Human Rights Baseline Assessment for Small and Medium Sized Technology Companies: Assessing risks relating to privacy

January 2020

GLOBAL PARTNERS DIGITAL

OPEN TECHNOLOGY INSTITUTE

Contents

Introduction

This section of the tool is designed to help you assess how your company's operations and practices may pose risks to the right to privacy. Although you have already answered some high-level questions on this topic, these questions are designed to help you evaluate these risks at a deeper level. Please note that some questions may be similar to questions you answered in Part 1 of this assessment. This is so you have all the relevant information on a given topic in one place. The topics covered by this section of the tool include data protection, data collection, data retention, data sharing, and data security.

Acknowledgements

We would like to thank Michaela Lee from Business for Social Responsibility and Evelyn Asward from the University of Oklahoma College of Law for their support in reviewing and creating this human rights impact assessment tool.

This tool was developed by New America's Open Technology Institute and Ranking Digital Rights as part of a consortium of organizations working on promoting business and human rights in the tech sector to advance internet freedom.

Assessing risks to privacy

Data Protection

Data protection policies are crucial to protecting the privacy and human rights of customers or users. Given the amount of data that companies collect and use, thinking carefully about managing user data in the context of a country's human rights landscape is important to help mitigate risks that could affect customers, stakeholders, and even employees of a company. Each country in which a company operates may have a different set of data protection laws and regulations, with some reflecting more heightened concern than others. The governments of some countries may themselves pose risks to customers' privacy rights. In addition, the legal requirements for safeguarding customers' data will vary from country to country. For example, operating in the EU, which has a strict set of data protection requirements under the General Data Protection Regulation (GDPR), is different than operating in a country where there are requirements that companies be able to provide unencrypted content of all user data upon government request. Evaluating the human rights landscape with advice from legal counsel and external stakeholders versed in international human rights law is crucial to developing policies that protect users from privacy risks.

The following questions are designed to help you assess the current state of your policies and practices related to data protection.

*

1. **Are you subject to any domestic or regional laws or regulations governing data protection or data privacy? (e.g. GDPR).**

a) If yes, please list relevant laws or regulations.

b) Have you evaluated how compliance with these laws or regulations might affect your activities in collaboration with legal counsel?

c) Have you evaluated how compliance with these laws or regulations might affect your activities in collaboration with external stakeholders?

2. Are you aware of specific or heightened human rights concerns surrounding data privacy in any of the countries in which you operate? (e.g. lack of legal protections for individual privacy and human rights or demonstrated technical surveillance of targeted groups).

a) If yes, have you evaluated how these human rights concerns could affect your customers or relevant external stakeholders in collaboration with legal counsel?

b) Have you evaluated how these human rights concerns could affect your customers or relevant external stakeholders in collaboration with external stakeholders?

Data Collection

Data collection directly impacts user privacy, and users should be able to choose whether to use or not use a product or service based on the information it collects. For example, if users are notified that a product/service collects location data, they may either choose not to engage with that product/service or to take steps that mitigate the privacy impact of that collection. Data collection can also have other serious human rights impacts. Data breaches, accidental or as a result of hacking, could expose private information on users, or data could be requested by third parties like governments or non-governmental actors and be used to target groups and individuals.

Most companies collect some form of data on their customers. The most basic is contact information for the customer, like name, email address, and potential physical address. If users sign up for an account, purchase a product, or provide information to receive mail or email, that company likely collects some sort of user data to accomplish that activity.

A company that collects information should have a publicly available data collection policy. This could be posted on a website, or distributed with other legal documents, but this policy is important to provide transparency and protect the security and privacy of customers or users. A good data collection policy notifies customers about what types of information are being collected (e.g. personal, communications content, location, biometric, and network), and when and how it is being collected.

Further, it is a best practice to minimize data collection, and only collect the information your company truly needs to support your products and services. Where possible, companies should make the collection of data optional for use of the product and allow users to “opt in” to data collection; alternatively, features could be included that allow users to turn on or off features that involve data collection, such as real-time data collection.

The following questions are designed to help you assess the current state of your policies and practices related to data collection.

1. **If your company collects user data, do you have documentation available that identifies what data is being collected and when?**

   a) Where on your website or platform are these policies or rules listed?

   b) Do you specifically highlight or communicate changes to these policies or rules to users (e.g. through blog posts or email updates)?

   c) Do you offer a public archive where users can see how these policies and rules have changed over time and reference old policies?

2. **Is submission of user data required in order to use your product or service?**

   a) If yes, what types of data are required?

   b) If yes, are any verification tools used to confirm whether the information is valid?

c) Do these tools use contact information (e.g. send a confirmation email or text a code) to verify an account?

d) Do these tools use government information (e.g. a social identification number, or an image of government ID) to verify an account?

3. Do your customers have a meaningful opportunity to opt in or out of the collection of specific types of personal data?

a) If yes, what types of data are covered by the opt in or opt out mechanism?

b) Is this feature or service clearly available to users?

c) Is the customer able to access core functions of the product or service if they opt out of certain types of data collection?

Data Sharing

Companies that collect any form of data may be called upon to, or decide to, share that data with other actors. This data sharing could pose significant risks to the privacy of their users, especially when that information is shared with government or law enforcement agencies.

Although data sharing has always been possible, the growing amount of information collected by companies make this data sharing more and more impactful, and expand the ways that privacy infringements could impact the lives of their customers. In some instances, governments may require companies to share certain data in a regular manner, or even to install equipment that allows governments to access data at will.

In other instances, governments may use legal mechanisms, like warrants, to force companies to share specific user data, content, or other related information. They can also combine information from various sources to gain deeper insight on individuals. These governments may not have legal regimes that are sufficiently protective of privacy and other human rights. As technology has advanced, companies now have even more sophisticated and granular data that could be requested by governments. Instead of turning over the phone number or email of a user, a company may be able to share information as to where that customer has traveled in real time. The ability to track physical location or biometric data is much more invasive, and can be easily abused. Government demands should be reviewed using a human rights framework to consider whether they are lawful, overbroad, or otherwise beyond the scope of information allowed to be requested.
In order to ensure that the right to privacy is respected in such scenarios, companies should establish and enforce clear policies for considering legal requests for user data.

At the same time, companies who independently decide to share data with non-governmental third parties, such as advertisers, create other privacy risks. Many companies have troves of information that can paint a far more accurate picture of an individual's life than ever before. Selling user information, or sharing it with related companies, can create serious potential impacts on user privacy. The processes that companies employ for sharing information might be completely unknown to customers. Not only could they be surprised, and their privacy put at risk, when they receive advertisements or other information from third parties that clearly possess their user information, but they may be exposed to an increased risk of their information being subject to a data breach, including from companies that they did not know were in possession of their personal information.

The following questions are designed to help you assess the current state of your policies and practices related to sharing of customer data.

*

1. **Are you subject to any domestic or regional laws or regulations related to government access to user data? (e.g. Australia’s Assistance and Access Act of 2018).**

2. **Does your company have an individual or team responsible for managing requests for user data, whether from government or third parties? If yes, describe who they are, where they are situated in your organization, and if they have training in international human rights law and/or have access to experts who can provide assistance in adhering to best practices (e.g. the UN Guiding Principles on Business and Human Rights).**

3. **Do you have documentation available that identifies what data is/can be shared, with whom, and under what circumstances?**

a) Are these policies or rules available to users?

b) Do you specifically highlight or communicate changes to these policies or rules to users (e.g. through blog posts or email updates)?

c) Do you offer a public archive where users can see how these policies and rules have changed over time and reference old policies?

4. Do you share data with government actors?

a) If yes, is this sharing the result of legal requests (e.g. warrants, subpoenas, or other judicial orders)?

b) If not, please describe the circumstances under which you share data with government actors.

c) Do you consult in-house or external legal counsel and/or other external stakeholders on receipt of these government requests?

d) Do you assess whether legal requests are overbroad or otherwise beyond the scope of legally-permissible requests?

e) Under what circumstances, if any, have you challenged government legal requests to share user data? For example, have you challenged any such requests on the grounds that they are not clear, they are not legal under the relevant domestic laws of the country concerned, that they are not legal given that country's international human rights law obligations, or on any other ground?

f) Do you notify users (if legally permitted to do so) when their data is shared with government actors?

g) Are there any legal restrictions that may prohibit you from notifying users that their data has been shared with government actors?

5. **Do you share data with non-governmental third-party actors (e.g. other companies)?**

a) Under what circumstances do you share data with third parties?

b) Do you have written policies establishing clear guidelines for when you will or will not share data with third parties and/or what limitations you may consider contractually imposing upon the use of that data by those third parties?

c) Do you consult legal counsel and/or external stakeholders when choosing to share data with non-governmental third-party actors?

d) Do you notify users (if legally permitted to do so) when their data is shared with non-governmental third-party actors?

e) Are there any legal restrictions that may prohibit you from notifying users that their data has been shared with non-governmental third-party actors?

Data Security

Effective data security practices involve both securing data on the company side to prevent a breach of customer information, and providing customers with best practice tools like multifactor authentication for their own digital security.

The following questions are designed to help you assess the current state of your policies and practices related to data security.

*

1. **Does your company have an individual or team responsible for managing digital security? If yes, describe who they are, where they are situated in your organization, and if they have training in international human rights law and/or have access to experts who can provide assistance in adhering to best practices (e.g. the UN Guiding Principles on Business and Human Rights).**

2. Does your company publicly disclose information about what data security best practices your company uses?

a) Where on your website or platform are these policies or rules available?

b) Do you specifically highlight or communicate changes to these policies or rules to users (e.g. through blog posts or email updates)?

c) Do you offer a public archive where users can see how these policies and rules have changed over time and reference old policies?

3. Does your company use data security best practices for the protection of data?

a) Do you use encryption for all communication in transit?

b) Do you use encryption for all data at rest?

c) Do you make available multi-factor authentication for employees and customers?

d) Do you require the use of multi-factor authentication for employees and customers?

e) Do you maintain current patches for all software?

f) Do you have policies for notifying customers in case of a data breach?

g) Do you have a mechanism established through which people can alert your company about security vulnerabilities that they detect?

4. Are you aware of any legal restrictions in the countries where you operate that limit the types of data security protections you are able to provide your users? (e.g. restrictions on strong encryption or government data access requirements).

Data Retention

Governments may require certain companies to retain particular types of data for specified periods of time. Companies that collect any type of user data should have a publicly available data retention policy that explains what legal requirements it is obliged to follow and what additional steps they may take to address the risks related to data retention.

This is important both for transparency to customers who can benefit from knowing how their data is handled, and also to evaluate the data breach concerns caused by the collection of user data. Privacy-protective best practices for user data include minimal data retention, and clear time limits for retention of user data.

This is also a trend in international data privacy discussions, with the GDPR stating that "personal data may only be kept in a form that permits identification of the individual for no longer than is necessary for the purposes for which it was processed."

The following questions are designed to help you assess the current state of your policies and practices related to data retention.

*

1. **Do you have policies outlining how long your company retains the various types of information or data relating to, or generated, by your users?**

a) If yes, do you differentiate various types of personal information? For each category, how long is that information retained?

b) For what purposes is that data retained?

c) Is data retention required and/or limited (i.e., vis-a-vis the duration of retention) by law?

2. Do you make documentation publicly available that identifies what data is being retained, when, and for how long?

a) Where on your website or platform are these policies or rules available?

b) Do you specifically highlight or communicate changes to these policies or rules to users (e.g. through blog posts or email updates)?

c) Do you offer a public archive where users can see how these policies and rules have changed over time and reference old policies?

3. Is information retained after users close an account or otherwise discontinue engagement with your company? If yes, for how long do you retain this information?

4. Do users have the option to request deletion or removal of their personal data?

a) If so, is the process for doing so clearly available to users?

GLOBAL PARTNERS DIGITAL

Second Home
68 Hanbury St
London E1 5JL

+44 203 818 3258