Phase 1 Criteria Research Draft - Ranking Internet & Telecommunications Companies on Free Expression and Privacy

(Revised August 12, 2013 for use in telco-focused case studies[1])

Overview:

In 2013 the Ranking Digital Rights project (http://rankingdigitalrights.org) is developing a methodology to rank the world's major information and communications technology (ICT) companies on policies and practices related to free expression and privacy. Due to the complexity of the ICT sector, we are taking a two-phase approach:

> **Phase 1 (2013-2014)** covers Internet and telecommunications companies. Research and stakeholder consultation required to develop the methodology is being conducted in 2013. A draft of the methodology will be published for public consultation in early 2014. Once finalized, the methodology will be applied to a data collection and analysis process in the first half of 2014. The project's first rankings report, in which companies will be scored, will be published in late 2014.
>
> **Phase 2 (2014-2015)** adds software, networking equipment, and devices. Methodology development takes place in 2014, with the project's second rankings report covering all categories of ICT sector companies to be published in late 2015.

This document contains the Phase 1 Criteria Research Draft for measuring Internet and telecommunications companies' policies and practices. This draft of the criteria will be applied by researchers in case studies to selected Internet and telecommunications companies in a range of different jurisdictions and contexts. That research in turn will contribute to the drafting of a full methodology by the end of 2013. This draft is based on:

- Feedback on two earlier drafts from academics, technologists, advocates, investors, experts on business and human rights, and specialists on corporate accountability and rankings (See http://rankingdigitalrights.org for details);
- Review of other corporate rankings and indexes, most focusing on other issues related to business and human rights and/or sustainability (see http://rankingdigitalrights.org/resources/);
- Review of other relevant research, publications, and corporate accountability projects (see http://rankingdigitalrights.org/resources/);
- Identification of specific rights risk scenarios for users of Internet and telecommunications platforms and services worldwide (see http://rankingdigitalrights.org/project-documents/risk-scenarios/).
- Extensive and long-running engagement with the Global Network Initiative (GNI), the UN Working Group on Business and Human Rights[2], and the European Commission's *ICT Sector Guide on Implementing the UN Guiding Principles for Business and Human Rights*[3].

[1] Internet company focused case studies will continue to use the July 11 version.

[2] http://www.ohchr.org/EN/Issues/Business/Pages/WGHRandtransnationalcorporationsandotherbusiness.aspx

[3] http://www.ihrb.org/project/eu-sector-guidance/index.html

Broader objectives:

Our purpose in ranking companies according to a version of the criteria below is to:

1) Educate a broader audience of Internet users, advocacy groups, consumers, investors, policymakers, and companies themselves on baseline standards of corporate policy and practice that we believe should be achievable in the medium-term by existing companies.

2) Identify: a) which companies can be considered industry leaders on free expression and privacy in what specific ways, and b) which companies could be doing much more to respect customers' and users' digital rights.

3) Point the way for all companies to improve their policies and practices through concrete, measurable steps.

Building on emerging global standards

In 2008 the **Global Network Initiative (GNI)**[4]**,** 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. Without such an assessment, there is no way that the public can be certain that company actions actually match their claims about and public commitments.

In 2011 the **UN Guiding Principles on Business and Human Rights** ("the GP's")[5] 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");

[4] http://globalnetworkinitiative.org
[5] http://www.business-humanrights.org/UNGuidingPrinciplesPortal/Home

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 who are at greatest human rights risk in relation to the company's product or service in order to address their concerns, understand their risks, and construct the best possible policies and practices for respecting their rights;

d) Providing remedy to aggrieved parties.

Explanation of draft criteria elements:

This draft criteria identifies three key issue areas: The first is based on general responsibilities of business in the context of long-established international human rights standards. The second two issue areas address businesses' specific responsibilities towards two specific rights: freedom of expression and privacy. Each is coded with a different letter:

G - General human rights responsibilities – As outlined in the "International Bill of Human Rights" comprising the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic and Social Rights.[6] The UN Guiding Principles on Business and Human Rights provide a framework for how businesses should uphold their responsibility to protect human rights, while the European Commission (EC)'s *ICT Sector Guide on Implementing the UN Guiding Principles for Business and Human Rights* provides specific guidance to the ICT sector in meeting all human rights obligations.

F - Free Expression - As articulated in Article 19 of the UDHR and Article 19 of the ICCPR.[7] These criteria relate to company responses to government censorship and service shut-down demands as well as to company enforcement of their own terms of service. The GNI Principles and Implementation Guidelines address companies' responsibility to uphold freedom of expression in the context of government demands, while the EC Guidance addresses free expression issues more broadly alongside all other human rights concerns.

P – Privacy - Article 12 of the UDHR and Article 17 of the ICCPR.[8] These criteria relate to all practices involving collection and sharing of information about users and customers that could have negative affects on the civil and political lives[9] of technology users. These practices include company responses to government surveillance demands, data collection and third-party sharing practices, as well as companies' own rules governing user or customer identity. The GNI Principles and Implementation Guidelines address companies' responsibility to uphold privacy rights

[6] http://www.ohchr.org/Documents/Publications/FactSheet2Rev.1en.pdf
[7] http://www.un.org/en/documents/udhr/index.shtml#a19 and http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx
[8] https://www.un.org/en/documents/udhr/index.shtml#a12 and http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx
[9] "Civil" and "political" defined here in the same way as in the UDHR and ICCPR.

in the context of government demands, while the EC Guidance addresses privacy issues more broadly alongside all other human rights concerns.

Within the three issue areas, three indicator categories are:

1. **Commitment –** This indicator measures whether and to what extent the company has made public commitments to uphold rights covered by each of the three issue areas. It also measures whether and to what extent it takes concrete steps to understand the real-world impacts of its products, services, and/or operations on human rights generally, and free expression and privacy specifically.

2. **Practice –** This indicator measures the existence of specific policies, practices and mechanisms carried out by the company.

3. **Transparency –** This indicator measures the extent to which a company communicates clearly with its users or customers, as well as the broader public, about how and to what extent it responds to government demands, how it formulates and enforces its own Terms of service or use, etc.

Each category contains a list of questions and sub-questions. Each question is coded with a letter for the issue category plus a number for the indicator. Questions answerable through desk research (review of publicly available material) are not highlighted. Questions requiring a company interview or survey are highlighted in blue. Questions likely requiring a combination of desk research followed up by interview are in green.

NOTE: companies will not be scored according to this Research Draft, which is for preliminary case study research and analysis purposes only. After the criteria below have been tested and analyzed by case study researchers, they will be revised and incorporated into a full methodology which includes a company selection process and weighting of the criteria. After the methodology is finalized and applied in 2014, each company will receive a score for each of the three issue areas (General, Free Expression, Privacy). That score will in turn be divided into three parts (Commitment, Practice, Transparency).

Starting with what we *know* we can measure *now*.

Many experts and stakeholders have emphasized that it is important to measure not only what companies *say* but what they *do.* This concern must be balanced by practical considerations of what questions about company practices we would *actually be able to answer*, in a consistent manner, across what dozens of companies headquartered in a range of countries.

There is also the question of manageable scope. A list of every possible measure that many advocates and technologists believe companies should take in order to maximize freedom of expression and privacy for the world's Internet users would produce a ranking – and require a data collection and analysis process – of excessive complexity that would overwhelm this project's scope and capacity.

Finally, it is important to recognize that the criteria we have included in this draft already represent a major challenge to most companies. We have learned a great deal from

observing the GNI founding companies' experience in making commitments, putting policies and practices in place, and undergoing independent assessment. Compared to the GNI Principles and Implementation Guidelines, these criteria are more prescriptive and represent a higher but not unattainable standard of commitment, practice, and transparency. It is therefore our view that if companies come anywhere close to meeting the standards laid out in these criteria, substantial, genuinely meaningful improvements in those companies' human rights impact will necessarily result - even if those improvements remain incomplete and imperfect.

Note on Terminology:

A few terms used in the criteria merit further explanation:

Multi-Stakeholder Organization - An organization that includes and is governed by members from at least three other groups besides industry: civil society, academics, at-large user or customer representatives, investors, and/or government.

Due Diligence and Human Rights Impact Assessments – In order to uphold their human rights responsibilities companies need to engage in a continuous internal process of identifying and assessing the negative impacts on human rights with which they may be involved in any way. These "impacts" include actual impacts (past or current) as well as potential impacts (those possible in the future). A detailed overview of best practices in human rights due diligence and impact assessments in the ICT sector context can be found in the *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* published by the European Commission and written by the Institute for Human Rights and Business and Shift.[10]

Independent Third-Party Assessment – A number of questions in the criteria ask whether the existence or quality of a particular policy or process has been verified by an independent assessor. These questions are based on the practical reality that if the claims made by a company cannot be independently verified, those claims have limited value. Only when a company's claims about its human rights policies and practices are verified by a credible independent third party assessment process, whose conclusions are made public, can that company be considered to have met basic standards of public accountability. While this idea may seem new to many executives in the ICT sector, it is a core principle on which a growing number of corporate accountability systems focused on other sectors and other human rights issues are now being built.

In 2013 the GNI is the only organization in the world offering an independent third-party assessment process for ICT companies on free expression and privacy criteria, whose conclusions are publicly reported.[11] However, it is important to note that having undergone GNI assessment may or may not earn the company a full score on that particular criteria item; it depends on whether GNI publishes sufficient detail about the results of its assessments so that an external researcher (who is not a GNI board member or participant) can satisfactorily determine the answers to specific criteria questions regarding assessment.

---

[10] http://ec.europa.eu/enterprise/policies/sustainable-business/corporate-social-responsibility/human-rights/

[11] Some other groups do conduct assessments, but to date their results are not made public or validated by a multi-stakeholder process.

RESEARCH DRAFT PHASE 1 CRITERIA

General Human Rights Responsibilities

G1 – Commitment

G1.1 - Does the company make a commitment to respect human rights in any of its publicly available materials? (If yes provide link/s or documentation.)

G1.2 - Has the company committed to implement the UN Guiding Principles on Business and Human Rights in any of its publicly available materials? (If yes provide link/s or documentation.)

G1.3 - Does the company publicly report on its efforts to implement the UN Guiding Principles (UNGPs)? (If yes provide link/s or documentation.)

G1.4 **-** Is the company a member of any industry organization that makes a collective commitment to respect human rights?

G1.5 - Is the company a member of any multi-stakeholder organization that works to uphold core human rights principles?

G1.6 – Human Rights Due Diligence and Impact Assessment

G1.6.1 - Does the company have a process to identify the human rights impacts of its existing services and operations?

G1.6.2 - Does the company carry out human rights impact assessments before launching new products or services, or entering new markets?

G1.6.3 – Does the company undergo an independent third-party assessment process to verify the existence and evaluate the quality of 1.6.1 and 1.6.2?

G1.7 – Rights-Compatible Terms (“terms of service,” “terms of use,” or the equivalent)

G1.7.1 - When formulating its Terms did the company assess the potential impact of those Terms on user and/or customer rights?

G1.7.2 - Does the company regularly assess how the rights of users and customers are affected by all measures that it uses to enforce its Terms?

G1.7.3 - Does the company have a process to evaluate the potential human rights impact caused by changes to its Terms or to its enforcement procedures before those changes are made?

G1.8 - Does the company embed a commitment to the human rights of users and customers – including the right to free expression and privacy – into its operating licenses with governments?

G1.9 - Does the company embed a commitment to the human rights of users and customers – including the right to free expression and privacy – into its contractual agreements with business partners?

G2- Practice

G2.1 – Does the company engage with governments in countries where it conducts business to advocate for changes to policies and laws that clash with international human rights law?[12] (If yes provide publicly available information about such dialogue.)

G2.2 – Expert Consultation and Stake-holder Engagement

G2.2.1 – Does the company consult with experts (from academia, civil society, government, etc., as appropriate and relevant) to identify "high-risk" user or customer groups?[13]

G2.2.2 - Does the company engage with civil society groups and representative "high risk" users or customers (directly or indirectly and where feasible) about the impact of existing as well as future potential products, services, operations, and Terms?

G2.2.3 - Does the company have a process for engaging its user/customer community in developing or changing its Terms?

G2.2.4 - Does the company engage with experts and high-risk users to identify measures and options available to the company in order to mitigate human rights risks?

G2.3 - Does the company have a process for incorporating the results of stakeholder engagement (described in G2.2) into decision making about product design, Terms, enforcement of Terms, business practices and processes, service management, business relationships, etc.?

G2.4 - Does the company have a user-friendly, publicly accessible mechanism through which users or customers can report human rights-related grievances?

G2.5 – Does the company have a process to evaluate and decide whether and how to comply with government demands to install specific equipment or software on their networks?[14]

G3 – Transparency

G3.1 - Does the company give notification to users and customers when it makes changes to its Terms - using language that is understandable to the average user or customer?

G3.2 - Does the company publish information about the criteria and mechanisms used to enforce its Terms?[15]

G3.3 – Does the company publish information about its own human rights due diligence and/or human rights impact assessments?

G3.4 – Does the company undergo an independent third-party assessment process to verify the existence and assess the quality of its human rights due diligence and assessment mechanisms?[16]

---

[12] As articulated in the International Bill of Rights.

[13] Those whose human rights are at greatest risk of violation in jurisdictions where the company's services are available. See http://rankingdigitalrights.org/project-documents/risk-scenarios/

[14] Added August 8 for use in telco-focused case studies.

[15] Recognizing reasonable limits in keeping with international human rights standards: disclosing some details may not be possible without empowering illegal/abusive behavior by users/customers seeking to violate the rights of other users/customers.

[16] Researchers have pointed out this is a duplication of G1.6.3 which needs to be resolved.

G3.5 – Does the company publish information about how it engages with stakeholders and experts?

G3.6 – Does the company disclose the circumstances under which some part of its facilities may be occupied by non-employees who are either contracted or employed by a government?

G3.7 – Does the company disclose the circumstances under which it may grant access to subscriber messaging services to external entities including law enforcement?

G3.8 – Does the company disclose whether and how it deploys any Deep Packet Inspection (DPI) technologies on its network, and if so for what purposes they are used?[17]

FREEDOM OF EXPRESSION

F1- Commitment

F1.1 – Does the company make an explicit and public commitment to freedom of expression[18]?

F1.2 - Does the company have an on-going process to assess how the free expression rights of users or customers have been affected by government or court demands to remove or filter content, block specific user communications, deactivate accounts, or shut down service to a particular area or category of users?[19] [20]

F1.3 - Prior to entering a new market or launching a new service, does the company have a process to assess the probability and likely nature of demands to remove or filter content, deactivate accounts, or shut down service to a particular area or category of users?

F1.4 – Prior to entering a new market or launching a new service, does the company have a process to assess how the types of demands described in F1.3 might affect users' free expression rights?

F1.5 **–** Does the company have a process for assessing how user or customer free expression rights are affected by measures (such as content removal and account deactivation), taken to enforce the company's own Terms?

F2 – Practice

F2.1 - Does the company have a process in place for evaluating and responding to government or court demands to remove or filter content, carry out bandwidth throttling or shaping, block specific user communications, deactivate accounts, or shut down service?[21]

F2.2 - Is there a policy on who in the company is responsible for making the decision about how and whether to comply with demands to remove or filter content, carry out bandwidth throttling or

[17] G3.6-8 were added on August 8 for use in telco-focused case studies.
[18] Article 19 of the UDHR and Article 19 of the ICCPR.
[19] As articulated in the UDHR and ICCPR.
[20] Modified August 8 for use in telco-focused case studies.
[21] Modified August 8 for use in telco-focused case studies.

shaping, block specific user communications, deactivate accounts, or shut down service?[22]

F2.3 - Does the company have clear procedures for challenging or rejecting demands for content removal or filtering, account deactivation, or service shutdown demands when it determines that those demands are of questionable legality in the relevant jurisdiction?

F2.4 - Does the company actively challenge government demands for content removal or filtering, account deactivation, or service shutdown in a court of law when it determines that it is within its legal rights to do so?

F2.5 - In cases when the company decides to comply with a demand to remove or filter content in a specific jurisdiction, does the company have a mechanism to ensure that the content remains visible to users in other jurisdictions where the content is not illegal and does not violate the company's global Terms of Service?

F2.6 – Does the company have a complaints or appeals mechanism through which users or customers can appeal for reinstatement of accounts or content deactivated or removed by the company in the course of enforcing its Terms or responding to external demands?

F2.7 – Does the company have a mechanism to respond to and/or provide remedy to users or customers who believe that their freedom of expression rights have been violated by the company?

F3 – Transparency

F3.1 - Does the company publish explanations of its procedures for receiving, evaluating, and responding to demands to remove or filter content, carry out bandwidth throttling or shaping, block specific user communications, deactivate accounts or shut down service?[23]

F3.2 - Does the company publish explanations of the laws and regulations (or other circumstances) under which it is compelled to remove or filter content, deactivate accounts, carry out bandwidth throttling or shaping, block specific user communications, or shut down service in every relevant jurisdiction?[24]

F3.3 – Does the company publish data at regular intervals about the number of demands it receives to remove or block content, carry out bandwidth throttling or shaping, or block specific user communications, in every jurisdiction where such demands are made, plus the number of demands it complied with? [25]

F3.4 - When the company responds to a demand to remove or filter content or block communications does it inform the user who published the content or initiated the communication about the reasons for its removal, filtering, or blocking?[26]

F3.5 - Does the company provide clear explanation of why content is no longer accessible to users who are attempting to access content that has been filtered or deleted?

F3.6 - After a demand to shut down service in a particular area or to a certain group of users has been complied with, does the company have procedures and practices in place for informing the

[22] Modified August 8 for use in telco-focused case studies.
[23] Modified August 8 for use in telco-focused case studies.
[24] Modified August 8 for use in telco-focused case studies.
[25] Modified August 8 for use in telco-focused case studies.
[26] Modified August 8 for use in telco-focused case studies.

public of the circumstances under which the action was taken?

F3.7- When the company takes action against a user for violating the company's own Terms (e.g. by removing specific content, deleting the user's account, or suspending some of the account's functions), is the user informed why the action was taken?

F3.8 - When the company takes action against a user for a Terms violation, is the user provided with information about an appeals process?

F3.9 - Does the company undergo an independent third-party assessment process to verify whether and to what extent the company implements its freedom of expression related commitments, policies, and practices?[27]

F3.10 – Does the company disclose whether it performs bandwidth throttling and/or shaping for commercial or other purposes unrelated to government demands, and if so for what purposes including specific applications or services targeted?[28]

PRIVACY

P1 – Commitment

P1.1 – Does the company make a public commitment to the right to privacy[29]?

P1.2 – Does the company make explicit reference in published materials to widely endorsed data protection principles such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, US FTC Fair Information Practice Principles, etc.?

P1.3 – In all jurisdictions where the company operates, does it have a process to assess the human rights impact of government surveillance demands?[30]

P1.4 – When conducting human rights impact assessments on new products, services, operations or entry into new markets, does the company include:

P1.4.1 – assessment of the expected extent and nature of government surveillance demands – such as whether government access demands would be on a case-by-case basis or whether the government will demand unfettered access to all stored or real-time communications.

P1.4.2 – assessment of the likelihood that surveillance could result in human rights violations based on publicly available information about the relevant jurisdiction(s) human rights record?

P1.5 - Does the company have a process to assess how its privacy policies affect user/customer rights in all jurisdictions where the company operates?

P1.6 – Does the company have an assessment process for evaluating the human rights impact of its data retention policies and practices in the context of government surveillance practices in jurisdictions where it operates?

[27] This question was added on July 11. It is the only substantive difference between the July 1 and July 11 documents.
[28] Added August 8 for use in telco-focused case studies.
[29] Article 12 of the UDHR and Article 17 of the ICCPR.
[30] "Surveillance demands" refers to demands for stored user data as well as real-time access to user communications – from law enforcement as well as from national security authorities.

P1.7 – Does the company have a process to assess the human rights impact of its identity policies?[31]

P1.7.1 - In jurisdictions where the law permits, does the company allow pseudonyms for users' public-facing identity?

P1.7.2 - In jurisdictions where "real ID" is required by law has the company assessed the human rights risks of providing specific services and features in those jurisdictions?

P1.8 - Do contractual relationships between the company and any third party service providers (including cloud service providers) extend all of the company's standards and practices related to privacy and data protection to those third parties? If not is the user/customer clearly notified?

P2- Practice

P2.1 – Does the company have internal measures in place to prevent user data from being used for purposes other than those that the user specifically agreed to?

P2.2 – Does the company have internal security safeguards against the following:

P2.2.1 – unauthorized access to user information

P2.2.2 – unauthorized use of user information

P2.2.3 – unauthorized disclosure of user information

P2.2.4 – unauthorized modification of user information

P2.2.5 – loss of user information

P2.2.6 – unauthorized destruction of user information

P2.3**-** In handling data that has been collected for relevant purposes with user consent, does the company make meaningful efforts to ensure that the data is accurate, kept up-to-date, and complete (including a log of all corrections, completions and deletions made)?

P2.4 – Does the company actively challenge government demands for real-time surveillance or stored user data in a court of law when it determines that it is within its legal rights to do so?

P2.5 - Does the company voluntarily build engineering design features into its tools and services that protect user privacy?

P2.5.1 - Do technical measures for the security of stored data and real-time communication (as relevant to the service) use up-to-date versions of transport and/or storage encryption of the relevant encryption standard applicable to each product or service?

P2.5.2 - Does the company take proactive technical steps to conceal non-essential user information (such as the user's IP address in e-mail headers, for example)?

[31] "Identity policies" refers to rules about how the user or customer is identified online – i.e., whether they can use a fake name or are required to use their real name, whether they are always or sometimes asked to verify their identity, etc.

P2.5.3 - Does the company allow (in both the policy and the technical sense) users to employ private communications technologies of their choosing (i.e., ciphertext or manual encryption)?

P2.6 - Does the company allow account deletion for all of its services?

P2.7 - Does the company have a process for meaningful consultation with its user/customer community on changes/improvements to its privacy policies, practices, and technical measures?

P2.8 – Does the company have a grievance mechanism through which users or customers can report on violations or breaches of their privacy rights?

P2.8.1 – Does the company have a mechanism to respond to and/or provide remedy to users or customers whose privacy rights have been breached or violated in the course of using the company's platform or service?

P2.9 - Does the company have a process in place for evaluating and responding to demands for real-time surveillance and stored user data in each jurisdiction where such demands are made?

P2.10 - Is there a policy on who in the company is responsible for making the decision about how and whether to comply with real-time surveillance or stored user data demands in each jurisdiction where such demands are made?

P2.11 - Does the company have procedures for challenging or rejecting real-time surveillance and stored user data demands when it determines a demand is of questionable legality in a given jurisdiction?

P3- Transparency

P3.1 - Does the company publish explanations about the laws and regulations under which it is compelled to comply with real-time surveillance and/or stored user data requests in every relevant jurisdiction?[32]

P3.2 - Does the company publish explanations of its procedures for receiving, evaluating, and responding to real-time surveillance and stored user data requests?[33]

P3.3 - To the extent permitted by law, does the company publish data at regular intervals about the number of stored user data requests it receives in every relevant jurisdiction, plus the number of requests it complied with?[34]

P3.4 - Does the company publish data at regular intervals about the number of real-time surveillance requests it receives in every relevant jurisdiction, plus the number of requests it complied with?[35]

---

[32] If the company publishes information about public security/law enforcement demands but not national security demands then the answer is "partial" *not* "yes".

[33] See previous footnote.

[34] See previous footnote. Researchers should also note whether the company reports law enforcement & national security requests separately or in an un-differentiated total.

[35] See previous footnote. Researchers should also note whether the company reports law enforcement & national security requests separately or in an un-differentiated total.

P3.5 - Where legally possible does the company publish its licensing agreements with governments?

P3.6 - Does the company publish information about all aspects of its contractual agreements with business partners that affect user/customer privacy?

P3.7 - Does the company publish information about which jurisdictions the user data is or might be stored in, and which jurisdictions their communications may be transmitted through?

P3.8 - Does the company publish information about its procedures for holding employees accountable for violations of company data protection policies?

P3.9 - Does the company notify users in a timely manner when their privacy has been breached due to employee violation, crime, or accident?

P3.10 - Does the company allow users to obtain all data collected and held by the company in an intelligible format, and any available information as to the data's source, without constraint at reasonable intervals and without excessive delay or expense?

P3.11 - Does the company publish clear information about the circumstances under which user communications may be visible to third parties (with whom the company may or may not have any relationship)?[36]

P3.12 – Does the company publish clear information about the circumstances under which it collects and retains user data from other third party entities?

P3.13 - Does the company publish clear information about the existence and nature of privacy and security features for all of its services?

P3.14 - Does the company notify users when it makes changes to its privacy policies?

P3.15 - Do the privacy policies of the company's services include the following elements:

P3.15.1 – information about what personal data is collected, under what circumstances, and for what purpose

P3.15.2 – information about what personal data is shared with which specific third parties, and for what purpose

P3.15.3 – information about whether and how users can opt-out of having their data shared with third parties (this includes third-party tracking of user activity, sale of user data to third-parties including commercial affiliates, etc.)

P3.15.4 – information about what different categories of personal data (including IP address) are retained by the company, for how long the data is retained and why it is retained

P3.15.5 – information about company policies and measures to protect user data

P3.16 - Does the company undergo an independent third-party assessment process to verify whether and to what extent the company implements its privacy-related commitments, policies, and practices?

[36] "Third parties" includes all possible government agencies as well as any government with which the may have entered into voluntary agreements. (Clarification added Aug. 8)