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

U.S. Charges Four Members of Chinese Military in Connection with 2017 Equifax Hack

By Gayatri Raghunandan, LL.M. Candidate 2020 | February 20, 2020

Earlier this month, the Department of Justice charged four Chinese hackers in the 2017 Equifax data breach. A federal grand jury charged the four named defendants with conspiracy to commit computer fraud, wire fraud, and economic espionage. The indictment also charged them with stealing Equifax's trade secret information containing its compilations and database designs.

The Equifax breach affected nearly 150 million Americans and is one of the largest in history. According to a DOJ announcement, the four hackers exploited a vulnerability in the Apache Struts Web Framework software and obtained names, birthdates, and social security numbers of nearly half the country. Although in late 2017, Equifax announced that nearly 143 million customers were affected, by 2018 the company identified the toll to be closer to 150 million victims. According to Equifax, it has identified that as many as 209,000 customers' credit card numbers were exposed and the personal information of 182,000 American consumers was compromised. Further, a staggering 10.9 million lost their drivers' license data. Shockingly, the effects of the breach were not limited to U.S. consumers; British and Canadian consumers were also targeted.

The response to this monumental breach shows the U.S. government's growing attention towards treating personal data with the utmost importance. The data is seen to have consumer and national security value and is classified as "proprietary business information." The ongoing investigation into Chinese TikTok owner, ByteDance, also emphasizes the importance accorded to the national security value of personal data in the U.S.

The breach and the DOJ's subsequent indictment of Chinese military officers may also have a strong impact on US-China relations. In a 2015 meeting with Presidents Xi Jinping and Barack Obama, it was agreed that China would not "conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." This commitment was a consequence of the very first U.S. indictment of Chinese hackers in 2014. However, continued attempts at theft of commercial secrets with little censure has proven that the 2015 agreement is ineffective. This has also called for a growing need to meet these ex-post actions with a framework of mandatory cybersecurity policies for corporate entities.

The Equifax data breach resulted in tumultuous implications, including multiple congressional hearings and the dramatic exit of its then CEO, Richard Smith. Although the company has agreed to settle with regulators for $700 million, those truly affected by the breach have yet to be compensated. Of the 150 million affected, only 10% have filed for compensation. More egregious is the fact that the company has only set aside $31 million for the settlement option of up to $125 per consumer. This amounts to less than $7 a person. It is only fair to wonder whether data breaches like this are really being looked at with pressing importance by these huge corporate entities with nearly unlimited access to sensitive consumer data.