TRAUB LIEBERMAN

December 4, 2014

Snapchat Data Breach - A Case Study

In early October 2014, the popular mobile messaging and social media app Snapchat suffered a very high profile leak of approximately 100,000 to 200,000 user images sourced from the database of a Snapchat third-party client, SnapSaved. Snapchat is a mobile messaging service that promises users the ability to send private messages and media to other users that are immediately deleted from the users' phones and Snapchat's database after viewing. The October data breach very publicly challenged the company's promise of privacy and raised important concerns for the responsibility of both the company as well as the end-users of the application to protect data and provide adequate security.

SnapSaved was one of many "unauthorized" third-party applications that reverse engineered Snapchat's application programming interface (API) to allow SnapSaved users to physically store images and media sent via Snapchat on SnapSaved's website and database. In a post on its Facebook page, SnapSaved's developer elaborated on the hack, stating it resulted from a misconfiguration in its Apache server. This post came in response to rumors and accusations that SnapSaved was purposely created by hackers to access stored Snapchat media and that SnapSaved allowed hackers access to its database. The SnapSaved website now offers users the ability to search whether or not any of their "snaps" were leaked.

Image not found or type unknown snapchat

While the leak may be relatively small in a vacuum (Snapchat users send over 350 million "snaps" per day), the company's response to the breach is noteworthy. In the days following the hack, Snapchat blamed its users' utilization of third-party apps for the leak, citing to provisions of its Terms Of Use agreement prohibiting use of third-party apps in conjunction with Snapchat.

However, this is not the first time Snapchat, a company that markets "user privacy" as its primary product, has faced cyber security issues. On December 31, 2013, hackers posted 4.6 million Snapchat users' phone numbers and usernames on a website that has since been taken down. At that time, the hackers stated their motivation was to raise public awareness of Snapchat's security flaws. Snapchat faced an investigation by the FTC for deceiving customers regarding how the application actually functioned and how much user data Snapchat stored. The FTC complaint also highlighted Snapchat's security flaws and the precise exploit involved with SnapSaved, voicing concerns over the ease of reverse engineering by third-party app developers. The FTC complaint was filed and settled long before the October leak.

In terms of liability, Snapchat's response relied upon its Terms Of Use agreement with users, but the provision relied upon is buried in the fine print of the TOU with no explanation or warning to users why such third-party applications are prohibited. This raises questions of the enforceability of that provision in a court of law. Snapchat's also suffered reputational damages from the occurrence.

Snapchat's interaction with its users and third-party clients raises important issues concerning the obligations of content providers for data security – particularly those that promise data security as a cornerstone of its product such as social media networks.