Safety First: The Imperative for Tech Companies

By Kayla Cardenas

In a world increasingly dependent on technology, concerns about data privacy and security have become paramount. As technology companies continue to innovate and develop new products and services, it is imperative that they prioritize privacy compliance and implement measures to safeguard their users' information. Tech companies should not undervalue the importance of user safety information, and must take the steps necessary to enhance privacy compliance and protect their users and their data.

User Data Safety and Autonomy

What truly sets tech companies apart is not just their groundbreaking technology and services, but their unwavering dedication to protecting user data and privacy. By prioritizing the protection of user data without compromising on innovative offerings, tech companies can realize a vision of a world where every individual has control over their online data.

One of the fundamental principles of privacy compliance is giving users control over their data. “More than 70 percent of smartphone apps are reporting personal data to third-party tracking companies like Google Analytics, the Facebook Graph API or Crashlytics” (Vallina-Rodriguez et al., 2017). Technology companies should provide users with the option to opt out of data sharing with third parties. By respecting users' preferences and allowing them to make informed decisions about

how their data is used, companies demonstrate their commitment to protecting user privacy. In addition to giving users control over their data, technology companies should also offer the option for users to download their data. This empowers users to access and review the information that companies have collected about them, promoting transparency and accountability in data handling practices.

Protection of Biometric Data

Moreover, data privacy should always include the protection of users' biometric data. Companies who collect fingerprints or facial recognition data, handle highly sensitive data that requires special protection. Technology companies must implement robust security measures to safeguard users' biometric information from unauthorized access or misuse. Encryption techniques and stringent access controls should be employed to ensure the confidentiality and integrity of biometric data.

Through robust encryption, stringent security measures, and prevention against sharing private information with third-parties, tech companies can guarantee users that their biometric data, if collected, is handled with utmost care and confidentiality. It ensures that data remains secure and inaccessible to unauthorized parties. Companies who protect the data transactions made with customers, employ cutting-edge encryption protocols to fortify the integrity of user information. By committing to security, companies may thus foster trust with customers.

Creating a Safer and Connected User Base

By prioritizing privacy compliance and implementing robust security measures, technology companies can create a safer and more connected user base. When users trust that their information is secure, they are more likely to engage with technology platforms and participate in digital communities, fostering a sense of connection and belonging.

In applications where user verification is crucial, such as social media platforms or online marketplaces, technology companies should implement verified user profiles. This verification process adds an extra layer of protection, mitigating the risk of fraudulent or malicious activity within the platform. “The concept of verified services, offering dedicated support and features, is attractive from both budgetary and logistical perspectives” (DeBois, 2023). By verifying user identities, companies can mitigate the risk of fraudulent accounts and promote trust and authenticity within their platforms.

Handling Users with Care

For applications that cater to a younger audience, such as gaming or educational apps, parental control settings are essential. Technology companies should offer robust parental control features that allow parents to monitor and regulate their

children's online activities, including setting limits on screen time and restricting access to certain content. “Statistics from a study conducted in 2019 indicate that more than 23% of children and young people are harmed by smartphone use” (How Effective Are Parental Control Apps?, 2024). In order to mitigate such statistics and promote a safer future, companies must recognize the importance of protecting younger users by considering parental oversight in today's digital age. Parental control features allow parents to monitor and regulate their children's technology usage, and control who they are allowed to interact with on online platforms.

Location tracking is a valuable feature in many technology applications, but it also raises privacy concerns. To address these concerns, technology companies should provide users with granular control over location tracking settings, allowing them to choose when and how their location data is shared. Clear and transparent privacy policies should also be provided to inform users on how their location data is used and protected. Safety isn't just about securing data—it's about empowering users with control over their own information.

Building Trust and Connectivity

In conclusion, prioritizing user safety and privacy compliance is not only ethically responsible but also essential for the long-term success and sustainability of technology companies. By giving users control over their data, implementing robust security measures, and offering transparency and accountability in data handling practices, companies can build trust and loyalty among their user base. As technology continues to evolve, it is imperative that companies remain vigilant in their efforts to protect user privacy and ensure a safe and secure digital environment for all.

Through robust security measures, user empowerment, and a steadfast refusal to compromise on ethical principles, more tech companies can step up and set a shining example for data safety and privacy policy worldwide. As we navigate the ever-evolving landscape of technology, individuals can only trust companies who prioritize transparency, integrity, and safety.

References

Vallina-Rodriguez, N., Sundaresan, S., & US, T. C. (2017, May 30). *7 in 10 smartphone apps share your data with third-party services*. Scientific American. https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/

How Effective Are Parental Control Apps? Screentime Monitoring | Safes Parental Control App. (2024, January 16). https://www.safes.so/blogs/how-effective-is-parental-control-app/

DeBois, P. (2023, March 28). *Verified Social Media Profiles & the impact on brands*. CMSWire.com. https://www.cmswire.com/digital-marketing/verified-social-media-profiles-wont-give-marketers-a-cx-boost-not-yet/