RANKING DIGITAL RIGHTS

Human Rights Risk Scenarios for Internet and Telecommunications Companies

February 2015

Background

This paper is part of a set of materials documenting the methodology development process for Phase 1 of a ranking of ICT sector companies on freedom of expression and privacy criteria.

To view or download all other materials please visit:
https://rankingdigitalrights.org/methodology-development/

About Ranking Digital Rights

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

For more about New America please visit www.newamerica.org

For more about the Open Technology Institute please visit www.newamerica.org/oti

Table of Contents

Introduction

When human rights defenders and journalists use technology, they are especially vulnerable to threats to their right to freedom of expression and privacy. Ranking Digital Rights encourages ICT companies to help mitigate the danger that high-risk users face.

We have drawn up the following risk scenarios in consultation with stakeholder groups, including such high-risk users. We hope these scenarios will help illustrate the type of harms that people can experience and that we seek to prevent when we ask companies to respect users' rights to freedom of expression and privacy.

The Risk Scenarios

Note: "Key questions" listed below highlighted with a grey background were incorporated into the RDR Phase 1 methodology. Questions not highlighted were discussed during the course of methodology development, but were not directly used. For further information about how we worked with these scenarios during the methodology development process, please see the second part of this document titled "How we used the risk scenarios in the methodology".

Freedom of expression

Scenario #1: Authorities in one jurisdiction demand to censor specific content, but when the company takes down the content, it is censored globally.

Scenario #2: Authorities demand to censor specific content, but instead of disabling access to that specific content, the company blocks access to an entire website or domain.

Scenario #3: Government authorities demand a company remove or filter content. The demand may not be legal in that jurisdiction, and the company fails to challenge the demand.

Scenario #4: The company removes content and fails to inform users that content was removed, why it was removed, and under whose authority (e.g., national law, the company's terms of service) it was removed.

KEY QUESTIONS (applicable to all of the above scenarios):

- When the company responds to a request to block or remove content, does it inform the user who published the content about the reasons for its removal?
- Does the company provide a clear explanation to users trying to access the content about why the content is no longer accessible?
- If the legal situation permits, does the company allow the user to challenge the content removal or blocking decision?

- Does the company have a clear process in place to evaluate the validity of government requests and determine who in the company is responsible for deciding how to respond?
- Does the company determine whether a demand for content removal, filtering, or blocking was conveyed in a legally binding manner?

- Does the company have adequate legal counsel that enables it to evaluate the legality of requests in all jurisdictions where the company has an operating base, and does it obtain adequate legal counsel when legal requests come from other jurisdictions?
- In cases where the company decides to carry out a request, does the company have a mechanism to block content that is illegal in one or more jurisdictions, just for those jurisdictions, while keeping it accessible to users in other jurisdictions where it is legal?
- In cases where the company decides to carry out a request, does the company have a mechanism to block only the specific offensive content, rather than blocking an entire website or domain?
- If the legal situation permits, does the company allow users to remove the content in question themselves?

Scenario #5: Network shutdown – The government demands that the company shut down all service to a specified area – a city district, a particular city or province, or even an entire country.

KEY QUESTIONS:

- Does the company carry out a human rights risk assessment – including an assessment of the likelihood that the government could make such demands, particularly in the context of a political crisis or civil disturbance – before entering a market?

- Does the company make an effort to embed provisions consistent with respect for fundamental human rights, including free expression, into its operating licenses with governments and their contractual agreements with business partners?
- Does the company put procedures and practices in place in advance so that if the government requests a network shut-down, the company has a clear plan for handling the situation?
- Does the company have a clear chain of responsibility for decision making in such situations?
- Does the company have procedures and practices in place to inform the public (as soon as possible and, in any case, no later than the commencement of the shutdown) of the circumstances under which the government forced it to shut down a service in a particular area?

Scenario #6: A government's filtering policy requires the company to block specific websites or applications, and the company fails to inform users of this policy when they try to access the blocked websites or applications. (This notification is usually done by displaying a customized "block page" or "error page" indicating that the content has been blocked. It typically identifies who required the block and under what authority.)

KEY QUESTIONS:

- Does the company make maximum efforts to inform the user of why and according to what authority, law, or regulation any given piece of content was blocked?
- Does the company determine the maximum extent to which it has the legal right in the given jurisdiction to inform users of instances where filtering has occurred on government demand?
- Does the company publish regular updates on the number and nature of government filtering requests it received, and the percentage of requests with which it complied?

Privacy

Scenario #1: The company receives a legally binding order to give police private content or data pertaining to a political activist, journalist, or persecuted religious minority, and it complies.

Scenario #2: The company fails to challenge government requests for user information that are over broad and/or of questionable legality in that government's jurisdiction.

KEY QUESTIONS:

- Does the company carry out a human rights risk assessment -- including questions about the company's expected involvement in surveillance by state authorities and about that country's human rights record -- in each market where it has an operating base before starting to do business in that country?
- Does the company have a clear process in place for evaluating government requests and determining who in the company is responsible for deciding how to respond?
- Does the company regularly publish information about the volume and nature of government requests it received and the percentage of requests with which it complied?
- Does the company provide its users with accessible and comprehensible information about what jurisdiction their data is being stored in, under what circumstances it could be shared with authorities, and with which country's authorities it could be shared?
- Does the company have adequate legal counsel that enables it to evaluate the legality of requests in all jurisdictions where the company has an operating base, and does it obtain adequate legal counsel when legal requests come from other jurisdictions?

Scenario #3: Users' private contacts and/or private communications are suddenly revealed publicly (hence to authorities and other adversaries) without adequate user notice or knowledge.

KEY QUESTIONS:

- Does the company carry out thorough privacy and human rights impact assessments to determine whether and how those vulnerable user groups most susceptible to human rights violations would be affected by the settings change or new product/service?

- If stakeholders identify severe privacy and human rights risks shortly after a new product roll-out, feature addition, or settings change, does the company work to remedy the problem as quickly as possible?

Scenario #4: The company fails to notify users user or obtain consent to share user information with authorities in situations where the company is within legal rights to notify users or obtain their consent.

KEY QUESTIONS: (In addition to above)

- Does the company establish clear procedures and processes for staff response to government requests?

- Has the company made clear efforts to understand the law and receive legal advice, both generally and specifically, regarding corporate obligations to law enforcement and also users' legal rights?

Scenario #5: Real time interception – Authorities intercept text messages sent to arrange an opposition meeting, journalist interview with whistleblower lead, or banned religious meeting, and arrest, detain, or threaten participants.

Scenario #6: Due to easy access to commercial network traffic, police are able to compile comprehensive archives of every user's emails, chats, general online activity in a country, violating individuals' privacy and posing risks to vulnerable users such as activists, investigative journalists, and leaders of religious minorities.

KEY QUESTIONS (in addition to above):

- Does the company try to anticipate prior to market entry (through a human rights impact assessment) if authorities are likely to demand blanket access to company equipment, facilities, or networks, and whether it would be possible to respond in a manner that limits human rights risks to users?
- Has the company deployed the highest possible level of encryption and security features for its products and services to safeguard the integrity of its network?

- Does the company publish regularly updated information about the nature and legal basis of all (mass) intercept requirements made by governments? If the company is prevented from doing so, does it publish a clear explanation of the law(s) preventing it from doing so in each jurisdiction?
- Does the company make an effort to embed provisions consistent with respect for fundamental human rights, such as freedom from blanket surveillance, into its operating licenses with governments and their contractual agreements with business partners?
- Does the company screen sensitive personnel to limit an individual's ability to infiltrate the company's network and compromise its integrity.?
- Does the company have whistleblower procedures and protections in place to ensure employees can report misconduct without fear of retribution?

Scenario #7: A legal jurisdiction requires the company to retain data about its users' online behavior for a limited period of time. After the time period elapses, the company retains this data, due to neglect, commercial purposes, or other reasons. When a security breach occurs (either during or after the data retention period), the users' personal data (IP addresses, websites visited, possibly messages sent) are made publicly available.

KEY QUESTIONS:

- Does the company communicate to users exactly what data it stores about them, and for how long?
- Does the company have proper security procedures in place to prevent unauthorized access to user data?
- Does the company make sure to permanently destroy all user data immediately when the legally required retention period ends?

Scenario #8: A user's computer is infected with malware after the user opened a malicious file that they received through a cloud-based file sharing service.

KEY QUESTIONS:

- Does the file sharing service or e-mail provider educate its users about phishing attempts and how to avoid opening malicious files?
- Does the file sharing service or e-mail provider scan for viruses?
- Does the file sharing service or e-mail provider offer an option to preview files without downloading them onto the user's computer?

Scenario #9: Lack of encryption and proper security mechanisms enable (government or non-government) intruders real time or historical access to user messages on a mobile messaging platform.

KEY QUESTIONS:

- Does the company use SSL encryption for transmitting messages between users directly or between users and the company's servers?
- Does the company put stringent security measures in place to protect communications, including encrypting all user data (including messages), stored on its servers?
- Does the company allow users to permanently delete stored communications for a given time period (e.g., messages that are older than one week, one month, three months, one year, or all stored messages)?

Scenario #10: A web platform is hacked due to the platform's inadequate security practices. The website had required users to register in order to access basic content. As a consequence of the intrusion, hackers obtain a list of users' e-mail addresses and unhashed passwords. The hackers sell this information to spammers and to an authoritarian government. Like many Internet users, a human rights defender in the authoritarian country is using the same password on multiple websites, including this platform and their e-mail account. As a consequence, security services in the authoritarian country access the user's e-mail account, her list of contacts, and e-mail history. The user is arrested for state undermining activities, and so are several of her e-mail contacts.

KEY QUESTIONS:

- Does the web service that stores personal information (e.g., e-mail, messages, personal files) offer two-step verification or similar non-password security mechanisms?
- Does the web service that stores personal information (e.g., e-mail, messages, personal files) offer an overview of recent account activity (moments and IP address)? Does seeing this recent account activity require an additional security step?
- Does the website require users to create accounts to access basic, unpaid functionality that doesn't require personalization?
- Does the e-mail service clearly inform users of every method by which their e-mail can be read at the moment (e.g., POP, IMAP, forwarding, etc.)?
- Does the service allow users to permanently delete all stored data that is older than a given time period? (e.g., data that is older than one week, one month, three months, one year, or all user data)

Scenario #11: A social network requires users to use their real names and to make their profiles public (and searchable by search engines). As a consequence, the online and offline identities of high-risk users are automatically connected, which can expose them and the people to whom they are connected.

KEY QUESTIONS:

- Does the company require user's profile names to be their real name?
- Does the company enable users to create a profile that is not publicly viewable?
- Does the company give users complete control over who sees their data (e.g., photos, status updates, messages, contacts)?
- Does the company allow users to permanently delete stored data that is older than a given time period (e.g., data that is older than one week, one month, three months, one year, or all stored data)?

Scenario #12: A user who is logged in to a company's website for one service is automatically signed into other online services of the company without explicitly intending to do so. For example, when the user is logged in to the company's e-mail service, the user is automatically also logged in to its search engine, document sharing platform, etc. When an intruder gains access to this account (for example as a consequence of the user's or company's lax security practice), a web of personal data is exposed.

KEY QUESTIONS:

- Does the company offer users the choice whether to use their account with one service to automatically sign in to other company services? In other words, does the company allow users to opt in to integrate profiles across different services, or is there a simple way to opt-out of such integration?

How we used the risk scenarios in the methodology

As part of the methodology development for Ranking Digital Rights, we identified specific "human rights risk scenarios" for users of Internet and telecommunications platforms and services worldwide.

The section below highlights a few key questions that were drawn from the scenarios and that were integrated as indicators in the ranking methodology. Rather than giving an exhaustive list of questions or elements included in the methodology, this section explains how we used the risk scenarios to develop those indicators. For a more comprehensive overview, elements that have in some manner been incorporated into the methodology have been highlighted in the risk scenarios above.

It is important to note that several questions that stakeholders and members of the project team found important were nonetheless left out of the ranking methodology due to the decision to include only publicly available information. (Please see the paper summarizing the case study research process for more information about how the methodology was developed.) During our methodological research and development phase, we found that some of the questions listed in the risk scenarios would be impossible to answer without active company participation in the ranking or technical investigations beyond the scope of this project's resources. Other questions arising from the risk scenarios did not make it into the ranking methodology for various reasons: their inclusion seemed less critical for protecting users' rights; they were specific to particular companies and not applicable to many of the companies we will include in the ranking; or because we had to prioritize and limit the methodology to a manageable scope.

The risk scenarios fell into two major categories: freedom of expression and privacy. The bullet points below include relevant questions from the human rights risk scenarios, and, in parenthesis, the related indicator in the Phase 1 Pilot methodology.

Freedom of Expression

One human rights risk scenario describes a situation where a company fails to challenge legally dubious demands from government officials to block or filter content. In other scenarios, a company removes content (either at the request of a government or through the enforcement of its own terms of service), but does not inform users that it removed the content, why it did so, and/or under whose authority it happened. Several questions that came out of these scenarios were incorporated as indicators in the pilot ranking methodology, including:

- Does the company have a clear process in place for evaluating the validity of government requests and determining who in the company is responsible for making the decision about how to respond? (**F3**)
- If the legal situation permits, does the company allow the user to challenge the content removal or blocking decision? (**G11**)
- Does the company provide clear explanation to users trying to access the content about why the content is no longer accessible? (**F8**)

Privacy

Stakeholders we consulted tended to focus primarily on human rights threats posed by governments. Several risk scenarios described situations whereby a company hands over the private data of a human rights defender, journalist or other targeted individual to government authorities upon receipt of legally binding order.

Four questions came from such scenarios and later helped us to formulate indicators:

- Does the company carry out a human rights risk assessment -- including questions about the company's expected involvement in surveillance by state authorities and about that country's human rights record -- in each market where it has an operating base before starting to do business in that country? (**G1**/**G2**)
- Does the company provide its users with accessible and comprehensible information about what jurisdiction their data is being stored in (**P7**), and under what circumstances it could be shared with authorities, and with which authorities it could be shared? (**P8**)
- Does the company establish clear procedures and processes for staff response to government requests? (**P9**)

Other risk scenarios dealt with the question of whether companies make any effort to protect users against surveillance (by any party with the technical means) undertaken without lawful requests or formal due process. One indicator that came out of such scenarios deals with the company's security practices:

- Has the company deployed the highest possible level of encryption and security features for its products and services to safeguard the integrity of its network? (**P23**)

As mentioned above, some other relevant questions were not incorporated, as they were impossible to research based on publicly information. This was especially the case when we learned that companies would rarely be able to divulge certain information, often due to legal constraints. One such example dealt with operating licenses:

- Does the company make an effort to embed provisions consistent with respect for fundamental human rights, such as freedom from blanket surveillance, into its operating licenses with governments and their contractual agreements with business partners?

The risk scenarios also described situations where companies can help users protect themselves, for example, when a user's computer is infected with malware or when a user's e-mail account is hacked. High-risk users are often the target of such digital attacks not only by criminals but also by governments. Such attacks can expose users' professional and personal information and pose danger to users' networks of contacts. From such scenarios we derived questions looking at the security features and education that companies offer their users, including:

- Does the file sharing service or e-mail provider educate its users about phishing attempts and how to avoid opening malicious files? (**P24**)

- Does the web service that stores personal information (e.g., e-mail, messages, personal files) offer two-step verification or similar non-password security mechanisms? (**P24**)

- Does the web service that stores personal information (e.g., e-mail, messages, personal files) offer an overview of recent account activity (moments and IP address)? Does seeing this recent account activity require an additional security step? (**P24**)

Questions highlighted in this paper have helped us think through how particular company policies and practices affect the freedom of expression and privacy of high-risk users, and what the best practices for limiting negative impact should be.