BerkeleyLaw
UNIVERSITY OF CALIFORNIA
Berkeley Center for
Law and Business

Berkeley Center for Law and Business
University of California, Berkeley
School of Law
Boalt Hall #7200
Berkeley, CA 94720-7220

Facebook's Massive Cybersecurity Breach: Regulating the Unknown

By Ben Lee, J.D. Candidate 2021 | October 8th, 2018

Just months after clips of Facebook CEO Mark Zuckerberg's testimony before Congress regarding the Cambridge Analytica scandal faded from the forefront of the internet, Facebook is again facing major scrutiny in what has been labeled the company's biggest cybersecurity breach to date.

On September 28, Facebook announced that the digital login access tokens of 50 million users had been stolen, signifying that those accounts and their contents had been compromised. Another 40 million had been placed at risk before the company was able to "patch the security vulnerability." Exploiting three bugs in the website's "View As" function, hackers were able to access users' login tokens, effectively giving them access to all of the content in roughly 50 million accounts.

The legal system's approach to increasingly massive cybersecurity issues like these is similar to how it dealt with Uber's major security breach back in 2014: as they tread into the relatively uncharted arena of cybersecurity, regulatory agencies and courts are desperately attempting to delineate the responsibility that these companies have in terms of security protection for their users. As of now, many businesses, especially small ones, share the sentiment of "shooting a bit blind regarding how to protect data and the consequences for not doing so."

A wrinkle in this investigation that poses an especially interesting inquiry for the legal world stems from Facebook's Single Sign-On (SSO) feature, an idea implemented nearly a decade ago, which allows users to sign into third-party applications with a single Facebook login token. Companies like Airbnb, Tinder, Instagram, and thousands more utilize the SSO feature to streamline the sign-up and login process, thereby rapidly expanding their user bases at a higher speed. Because hackers acquired Facebook users' digital login keys, they theoretically could have had access to accounts in these third-party companies as well.

So as the FTC attempts to better delineate Facebook's security responsibilities within its own company for its own users, the SSO issue poses an additional layer of inquiry that it must answer: does an SSO require heightened scrutiny in terms of cybersecurity? What is the burden that a company like Facebook has in relation to third-party companies that utilize features like

SSOs? Facebook benefitted immensely from the feature for years despite the multiplicity of security risks that would happen in the event of a security breach. That event, with this hack, has finally arrived.

Thanks to the landmark 2015 ruling in *FTC v. Wyndham Worldwide Corporation*, the FTC now has the green light from the Third Circuit to establish companies' responsibilities and liabilities in the "Wild West" of the cybersecurity world. As investigations continue, the FTC will not only see the real magnitude of the harm that may have been multiplied by Facebook's SSO feature, but also, in conjunction with the courts, come to a clearer judgment about cybersecurity responsibilities.