Final Project

Privacy Policy Regulation

Ankith Gunapal

Table of Contents

Highlights of Recommendations

- Privacy Policy Overview: Scope, Availability & Readability
    - Use simple language in the Privacy Policy.
    - Give easy access to Privacy Policy and encourage people to read them.
    - Privacy Policy should have Privacy Policy Rubric in the first page.
- Data
    - Data Accessibility
        - Users should be able to view, download and delete any personal data.
    - Data Collection
        - Data should be physically located in the United States.
        - Don't collect information on others without consent.
    - Data Analysis
        - Organizations are encouraged to use broader data trends.
    - Data Sharing
        - Organization's responsibility to remove data from affiliates and subsidiaries.
    - Data Recession
        - Should be easy to delete any personal data, if a user chooses to.
    - Data Protection
        - Measures in case of data breach.
        - Accountability in case of non-state sponsored data breach.
- Individual Choice and Access
    - Choice in analysis, sharing and recession of data.
    - Users need to be warned in case of default opt-in kind of solution.
- A/B Testing
    - Informed Consent
        - Need consent for any A/B testing related to content.
    - Assessment of Risks and Benefits
        - Participants need to be compensated accordingly.
    - Selection of Subjects
        - Participants should be chosen fairly.
- Privacy Invasion
    - Users must be notified in case of privacy invasion
    - Organization is responsible for any third-party related insights affecting the user.
    - Users can remove any information related to them.

- Privacy Policy Rubric
    - Every Privacy Policy should have a Privacy Policy Rubric in the first page
    - This helps users identify an organization's compliance with the Privacy Policy Regulation.

- Accountability & Enforcement
    - Multi-tier fines in case of violation
    - Maximum penalty of 5 percent of global annual revenue

Problem Statement:

Introduction:

The Belmont Principles [2], FTC Guidelines [3], California Online Privacy Protection Act [4] do a pretty good job of laying out the framework to protect consumer's privacy. However, with rapid advancement in technology, these guidelines fall short of addressing many issues. The goal of the proposed framework is not to impede advancement in technology or discourage new businesses. The goal, instead, is to put the onus on companies to work harder to innovate, without disregarding people's privacy.

Inspiration:

The Belmont Principles touch upon some important points with regards to fairness [2]. Solove's Taxonomy explains the various ways in which people's privacy could be harmed [5]. The California Online Privacy Protection Act [4] does a pretty good job of laying down the basic framework needed in a privacy protection guideline. The EU General Data Protection Regulation [6] has put in some very strict regulations in place to the privacy of EU citizens. The regulations specifically cover cases of data protection, data accessibility and data erasure. It also proposes hefty penalties in case of data breaches.

Solution Framework:

Privacy Policy Overview:

The Privacy Policy document should provide a comprehensive overview of your practices regarding the collection, use, sharing and protection of personally identifiable information [4]. It should, at a minimum, comply with legal requirements for such policies [4].

Scope:

The Privacy Policy should clearly state the scope of what it is covering. For example, it could cover just the online data, one particular service from a range of solutions offered by you. It should clearly indicate if it covers any subsidiaries and affiliates [4].

Availability:

Make the Privacy Policy clearly visible in case of a website. It should be easily spot-able on the homepage. The text with a link to the Privacy Policy should be larger than surrounding text and it should be written with legible font and color. The colors chosen should also not make it hard for majority of the colorblind population to read [4].

In case of a mobile application, the Privacy Policy should be clearly visible on the application download page, users should be given a prompt to read the policy when they click on download. Once the application is installed, users should easily be able to view the Privacy Policy from the home page of the application [4].

Readability:

The Privacy Policy should be written in simple language. It should use short sentences. Important sections of the policy should be clearly highlighted. The Privacy Policy should contain the Privacy Policy Rubric appropriately color-coded as described later.

Data

The Privacy Policy needs to describe in detail all necessary information related to data.
It should clearly highlight and describe each of the following five sub sections with regards to data

Data Accessibility

The Privacy Policy should clearly specify how users can view any data that has been collected by directly by your company or by any other affiliate or subsidiary. Users should be able to view, download or delete any section of the data collected by your company. At the bare minimum, users should easily be able to delete any data collected on them with a few clicks of buttons. If the company wants to give granular control on what kind of data can be deleted, that is up to the company to decide.

Data Collection

The Privacy Policy should clearly specify what kind of data is being collected from the users. There should be a separate section for Personally Identifiable Information. This section should mention all the personally identifiable information that is being collected directly by the

company or by any other affiliate or subsidiary. This section should include any details that can be traced back to any one person. Some examples include Name, address, credit card number, ethnicity, Date of Birth, Data related to electronic devices such as IP address, mac address [4]. You should ensure that any data that is collected on any user in the United States needs to be physically located in the US. If you violate this and you are not able to guarantee the protection of this data, you are liable for a lawsuit.

You shall not collect information on anyone else other than the user making use of your service. Information can be pictures, voice, texts, emails. You are held accountable for any violation of this.

Data Analysis

The Privacy Policy should explain at a broad level what kind of analysis is being done with the data. The policy should indicate if the company is doing the analysis using personally identifiable information or using broad trends. You are encouraged to analyze and recommend services based on broader trends. There is a greater scrutiny over analysis done using personally identifiable information.

Data Sharing

The Privacy Policy should explain how the company is sharing user data with its affiliates and subsidiaries and what regulations it has put in place while sharing data. If a user wants to delete data, it is the company's responsibility to remove the data from the repository of any third party which has been given access to the data.

Data Recession

The company should make all efforts for removal of data very simple and hassle free. The Privacy Policy needs to clearly describe the steps. Also, as stated previously, it is the company's responsibility to remove data from any third-party company who has been given access to a user's data, should the user choose to remove the data.

Data Protection

Explain to the user what measures you are taking to protect user data. Explain what steps are taken in case of a data breach. The penalty for any non-state sponsored data breach is hefty and will be explained later.

Individual Choice and Access

The Privacy Policy should describe the choice a user has with respect to use, analysis, sharing and recession of data [4] These choices must be specified in simple language. The company can decide what is the default option for a service but in case of default opt-in systems, the user should get a clear warning on the screen about the same. The system should consent the user before proceeding. Any choice made by the user should be honored within a reasonable amount of time.

A/B Testing

The Privacy Policy should have a section dedicated to A/B Testing [7]. If you are going to conduct A/B Testing on users, it should be mentioned in the Privacy Policy. You should explain, to the best of your ability, the type of A/B Testing a user can expect.

Informed Consent

For A/B Testing related to the design of a webpage, you are not required to get user consent. However, you need to get explicit consent from the users for any kind of A/B Testing related to content. It is up to you to decide how it gets consent from the users. When a user starts using your platform, it is up to you to make users opt-in or out of A/B Testing. You need to specify in the Privacy Policy how users may opt-in or out of A/B testing. Users must be given the option to be notified of every A/B testing with regards to content.

Assessment of Risks and Benefits

If you want to make use of A/B testing, you may do so by compensating the users who are participating. Compensation need not be monetary. You may compensate participants in the form additional services and features. It is up to the company to decide what is a fair compensation. However, there should not be any discrimination with compensation for all participants within an A/B test.

Selection of Subjects

You should make every effort to choose the participants for an A/B Test fairly.

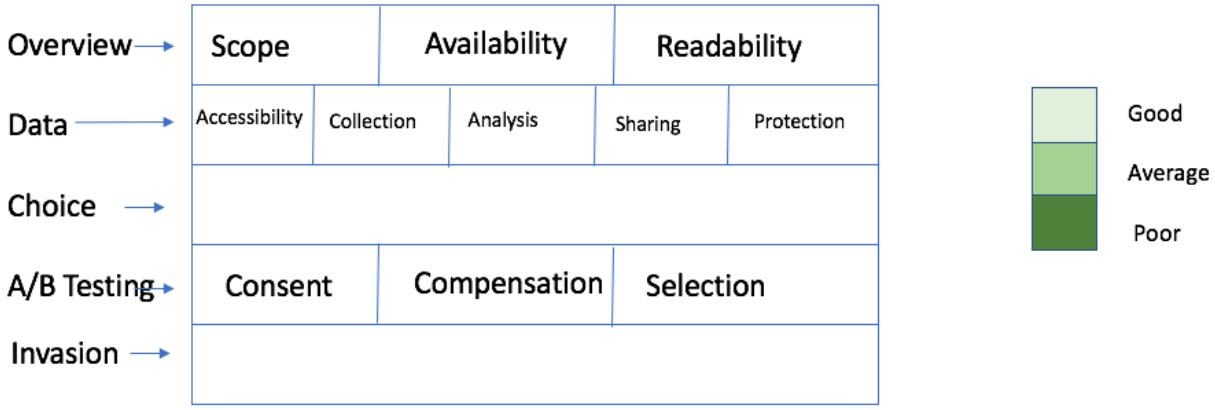
Privacy Invasion

Based on the data analysis done on any user, you might be taking some action on the user for another service. If this is being done, the user must be notified. You may keep the users opted-in by default for this invasion but users must be given the choice to opt–out without a lot of hassle. In case of any insights on a sold to a third party, it is your responsibility to make the third party accountable for removing the information.

If a user is being recommended services or if there is a denial of service because of external data, this needs to be mentioned to the user. This is especially true in cases of analysis done based on close family's data. The user shall have the right to remove any such information if the user chooses to.

Privacy Policy Rubric

The Privacy Policy must have a rubric in the format shown below. You should self-evaluate your ability to implement various points set forth in this document. For example, if you believe, you are doing a good job following the directives with regards to any section, you should fill it with a  . It is up you to define how you define what is good, average and poor. However, in case of a glaring mistake in filling in the rubric, you may be held accountable.



Accountability & Enforcement

Organizations can be charged for violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce [8]

Organizations based out of California can also be charged through California's Unfair Competition Law (UCL), which is located at Business and Professions Code §§ 17200-17209. Under the UCL the California Attorney General's Office, district attorneys, and some city and county attorneys can file suit against businesses for acts of "unfair competition," which are considered to be any act involving business that violates California law. As a result, violations of PPR may be considered violations of the UCL. Government officials bringing suit for violations of PPR may seek civil penalties and equitable relief under the UCL. In addition, the UCL provides that private plaintiffs may assert private claims for violations of PPR under the UCL [9].

Organizations can be fined up to 5 percent of their global annual revenue for breaching the Privacy Policy Regulation. The fines will follow a multi-tier approach, with fines corresponding to the severity of the breach. Consumers may take a quick look at the Privacy Policy Rubric to decide how compliant you are with the Privacy Policy Regulation. Hence, it is in your best interest to accurately represent the rubric. There is a board setup which reviews compliance of the Privacy Policy Rubric. It is up to the discretion of the board to decide what is a violation, on a case by case basis. [6]

References:

1. EU Data Protection Directive
2. The Belmont Principles
3. FTC Guidelines
4. California Online Privacy Protection Act
5. A Taxonomy of Privacy – Daniel J Solove
6. The EU General Data Protection Regulation
7. A/B Testing
8. FTC Enforcement
9. California's Unfair Competition Law Enforcement