Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

'It Wasn't Me' Defense Holds Promise For Snapchat, Dropbox

By **Allison Grande**

Law360, New York (October 17, 2014, 2:30 PM ET) -- Snapchat Inc. and Dropbox Inc. recently responded to purported user-data thefts by asserting the compromised information was lifted from unaffiliated third parties and not their own servers, a defense that attorneys say likely would protect them in breach litigation, as long as they have robust internal security controls and no connection to the third parties.

On Monday, Dropbox **challenged claims** that hackers had lifted nearly 7 million users' login credentials from its servers by asserting that its systems had not been breached and that the data had been stolen from unrelated sites. According to the file-hosting service, hackers took the credentials from other sites and used that information to unsuccessfully try to log into Dropbox accounts.

The disclosure came less than a week after Snapchat **rattled off a similar response** to reports that hundreds of thousands of nude photos and other private messages sent by users had been accessed and publicly posted online. The mobile messaging service claimed that its servers were secure and that the compromised data was lifted from third-party apps that store the content.

While companies such as Target Corp. and the Home Depot Inc. **have learned that** the unauthorized disclosure of consumers' personal data generally leads to a barrage of class actions, attorneys on both sides of the bar told Law360 that plaintiffs would have a hard time maintaining claims against Snapchat or Dropbox based on the details that have been released so far.

"For consumers, it would be difficult to bring claims against those companies so long as the compromised data wasn't taken from an affiliated vendor that the company controlled," said Matthew George, a partner at plaintiffs firm Girard Gibbs LLP.

"If for some reason plaintiffs could show that the source of the breach was data stored with a vendor or contractor, or that there was a design flaw they were aware of or didn't fix that allowed the data to be compromised, they would probably be able to bring those claims and it would be a little bit of a stronger case," George added. "It's a tricky claim, but I wouldn't put it out of the realm of possibility, even though there don't appear to be any facts yet to support it."

Under many state breach notification laws, companies are responsible for reporting an incident in cases where personal information was stored, processed, or otherwise maintained by a third party. They are also obligated to ensure that a third party that they have shared personal information with has adopted reasonable safeguards to protect that information, attorneys noted.

"A data owner cannot disclaim liability by pointing to a service provider and placing blame on the provider," said Lisa Sotto, head of Hunton & Williams LLP's global privacy and data security practice. "While the data owner might be able to make a claim against the vendor based on their contract, the owner ultimately is responsible to the affected individuals and regulators."

But in cases where an unaffiliated third party has come into possession of user data in a way not explicitly sanctioned by the company, pinning the blame on the original source of the data would be harder, according to attorneys.

"If the breach is because the hacker utilized passwords that the consumer also uses for other services, perhaps because they're easy to remember, then the case law usually states that the breached entity is not liable under such a scenario," said Al Saikali, the co-chair of Shook Hardy & Bacon LLP's data security and privacy group.

In the case of Dropbox, the company said that the more than 6.9 million Dropbox account credentials that an anonymous hacker claimed to have accessed and threatened to post on the text-sharing Web application Pastebin were actually stolen from unrelated services with the hope that users had chosen the same login information for their Dropbox account. The company said that it had checked the list of 400 usernames and passwords that had been posted to Pastebin and had confirmed that "these are not associated with Dropbox accounts."

Snapchat also claimed that the nude photos and other messages posted on the online message board 4chan had not originated from its servers. Instead, the company said that users had been "victimized by their use" of unsanctioned third-party message-saving apps such as Snapsaved, which on Saturday admitted to having been breached.

Relying solely on the details that have emerged so far, assigning liability to Snapchat or Dropbox based on the theory that they should have done more to plug the data leaks would be an uphill battle, attorneys say.

"The law doesn't put quite as strong a burden on companies to be proactive in terms of going far beyond their own borders," said Christopher Dore, a partner at plaintiffs' firm Edelson PC. "If the companies are working with the third parties and aware of what the third parties are doing and are not taking any steps to prevent it, that raises the bar."

Joseph Siprut, the founder and managing partner of plaintiffs' firm Siprut PC, noted that Snapchat's choice to state in its terms and conditions that the use of third-party services that transmit Snapchat images is expressly prohibited due to security concerns is likely to help the company, given that liability is likely to hinge heavily on the companies' support for the purportedly breached entities.

"For example, if either service actively promoted the use of such third-party services with the core product, both in terms of representations made and configurations in the product that allow for third-party plugins, that could expose them to liability," Siprut said. "On the other hand, if Snapchat took steps to proactively disavow such practices, that would help establish a defense."

The plaintiffs' bar as well as federal and state regulators are also likely to focus on the representations that both companies made about the strength of their data security controls, which could leave the door open to potential liability, attorneys noted.

"Social media sites can still get in trouble, even when a breach originates with a third party site," said Mike Bennett, a partner at Edwards Wildman Palmer LLP. "Liability arises when companies make overly broad security assurances to their users."

Bennett specifically pointed to Dropbox's declaration in its response Monday that "your stuff is safe" as a statement that could cause problems down the line.

"With new, major breaches occurring weekly, that is a very bold statement," Bennett said. "And if Dropbox is subsequently hacked, regulators could view that statement as an overly broad security claim which is deceptive."

The Federal Trade Commission has been particularly active in this area, having settled more than 50 data security cases in recent years, including one **alleging Snapchat made** false promises about the disappearing nature of messages on its app, the amount of personal data the company collected and the strength of its data security.

But while the regulator has found success with such claims, plaintiffs have had a more difficult time maintaining privacy allegations due to a perceived lack of actual harm, attorneys noted.

"Courts have been divided on this, with some of them declining to find any basis for a claim and others finding unjust enrichment or that some kind of negligence has resulted in harm to the individuals," said Dykema Gossett PLLC member Jonathan Feld. "It will likely depend on specifics about what was represented to the parties about the state of security and protections for their information."

Given that the Dropbox and Snapchat breaches involved third-party services that users were either advised not to use or logged into with the same credentials they chose for other services, the companies have at their disposal the unique yet potentially polarizing argument that the thefts could be directly linked to users' own security shortcomings, which could provide another tool to help them fight off liability, attorneys say.

"We may be beginning to see more of a new flavor of breaches, that center less on how companies handled user data and more on the fact that consumers need to practice good data security hygiene and companies can only do so much," said Manatt Phelps & Phillips LLP partner Donna Wilson.

--Editing by John Quinn and Richard McVay.