Dan Ortiz
W231 Spring 2021 4:00 PM
Spotify USA
https://www.spotify.com/us/legal/privacy-policy/

Privacy seems to be about everything, and therefore it appears to be nothing (Solove, 2002). The concept of privacy is thrown around in many different contexts and is interpreted as many different things making it difficult to gauge when harm is done(Solove, 20021). To assist customers on their choice to use a service, companies developed privacy policies which inform the customer on what data is collected and how it is used. Although privacy policies are intended to be read and understood by the average user, customers can still miss key details in, or omitted, from the policies. Spotify is a multinational player in the music streaming service. Analyzing their privacy policy, will provide key insights into how privacy policies fall short of its intent; the average user should be able to fully understand what data is being collected and how it is being used.

The privacy policy is a legal requirement to maintain compliance with CalOPPA and the GDPR. The intent of these documents is to increase the level of transparency on what data is collected, how it is used, and to inform individuals so they can make an informed decision on utilizing a service. In addition, these statements are required to remain in compliance with both CALOPPA and the GDPR (Writing a GDPR-compliant privacy NOTICE, 2019). Since Spotify is a global company, it must comply with both of these regulations. Spotify's privacy policy covers: 1) The users rights, access and how to exercise these rights, 2) Personal data collected from the user and third parties about the user, 3) What the data is used for, 4) The legal basis for the data collection, 6) Who the usere's data may be shared with, 7) Retention and Deletion, 8) Data Transfer, 9) Children, and 10) Security. In addition, the document is written in "normal" english,

mostly free from legal jargon. In short, a cursory review of Spotify's privacy policy appears to be aligned to these regulations.

Spotfiy's customer expectations generally align with what the company outlines on its privacy policy. At its core, Spotify is a web based media rental company, and over the years there have been established norms around data privacy both in the rental space and the internet space. Customers expect their profile, payment, usage, and browsing data to be collected when using the service and disclosed to the appropriate parties. For example, the three individuals in the user panel expected their payment information to be shared with payment processors (for the premium subscription), their usage data to enhance the personalization of the service, their location to confirm content licensing eligibility, and their browsing history to be shared with advertising networks on the free subscription. This is inline with Nissenbaum's concept of Contextual Integrity; the digital world is part of daily life and the social norms of data privacy in the real world should be reflected in the digital world (Nissenbaum, 2011). Unfortunately, a few aspects of this policy violates this concept.

Spotify collects data and uses it in ways customers do not expect or fully understand. One of the panelists noticed that Spotfy logs all the internet enabled devices connected to any network in which a single device uses its service. Another panelists raised a concern on how her usage data would be used to detect fraud, and the third was concerned about how Spotify could report voice data to law enforcement. A few of the panelists raised concerns about how data is shared with researchers and wanted further clarification on this aspect of the policy. In addition, the panelest all conveyed an expectation that the data collected and shared with advertisers would be limited in the premium plans. Spotify's policy does not explicitly note any data collection differences between free and paid users. In addition, panelists had different levels of expectations on data syncing between authentication providers (i.e. Facebook or

Google). Although the policy indicates user consent is required to transfer data between the services, it does not go into detail if it is a one time transfer or if data will sync across services. The gap between users expectations and Spotify's practices runs a high risk of violating users expectations and thus installing a feeling of invasion in their customer.

To use Spotify's service, customers must consent to providing user data to initiate an account and to pervasive surveillance while using the application and its features. This data, along with data purchased from third parties, is then aggregated and identified to build unique profiles for its users. Spotify frames this as a feature which enables personalized service, a feature that members of the panel cited as a reason why they use the service. Spotify uses the customers' location data to confirm eligibility for both media licenses and service plan eligibility. In addition to servicing customers, Spotify leverages this data for targeted advertising, troubleshooting, and business planning. With the exception of the secondary uses in research and development, the panelist felt this collection and use of data was fair and did not violate expectations, however they expressed concerns on how Spotify will keep their data safe. The panel's concerns are not unfounded. Spotify had three data breaches in 2020 alone (Spotify data breached, 2020). This unintended, unauthorized dissemination of users data leads to a breach of confidentiality and the disclosure could cause harm to its customers.

The data spotify collects has the potential to cause real harm if the data entrusted to the company is misused. The first of these concerns is the unauthorized access to a customer's profile, including payment information. User authentication is required to ensure authorized access and prevent harm to the user including the unintentional disclosure of personally identifiable information. Spotify is legally required to keep its authentication servers secure and private. Unauthorized access can not only result in identity theft but can open up an individual to a social engineering attack. In today's canceled culture society a hacker can cause real social

harm to a user if they alter that user's profile in hanus ways. The failure to protect this information can result in the customer spending time and energy rebuilding their social and financial reputation.

In addition to its core service, Spotify offers voice recognition to its customers which allows them to control Spotify with a simple voice command. Spotify sends the voice data to its servers to transform the command to one that the service can understand and execute. In addition both voice, and its derived data, may be stored by Spotify, which is outlined in a linked document from the privacy policy. No panelst mentioned the link or navigated to it to review Spotify's policies around voice data, leading to concerns that users may not fully understand what they are consenting to and challenging the notion of individual choice/ informed consent. The collection of voice data is rarely limited to just the user, there is a real chance that a bystander or an unrelated conversation is recorded. These bystanders did not consent to Spotify's policies and may not be aware of how Spotify may use their data. This completely violates any notion of individual choice/informed consent. One way Spotify can resolve this is to process the voice data at the device level and only transmit the commands to the server. This would reduce the risk of bystander data from being recorded without consent.

Spotify requires users to be 13 and older and has a separate product for those younger. They rely on parental supervision and surveillance to support this policy. All that is required for a child to sign up for a Spotify account is an email address. The new user is not even prompted to confirm their age. Spotify children require a credit card and premium subscription to sign up. Due to these sales channels there is less friction to open a standard Spotify account then a Kids account and thus is plausible children are signing up for the standard service. As outlined by the 2019 COPPA Youtube violation, the method Spotify uses to prevent the collection of users data is insufficient in the event its service is determined as "Child-directed" by the FTC (Google and

Youtube will pay record $170 million for alleged violations , 2020). Spotify's policy of reaction rather than prevention is concerning on both a legal and ethical view and comes off as flippant in their policy. It would be good for Spotify to outline how they detect unauthorized use of ineligible people from their service.

Spotify's privacy policy is written in a way to maintain compliance with CalOPPA and GDPR, and generally is what I expected from the document. However, Spotify's privacy policy does not go far enough to inform users how their data is collected or used. Areas of concern include how spotify regulates its service from collecting data from children, how it keeps user data secure, and clarity around premium member data collection for advertising purposes. The general vagueness around these policies impedes the user's ability to make an informed decision and challenges the notion of informed consent. At best, these concerns occupy a moral grey area and, at worse, could be in violation of legal statutes and falls short of the intent of the privacy policy. It's intent is to be understood by the average consumer so they can make an informed decision in selecting a service to use. These policies should be revisited and reauthored in alignment of this intent.

Work Cited

Google and Youtube will pay record $170 million for alleged violations of children's privacy law. (2019, November 20). Retrieved February 17, 2021, from https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374*(2083), 20160118. doi:10.1098/rsta.2016.0118

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, the Journal of the American Academy of Arts & Sciences*.

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review, 90*(4), 1087. doi:10.2307/3481326

Spotify data breached for the third time in 2020: Upguard. (n.d.). Retrieved February 17, 2021, from https://www.upguard.com/news/spotify-data-breach-2020

Writing a GDPR-compliant privacy NOTICE (template included). (2019, February 13). Retrieved February 17, 2021, from https://gdpr.eu/privacy-notice/