**Pourna Sengupta**

**CYBR 4400**

**Unit 5 Assignment**

**4/10/2020**

**Step 1**

Netflix is a streaming platform with millions of users around the world. They collect personal data such as name, email, address, and payment information so that they can provide their paid service to users. Netflix’s most recent privacy statement provides a detailed overview that, with some reading, any user can understand. They provide a thorough summary of information that they collect, including information shared by the user, collected automatically, and information from partners and other sources. For each category of information and subcategories within them, Netflix explains their need for each specific piece of user information and why they collect. They go on to describe how they use each piece of user information and how user experience benefits from this use. They also discuss user settings and other user options such as the “remember me” function, account access, profiles, and device access. In each of these sections, they thoroughly describe what each setting or option/function does and how a user can turn it off or change it. The privacy statement continues on to describe notifications and user choice in how they receive these notifications. Like all other user functionalities, they give details on how to make changes on the user end. Netflix provides users access to their information and the option to “correct or update out-of-date or inaccurate personal information” [1] by either changing information on the user side or contacting Netflix. The privacy statement describes their use of cookies and other technologies as well and describes why they use them in order to provide transparency to their users. Netflix fails to provides users with an understanding of how their data is secured and what specific measures they use but they do state that they have measures in place.

Tik Tok is a social media app that allows users to view and upload original content. Users create accounts and follow other users such as friends and influencers. They also choose interests when creating their account so that Tik Tok can show them content similar to their interests. Tik Tok provides users with a lengthy privacy policy that shows previous policies and new updates. Like Netflix, they distinguish between information provided by the user, shared by other sources, and collected automatically. A concern about Tik Tok is the amount of information they collect. Unlike Netflix, they fail to provide reasons for collection of certain user data which could raise issues amongst users. Tik Tok collects data from Social Media that is linked to the app, advertising/analytics partners, and other users (through customer service inquiries). What is even more concerning is the data they collect automatically through users devices. This includes device information and location data that collects information regarding your IP address, location, device identifiers, time zone, screen resolution, app and file names and types, keystroke patterns or rhythms, amongst many other identifiable data. Though Tik Tok does clearly state the types of data they collect, they completely fail in explaining usage of this data or reasoning behind their extensive collection. What they do provide is a ‘general’ description of usage. This includes a long list of reasons why they may collect data, but does not relate these reasons to specific data types. Much of their data sharing seems to be when users access third-party services and apps, which could be done unknowingly on the user end. Tik Tok allows users to submit requests to delete their information or access it. Furthermore, Tik Tok provides users with a general list of their choices in data collection such as “limiting ad tracking”, “do-not track” or switching off GPS location information [2]. Like Netflix, Tik Tok fails to provides users with an understanding of how their data is secured and what specific measures they use but they do state that they have measures in place.

Symbolab is an educational site that contains many resources for students studying math. They provide lessons and practice problems as well as a problem solver that shows students how to solve a problem step by step. This service does not require an account and is available to all users on the internet. Symbolab keeps their privacy policy short and easy to understand for all users. They provide a simple description of what, when and how they collect and user personal user information. They provide simple but detailed explanations of how a user provides their information and which functionalities provide this information. Unlike Netflix and Tik Tok, Symbolab goes one step further and describes how they protection user information including scanning for security holes and vulnerabilities, Malware scanning, and their use of secure networks. They also state that they user Secure Socket Layer (SSL) technology. Lastly, they state that “all transactions are processes through a gateway provider and are not stored or processed on our servers.” Though users may not have thorough understanding of all of these security measures, Symbolab provides users with enough detail so that they feel safe sharing data with the platform. Symbolab states that they “do not sell, trade, or otherwise transfer to outside parties” [3] user information without advanced notice. They state that Google AdSense Advertising is used on their website and they provide thorough description of how it is used and what information they share with Google. Symbolab also provides directions on how to opt out of this. Another section included in their privacy policy is description and details of measures they take in order to comply with Fair Information Practices Principles. They clearly state policy regarding action for possible data breaches and discuss individual rights regarding failure to protect user information.

**Step 2**

First and foremost, a concern regarding transparency and information/data protection is the lack of uniformity in sections regarding data security in each privacy policy. Symbolab provides users with a detailed understanding of security measures regarding personal data. Both Netflix and Tik Tok, platforms which collect much larger amounts of data and have many more users, fail to disclose the same level of detail in their security measures. Secondly, Tik Tok fails to provide users with the same level of detail and direction for user choice as Netflix and Symbolab do. Netflix and Symbolab provide users with steps on how to make changes on functionalities and settings they have a choice in. Tik Tok provides a list of what choices users have with no steps on how to change them. This essentially takes away the transparency provided by the platform in how users can change settings or other functionalities and protect their data.

**Step 3**

One of the main technologies used by platforms are cookies. All privacy policies state their use of cookies, what they do, and user rights to disable or limit their tracking. Netflix’s privacy statement provides users with a list of the technologies used by their platform which include cookies as well as web beacons and resettable device identifiers. These technologies help platforms collect user data in order to provide users with a better, more personalized service. Discussing technologies used by platforms such as cookies allows users to better understand which third-party services have access to their data and how it may be protected.

**Step 4**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Description of Attribute** | **Status Quo** | **Policy Option 1** | **Policy Option 2** |
| **User Readability** | Ease of reading and understanding by users. | Up to platforms on how they choose to share their privacy policies with users. | Up to platforms on how they choose to share their privacy policies with users. This must be done in an easy to read, simple fashion with a possible page/word limit. | Platforms must provide users with details regarding how, when, and why specific personal information and data are being used. This must be done in an easy to read, simple fashion with a possible page/word limit. |
| **Security** | User understanding of security measures regarding personal information and data protection. | Organizations and managers of systems are responsible for the reliability and security of their systems and for the damage done by them. | In addition to the status quo, platforms must have at least 2 security measures taken to protect user information and data. They must also have guidelines on how data is stored and secured including access rights. This does not have to be shared with users. | In addition to the status quo, platforms must provide users with at least 2 descriptions of security measures taken to protect user information and data in their privacy statement/policy. They must also state details on how data is stored and secured, including access rights. |
| **Usability** | Users ability to user privacy statement/policy to make choices and changes within their own settings and functionalities. | Individuals have fights of access, inspection, review and amendment to systems containing information about them. | Platforms must provide a link or description of how users can access or change the setting or functionality. | Platforms must provide a link or description of how users can access or change the setting or functionality as well as steps on how to do so once they’ve reached the link. |

**Step 5**

The three factors used for evaluation of policy options are directly from the Fair Information Practice Principles (FIPPS). The five categories they use to maintain privacy law in the United States must be upheld by all privacy statements/policies and therefore are defining factors in policy changes.

Firstly, the security of user data and information is of utmost importance as platforms are responsible for collected data. The first policy option requires platforms to have a minimum of two security measures in place to protect user data and information as well as guidelines on data storage, security, and access. By not sharing this in their privacy statement/policy, platforms may be able to protect themselves from data breaches as their security measures are unknown and therefore less vulnerable. The second policy option requires platforms to define their security measures in detail as well as the storage and access of user data. This policy change essentially forces all platforms to have adequate security measures in place in order to adhere to the policy.

The second factor for evaluation is transparency with users. The first policy option loses transparency with users, as it does not disclose security measures with users. User readability, transparency in security, and usability in the second policy option all allow for increased transparency. By improving user readability, platforms provide users with detailed information regarding how, when, and why their data is used allowing them to fully understand their platforms need for user data. Transparency regarding their security measures gives users more trust in sharing data with the platform allowing them to improve their services based on user data and feedback. By improving the usability of their privacy policy to users, platforms provide their users with transparency in user choice and how to access those rights.

Lastly, the third factor for evaluation include both data and information protection. As discussed, with improved transparency in security, platforms are required to have adequate security measures in order to adhere to the policy on privacy statements/policies. This measure protects user data and information alongside increased usability. By giving users clear details on choice and rights, users can further protect their own data if they so choose to. When comparing security between policy option one and two, the first allows for increased security. Data breaches are less possible as information on security measures are not as readily available to the public.

By evaluating the three factors, security, transparency, and data/information protection, policy option two provides users with an increase in all three categories. Though policy option one allows for possibly better security and data/information protection, it loses some transparency with users. Platforms can easily combat security concerns when sharing security information with users by implementing further measures, increasing both security and data/information protection. Because of this easy solution to the loss of transparency from policy option two, the second option improves all three factors of evaluation.

[1] <https://help.netflix.com/legal/privacy>

[2] <https://www.tiktok.com/legal/privacy-policy?lang=en>

[3] <https://www.symbolab.com/public/privacy.pdf>