MINTZ

A Deep Dive into Privacy/Security Disclosures in Snap's S-1

March 06, 2017 | Blog | By Julia Siripurapu, Joanne Dynak, **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

Last week, Snap Inc. ("Snap" or the "Company") – the parent company of the wildly popular app **Snapchat** ("Snapchat" or the "App") – became a publicly traded company on the New York Stock Exchange in the **biggest tech IPO** since Alibaba in 2014. Priced at $17 per share, the Snap stock opened at $24 per share on Thursday morning and closed at $24.48 per share, bringing the Company's market capitalization to approximately $28 billion. In today's post, we're taking a closer look at **Snap's S-1 filing** ("Snap S-1") with the U.S. Securities and Exchange Commission (SEC) with a particular focus on the Company's disclosures of risk factors associated with cybersecurity and privacy risks.

Background

Since launching in 2012, Snapchat has earned a spot among the most popular social media apps for iOS and Android devices, logging millions of daily users and constantly evolving to accommodate its growing base. Snapchat has skyrocketed in popularity in recent years by allowing users to send their friends ephemeral photo and video messages that disappear seconds after opening. According to the Snap S-1, Snapchat had "***158 million Daily Active Users on average in the quarter ended December 31, 2016***", with the majority of users being between 18 and 34 years old. In contrast to other major social media platforms like Facebook and Twitter (and texting, for that matter), Snapchat doesn't create a permanent, visible log of your posts and interactions with friends. Rather, the App compares its services to the nature of our everyday in-person conversations – once that moment is shared in a given context, it's over and gone. Snapchat allows users to shoot their friends a quick "snapshot" of a moment in their lives without inscribing them into a digital timeline that can be scrolled through, re-read, or shared publicly. This makes users more comfortable sharing things with their friends that they might not normally post online, or even send in a text or email. With all that being said, Snapchat does collect a good amount of information about its users. As described in **Snapchat's privacy policy**, in addition to collecting a user's unique username, password, email address, phone number, and date of birth, and any information a user sends through the App (e.g., snaps and chats), the App also collects usage information (in other words, it knows to whom a user sends snaps, how frequently a user does so, and if a user consent to sharing her geographic data, the location from where the snaps are sent), content information (including metadata), and device information (including, with consent, device phone book information).

An app that lets users communicate without a trace: what could possibly go wrong? As it turns out, quite a bit. As the popularity of the mobile application grew, so too did concerns regarding its data security practices and its ability to deliver on the promises made to its users. Snapchat was accused of misleading its users when it was revealed that the images and videos that allegedly "disappear forever" were actually being stored on company servers, and that a number of other features of the app (such as screenshot detection) were not as reliable or secured as originally represented. The App was **hacked in 2014**, resulting in the exposure of consumer data from 4.6 million accounts. Following a **major FTC investigation and settlement,** Snap was required, among other things, to implement a comprehensive privacy program and submit to monitoring for a period of 20 years. Following a subsequent settlement with the Maryland's Attorney General a month later, Snap was required, among other things, to comply with the **Children's Online Privacy Protection Act ("COPPA")** and, for a period of 10 years, to take specific steps to ensure children under the age of 13 are not creating Snapchat accounts. Both of these settlements are described as part of the risk factors in the Snap S-1.

Snap S-1 Cybersecurity and Privacy Risk Factors

As expected, the cybersecurity and privacy-related risk factors listed in the Snap S-1 are in line with the **SEC's 2011 guidance regarding disclosure obligations relating to cybersecurity risks and cyber incidents**. Apart from the discussion of Snap's 2014 settlements with the FTC and the Maryland Attorney General, as you can see by looking at the risk factors we reproduced below, the disclosures are rather

generic. Snap generally describes the various privacy and security risks the Company is facing as a result of its business model and emphasizes the direct and secondary consequences and risks associated with security and privacy breaches, which could apply to any similar social media platform:

- "***If our security is compromised or if our platform is subjected to attacks that frustrate or thwart our users' ability to access our products and services altogether, which could seriously harm our business".***
- ***"Mobile malware, viruses, hacking and phishing attacks, spamming, and improper or illegal use of Snapchat could seriously harm our business and reputation.***
- ***"Because we store, process, and use data, some of which contains personal information, we are subject to complex and evolving federal, state, and foreign laws and regulations regarding privacy, data protection, and other matters. Many of these laws and regulations are subject to change and uncertain interpretation, and could result in investigations, claims, changes to our business practices, increased cost of operations, and declines in user growth, retention, or engagement, any of which could seriously harm our business".***
- ***"We may be subject to regulatory investigations and proceedings in the future, which could cause us to incur substantial costs or require us to change our business practices in a way that could seriously harm our business".***
- ***"We may face lawsuits or incur liability based on information retrieved from or transmitted over the internet and then posted to Snapchat. We have faced, currently face, and will continue to face claims relating to information that is published or made available on Snapchat. In particular, the nature of our business exposes us to claims related to defamation, intellectual property rights, rights of publicity and privacy, and personal injury torts".***
- ***"We plan to continue expanding our operations abroad where we have limited operating experience and may be subject to increased business and economic risks that could seriously harm our business…. In addition, we are subject to a variety of risks inherent in doing business internationally, including…risks related to the legal and regulatory environment in foreign jurisdictions, including with respect to privacy, and unexpected changes in laws, regulatory requirements, and enforcement."***

One rather unusual risk factor listed in the Snap S-1 is that Snap relies on Google Cloud "***for the vast majority of [its] computing, storage, bandwidth, and other services***" and that "***any disruption of or interference with [its] use of the Google Cloud operation would negatively affect [its] operations and seriously harm [its] business"***. While the practice of using a third party's technology infrastructure to host and operate an online platform is certainly not novel, and in fact, increasingly common for Internet businesses, Snap's disclosure emphasizes the increased risk not just to the operation and continuity of Snap's business but also to the security of the Snap data shared with and stored by the service provider. From a business continuity risk perspective, Snap disclosed the risk of having architected its product and computer systems "***to use computing, storage capabilities, bandwidth, and other services provided by Google, some of which do not have an alternative in the market***" and that it has committed to spend $2 billion with Google Cloud over the next five years. As a somewhat secondary risk, Snap mentioned that because Google's services are restricted in China, it is uncertain whether Snap "***will be able to enter the market in a manner acceptable to the Chinese government***." Although Snap did not specifically focus on privacy and security when discussing the risks of using Google Cloud, as a part of the general discussion of the various risks to the security of Snap user information, Snap mentioned the risk of improper disclosure and access to such information when stored by the Company's third party partners and advertisers, even when such third parties implement adequate security measures and comply with Snap terms and policies.

In addition to discussing the various cybersecurity and privacy related risks stemming from its business model, like its competitors, Snap also lists the following effects of security and privacy breaches on the Company and its business:

- ***"There are many factors that could negatively affect user retention, growth, and engagement, including if….there are concerns about the privacy implications, safety, or security of our products."***
- ***"Our financial condition and results of operations in any given quarter can be influenced by numerous factors, many of which we are unable to predict or are outside of our control, including….system failures or breaches of security or privacy….or changes in the legislative or regulatory environment, including with respect to privacy, or enforcement by government regulators, including fines, orders, or consent decrees."***
- ***"Unfavorable publicity regarding us, for example, our privacy practices, product changes, product quality, litigation, or regulatory activity, or regarding the actions of our partners or our users, could seriously harm our reputation***."

What does going public mean for Snap from a cybersecurity and privacy perspective?

As a public company, Snap will be subject to extensive public filing and disclosure requirements, including, to the extent material, security and privacy. As noted in the Snap S-1, "*by disclosing information in this prospectus and in filings required of a public company, our business and financial condition will become more visible, which we believe may result in threatened or actual litigation, including by competitors and other third parties*." Snap will also now have shareholders to answer to. In the coming months, we (along with the SEC, FTC and other regulators) will certainly be keeping an eye on Snap to observe how it will uphold its commitment to consumer data privacy and keeping its services

safe and secure for users across the globe.

Authors

Julia Siripurapu

Joanne Dynak

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.