms were last modified.
- No public archive or disclosure – The terms do not say when they were last modified
- N/A

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.
- 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

Remedy:

G11. Does the company have a mechanism to receive complaints and provide remedy to individuals who believe that the company has violated or directly facilitated violation of their freedom of expression or privacy rights?

Elements to be assessed in scoring:

1. The company has a comprehensive public policy on remedy that includes the purpose and scope of its complaints and remedy processes;
2. The company discloses the processes that it makes available for receiving complaints or grievances;
3. The company lists the kinds of complaints it is prepared to respond to;
4. The company articulates its process for responding to complaints.

Answer categories:

- Strong – Evidence that all 4 elements are satisfied
- Fair – Evidence that 3 of 4 elements are satisfied
- Partial – Evidence that 2 of 4 elements are satisfied
- Weak – Evidence that 1 of 4 elements are satisfied
- None/No evidence
- N/A

Specific to telecommunications services:

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

Elements to be assessed in scoring:

1. If the company discloses the fact;

2. If it also discloses the purposes for doing so.

Answer categories:

- Strong – Disclosure and explanation/commentary on packet inspection
- Weak – Admits to packet inspection without explanation
- None/no evidence
- N/A

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.[5]

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?

Elements to be assessed in scoring:

1. Officer with explicit functional capacity on freedom of expression issues/Managerial responsibility for freedom of expression
2. Regular training for relevant employees on freedom of expression issues
3. Reporting on freedom of expression issues

Answer categories:

- Strong – Evidence of all 3 elements being satisfied
- Partial – Company satisfies 2 of 3 elements.
- Weak – Only 1 element is clearly satisfied.
- None/no evidence
- N/A

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

Transparency: Content Restriction Policies

F2. 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?

Answer categories:

- Strong – Yes, and it does so in sufficient detail to direct user behaviour
- Partial – Yes, though the details are limited
- Weak – Yes, but they are vague/difficult to understand, or clearly not instructive
- None/no evidence
- N/A

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?

Elements to be assessed in scoring:

1. Publishes a policy or process
2. Discloses guidance/examples of policy implementation
3. Requests from headquarters country are covered
4. Requests from foreign jurisdictions are covered
5. Includes direct government requests
6. Includes court orders obtained by gov. reg. bodies
7. Includes court orders in civil cases

Answer categories:

- Strong – Policy statement includes requests within its headquarters country as well as foreign jurisdictions
- Partial – Policy statement only covers requests within its headquarters country
- Weak – Policy lacks detail
- None/no evidence

- N/A

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?

Elements to be assessed in scoring:

1. Publishes a policy or process
2. Discloses guidance/examples of policy implementation
3. Requests from headquarters country are covered
4. Requests from foreign jurisdictions are covered

Answer categories:

- Strong – Yes, with examples/guidance
- Partial – Yes, but no details
- None/no evidence
- N/A

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?

Elements to be assessed in scoring:

1. Number of requests per country
2. Number of accounts affected
3. Compliance rate
4. Breakdown of reasons for the requests (subject matter)
5. Specific legal authority making the requests
6. Are copies of original requests made available via a third-party archive such as Chilling Effects or similar?

7. Reporting at least once a year
8. Whether the data reported by the company can be exported

Answer categories:

- Strong – At least 7 of 8 elements are satisfied
- Partial – 4 to 6 of the elements are satisfied
- Weak – 1 to 3 of the elements are satisfied
- None/no evidence
- N/A

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?

Elements to be assessed in scoring:

1. Number of requests per country
2. Number of accounts affected
3. Compliance rate
4. Breakdown of reasons for the requests (subject matter)
5. Basis on which the request is made
6. Are copies of original requests made available via a third-party archive such as Chilling Effects or similar?
7. Reporting at least once a year
8. Whether the data reported by the company can be exported

Answer categories:

- Strong – At least 7 of 8 elements are satisfied
- Partial – 4 to 6 of the elements are satisfied
- Weak – 1 to 3 of the elements are satisfied
- None/no evidence

- N/A

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?

Elements to be assessed in scoring:

1. Number or meaningful indication of the volume/magnitude of content-restrictive actions taken;
2. Breakdown per type of restriction;
3. Number of accounts affected;
4. Breakdown of reasons for the action;
5. Reporting at least once a year;
6. Whether the data reported by the company can be exported

Answer categories:

- Strong – At least 5 of 6 elements are satisfied
- Partial – 3 to 4 of the elements are satisfied
- Weak – 1 to 2 of the elements are satisfied
- None/no evidence
- N/A

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

"Users" for the purposes of this question should be understood as people who post the content as well as those trying to access the content.

Answer categories:

- Strong – The company provides a detailed explanation to users.
- Fair – The company provides a generic explanation to users who attempt to view the content as well as those whose content was restricted.

- Partial – The company provides a generic explanation to but only to one type of user or the other.
- Weak – The company just mentions that content was restricted without explanation
- None/no evidence.
- N/A

Net Neutrality:

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

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.[6]

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

Elements to be assessed in scoring:

1. Privacy officer/Managerial responsibility for privacy and data security
2. Regular training for relevant employees on privacy issues
3. Internal reporting on data privacy and security issues

Answer categories:

- Strong – Evidence of all 3 elements being satisfied
- Partial – Company satisfies 2 of 3 elements.
- Weak – Only 1 element is clearly satisfied.
- None/no evidence
- N/A

Privacy Policies:

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?

Elements to be assessed in scoring:

1. Free: The company's privacy policy(ies) is/are freely available.
2. Language: It is evident that the company has made an effort to provide its privacy policy(ies) in most of the languages spoken by its users.
3. Legalese-free: Easy-to-understand summaries in plain language of what certain paragraphs/section mean.

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

Answer categories:

- Strong – 3 of 3 elements are satisfied
- Partial – 2 of 3 elements are satisfied
- Weak – 1 of 3 elements are satisfied
- None/no evidence
- N/A

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

Elements to be assessed in scoring:

1. Method of notification, e.g., email, SMS, etc.
2. Timeframe within which notification is provided, e.g., two weeks prior to changes occurring

Answer categories:

- Meaningful notice – Meaningful notice is provided to users, i.e., detail on method and timeframe is provided
- Some notice – Company commits to providing notice, but insufficient detail is available on method and timeframe
- No evidence
- N/A

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

Answer categories:

- Comprehensive archive with redline – The company keeps a comprehensive, public archive of previous privacy policies as well as a “redline” version that allows users to compare changes between old and new versions.
- Comprehensive archive without redline – The company keeps a comprehensive, public archive of previous privacy policies but does not provide a “redline".
- Disclosure without archive – The company lacks an archive but discloses when the

current privacy policies were last modified.

- No public archive or disclosure – The privacy policy(ies) do not say when they were last modified.
- N/A

Transparency: 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?

RDR 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) at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2271442

Answer categories:

- Strong – Answers "what," "how," and "why"
- Partial – Answers only 2 of the 3, or answers all 3 but with insufficient clarity
- Weak – Answers only 1 of the 3
- None/no evidence
- N/A

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?

Answer categories:

- Strong – Addresses all 3 parts of the question in a clear manner
- Partial – Addresses only 2 of the 3 parts, or answers all 3 but with insufficient clarity
- Weak – Addresses only 1 of the 3 parts
- None/no evidence
- N/A

Data sharing:

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?

Answer categories:

- Strong – Yes, including detail on storage and transit
- Partial – Some detail is provided on either jurisdiction of storage OR transit
- Weak – Only a general statement is made with no substantial detail
- None/no evidence
- N/A

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

Answer categories:

- Strong – Yes, with comprehensive detail
- Partial – Yes, but only with limited detail
- None/no evidence
- N/A

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?

This includes subpoenas in civil court cases.

Answer categories:

- Strong – Published process is clear and includes foreign requests
- Good – Published process is clear, but does not include foreign requests
- Partial – Process is vague, but does include foreign requests
- Weak – Disclosure is vague and does not clearly include foreign requests

- None/no evidence
- N/A

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

This pertains to direct requests that might be made by any private entities without going through a court or government authority.

Answer categories:

- Strong – Yes, clearly disclosed and detailed
- Partial – Yes, but details are lacking
- None/no evidence
- N/A

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?

Answer categories:

- Strong – Makes a clear commitment to notification and explains circumstances under which notification is possible
- Partial – Makes a vague commitment to notification
- None/no evidence
- N/A

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

Answer categories:

- Strong – Makes a clear commitment to notification and explains circumstances under which notification is possible
- Partial – Makes a vague commitment to notification

- None/no evidence
- N/A

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?

Elements to be assessed in scoring:

1. The number of user data and real-time access demands;
2. The number of user accounts affected by those demands;
3. Breakdown of the specific legal authority for law enforcement and national security demands;
4. Whether the demand sought communications content or non-content (e.g., metadata) or both, and how the authorities define these terms;
5. Compliance rate by category of demand;
6. Information that is or may be omitted;
7. Reporting at least once per year;
8. Data reported by the company is exportable.

Answer categories:

- Strong – At least 7 of 8 elements are satisfied
- Partial – 4 to 6 elements are satisfied
- Weak – 1 to 3 elements are satisfied
- None/no evidence

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?

Elements to be assessed in scoring:

1. The number of demands;
2. The number of user accounts affected by those demands;
3. Breakdown of the types of sources of the demands (e.g., civil subpoena, request from

private security company or private investigator, etc.);

4. Whether the demand sought communications content or non-content (e.g. metadata) or both;
5. Compliance rate by category of request;
6. Reporting at least once per year;
7. Data reported by the company is exportable.

Answer categories:

- Strong – At least 6 of 7 elements are satisfied
- Partial – 4 to 5 elements are satisfied
- Weak – 1 to 3 elements are satisfied
- None/no evidence
- N/A

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.)?

Answer categories:

- Strong – The company has clear requirements for privacy policy elements, user consent, user notification, and confidentiality agreements as applicable
- Partial – Some requirements for some situations and/or some types of third parties, but not all
- Weak – Very vague requirements
- None/no evidence
- N/A

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?

Answer categories:

- Strong – Yes, comprehensive
- Partial – Yes, but with a limited scope
- None/no evidence
- N/A

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

Answer categories:

- Strong – No user information is accessible by third parties without the user's express consent regarding specific information AND public information is explicitly specified
- Partial – Some amount of user information is public, but this is detailed by the company
- Weak – Description is vague or involves guesswork
- None/no evidence
- N/A

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?

Answer categories:

- Strong – Yes, and the third parties are identified by name
- Partial – Third parties are generally/broadly described
- Weak – Mentions the fact that data is collected from third parties but no further details
- None/no evidence
- N/A

User control:

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?

Elements to be assessed in scoring:

1. If the user can opt out for some services but not all;
2. If the user can opt out for all services;
3. If the user is offered a mix of opt out and opt in for different services;
4. If the user can opt in for all services.

Answer categories:

- Strong Opt-in – The company requires users to opt in for all non-essential collection of PII.
- Mixed – The company offers a mix of opt out and opt in for non-essential collection of PII.
- Strong Opt-out – The company allows users to opt out for all non-essential collection of PII.
- Weak Opt-out – The company allows users to opt out for some but not all non-essential collection of PII.
- None/no evidence
- N/A

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?

Elements to be assessed in scoring:

1. If the user can opt out for some services but not all;
2. If the user can opt out for all services;
3. If the user is offered a mix of opt out and opt in for different services;
4. If the user can opt in for all services

Answer categories:

- Strong Opt-in – The company requires users to opt in for all non-essential sharing of PII.
- Mixed – The company offers a mix of opt out and opt in for non-essential sharing of PII.
- Strong Opt-out – The company allows users to opt out for all non-essential sharing of PII.

- Weak Opt-out – The company allows users to opt out for some but not all non-essential sharing of PII.
- None/no evidence
- N/A

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?

Elements to be assessed in scoring:

1. If the company allows users to view that data;
2. If the company allows users to receive a copy of that data;
3. If that data is in an interoperable format;

Answer categories:

- Strong – All 3 elements are met: view; download/obtain; in user-friendly format
- Partial – View and download/obtain but not user-friendly format
- Weak – View only
- None/no evidence
- N/A

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

Answer categories:

- Strong – Clear explanation with details about whether, how, and to what extent account deletion can be achieved
- Partial – Some explanation but very general
- Weak – Other than indicating whether the option exists, no further elaboration
- None/no evidence
- N/A

Security:

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

Elements to be assessed in scoring:

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

Answer categories:

- Strong – The company clearly explains how it protects user data and metadata, identifies reputable standards that it uses to protect data at rest and data in transit, and supports client-to-client encryption.
- Partial – The company describes how it protects user data and metadata but does not specify if it protects data-in-transit and data-at-rest, or does not identify a reputable standard.
- Weak – The company mentions security and encryption practices but does not provide any explanation regarding protection of user data and metadata, client-to-client encryption, or which standards it uses.
- None/no evidence
- N/A

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

Elements to be assessed in scoring:

1. Authentication: Enables two-factor authentication, displays which devices have access to the account
2. User notification: Notifies users about unusual account activity, most recent account activity, and possibility of unauthorized access
3. Discloses known vulnerabilities and how the company has addressed them.

4. User education: Publishes materials that educate users on how to protect themselves.

Answer categories:

- Strong – All 4 elements are satisfied.
- Partial – The first 3 elements are satisfied.
- Weak – 1 or 2 elements are satisfied.
- None/no evidence
- N/A

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

Elements to be assessed in scoring:

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

Answer categories:

- Strong – All 3 elements are satisfied.
- Partial – The first 2 elements are satisfied.
- Weak – The company discloses the existence of an audit without further information.
- None/no evidence
- N/A