Data Practices Recommendation for Booking Holdings

May 2024

Ruby Cheung

Booking Holding's is an online travel company serving 220 countries with 28M+ listings. In 2023 alone, one billion room nights were booked on one of the many subsidiaries operating under Booking Holdings [1]. The trove of detailed information required to book accommodations makes the hospitality industry particularly attractive to hackers and vulnerable to data breaches. The extensive amount of data collected also puts Booking Holding's at a significant risk for violations, if not handled ethically and in accordance with current regulations. Violations could result in substantial financial penalties as well as damage to the company's reputation. This assessment revealed current practices pertaining to personal data collected from users where improvement would significantly reduce risk. Recommendations are provided to address current issues of potential data breaches, avoid dark patterns, and considerations that will help make Booking Holdings compliant with forthcoming AI regulations in the United States and abroad.

In recent years, several accommodation partners of Booking Holdings have been subject to phishing attacks. The liability often falls on listings and 3rd parties'. However, public confidence in the security of Booking Holdings and its subsidiaries continue to degrade the brand when these affiliated entities fall victim to phishing attacks that are becoming more sophisticated and convincing [3]. While there is no silver bullet to prevent data breaches as a result of phishing attacks, Booking Holdings should continue to take steps to improve upon the existing security systems to try to stay ahead of these threats and to avoid potential data breaches of Booking Holdings and its subsidiaries. One recommendation aligns with article 35 of the General Data Protection Regulation(GDPR): Data protection impact assessment [3]. Since the GDPR is currently considered to be the gold-standard of data protection legislation it is no surprise that many countries are now adopting their own legislation modeled after GDPR. It is recommended that Booking Holdings should with reasonable regularity be up to date with a data protection impact assessment as outlined by the GDPR. The assessment is

systemic and extensive covering processing operations and purposes, assesses the necessity of its operation and its risks to the data subjects. A, perhaps annual, evaluation would allow Booking Holdings to remain compliant to regulations and serve to continue to improve upon in-house data security measures. All contracts with third parties, such as marketing companies or insurance services, should be scrutinized to ensure they align with Booking Holdings' data privacy policies and local regulations. Brief annual training on data privacy practices for all employees, particularly those that are charged with access to personal data is strongly suggested.

It is not feasible to stay informed of detailed data security measures and compliance of all entities affiliated with Booking Holdings even for an organization as large as Booking Holdings. Again, there are 28M+ affiliated listings alone across all its subsidiaries. Some of the responsibility for data security falls on the listings and the users themselves. Booking Holdings can support their millions of users through low-cost means. Updating Booking Holding’s data privacy notices will increase transparency, build confidence among its users, and allow for users to be more informed of their rights, aware of the risks, and have more agency over their data. These updates will also prevent violations of the Federal Trade Commision Act, section 5, which prohibits unfair or deceptive acts or practices in or affecting commerce [4]. Opt-in and Opt-out forms should be reviewed for clarity and conciseness as well as consistency across all websites. Users should not be bogged down by wordy data privacy consent notices and forms. This is particularly important for US residents as US legislation adopts an opt-out model for data consent. Exercising data privacy rights is particularly cumbersome for California residents protected under the California consumer privacy act. The current Booking Holdings privacy notice includes the additional rights of California residents, where the key pieces of information are presented in a concise manner on one page. This is ideal but this is not true of all its websites. The amount of linked pages should be minimized, if necessary provide links to pages where these additional rights already presented in the main notice are further explained. Provided directions that allow for California residents to request access to information regarding disclosure of personal data to other parties for marketing purposes on the current privacy notice is clear but buried in a mass of text and the procedure is not consistent among all its websites. It is

recommended that this procedure be made to be as concise and consistent as possible across all Booking Holdings' websites. This not only makes it less confusing for California residents, standardized procedures can be informative by distinguishing Booking Holdings from affiliates and third parties where Booking Holdings does not have responsibility and where policy diverges. All fine print should be removed, any information should be displayed in a legible manner. Updates to the privacy policy notice not only promotes transparency and builds confidence among users it also serves to correct potential dark patterns.

The last consideration pertains to the emerging use of generative AI. Customer service chatbot and AI trip planners are now used to enhance the user experience. They pose a unique threat to data privacy. Recent indirect prompt injection attacks have exposed the vulnerability of the large language models. These types of attacks can lead to generating unintended content or disclosing the private data that the models were trained on. There are no fool-proof methods to mitigate these attacks. It is highly important for Booking Holdings to stay up to date and well informed of the AI models utilized, the potential threats, and current improvements available. This can be done by creating an ethics team or expanding the existing AI teams. Legislation in the US and in the EU are developing to create standards of practice. Currently in most jurisdictions, companies providing and companies using the AI technology will be held liable for data breaches [5]. Affected parties may seek recourse under current legal frameworks, and consequences for Booking Holdings include regulatory fines, compensatory damages, and reputational damage.

In 2023, Booking Holdings' EBITDA, earnings before interest, taxes, depreciation, and amortization was calculated to be $7.1B which was a 34% increase [2]. The recommendations will be a small price to pay to mitigate losses in growth and financial losses due to fines and compensatory damages. The recommended updates to current privacy policies across all websites are low-effort and low-cost. It would not require an expansion on the current teams already charged with maintaining the websites and current legal team to implement. A data impact assessment and AI monitoring would require contracting a neutral third party or developing or expanding upon an in-house team to do this work. Regular assessments and closely overseeing

the use of generative AI will reduce risks of data breaches. Updates to privacy notice will increase transparency and build confidence among users and affiliated parties listed on Booking Holdings various websites. These recommendations can effectively address vulnerabilities in the Booking Holdings current data infrastructure.

References

1. Booking Holdings Privacy Notice. Booking Holdings. March 2023. https://www.bookingholdings.com/privacy-notice/
2. Factsheets. Booking Holdings. https://www.bookingholdings.com/about/factsheet/
3. Goodin, Dan. Mysterious leak of Booking.com reservation data is being used to scam customers. ArsTechnica. February 8, 2023. https://arstechnica.com/information-technology/2023/02/mysterious-leak-of-booking-com-reservation-data-is-being-used-to-scam-customers/
3.https://gdpr-info.eu/art-35-gdpr/
4. What Hides in the Shadows: Deceptive Design of Dark. Congressional Research Service. November 4, 2022. Patternshttps://crsreports.congress.gov/product/pdf/IF/IF12246#:~:text=to%20be%20unlawful.-,Federal%20Trade%20Commission%20(FTC),%5D%20in%20or%20affecting%20commerce.%E2%80%9D
5. Cyber security risks associated with AI Chatbots being manipulated by bad actors. DWF. September 11 2023. https://dwfgroup.com/en/news-and-insights/insights/2023/9/cyber-security-risks-associated-with-ai-chatbots-being-manipulated-by-bad-actors