UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of Commissioner
Rohit Chopra

STATEMENT OF COMMISSIONER ROHIT CHOPRA
JOINED BY COMMISSIONER REBECCA KELLY SLAUGHTER

Regarding Data Security and the Safeguards Rule
Commission File No. P145407
March 2, 2020

Summary

- Corporate America's surveillance of our personal data is not just about privacy. Foreign actors are stealing and stockpiling this data, which threatens our national security.
- Companies like Equifax, with their unquenchable thirst for data and their shoddy security practices, are not victims. We must act to curtail the collection, abuse, and misuse of data.
- Rather than "hold our breath and wait" for Congress, the FTC should use the legal authority it has today to protect our citizens, our economy, and our country.

A few weeks ago, U.S. Attorney General William Barr announced criminal indictments against four members of the Chinese People's Liberation Army for conspiring to hack Equifax's computer systems. The Attorney General noted that China has a "voracious appetite for the personal data of Americans" and linked China with several other high-profile hacks of personal data held by large U.S. corporations, including the intrusions into one of America's largest hotel chains, Marriott, and one of America's largest health insurers, Anthem.[1]

The threat posed by China's hacks goes far beyond identity theft. As explained by Attorney General Barr, "these thefts can feed China's development of artificial intelligence tools as well as the creation of intelligence targeting packages."[2] Safeguarding personal data is undoubtedly a national security issue.

In spite of these risks, lax security practices continue to expose our data. According to an alert by the Department of Homeland Security, 85 percent of targeted attacks are preventable.[3] For example, it is hard to call Equifax a victim. Their shoddy approach to security was practically an invitation for the Chinese People's Liberation Army to raid Americans' data. Equifax received

---

[1] William P. Barr, U.S. Attorney General, Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax, Remarks as Prepared for Delivery, (Feb. 10, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military

[2] *Id.*

[3] Press Release, Department of Homeland Security, Alert (TA15-119A) Top 30 Targeted High Risk Vulnerabilities, (Sept. 29, 2016), https://www.us-cert.gov/ncas/alerts/TA15-119A

critical alerts on the need to patch software systems, but failed to do so. Equifax even stored sensitive usernames and passwords in plain text.[4]

The costs of maintaining the status quo approach are significant and mounting. According to industry analysis, the majority of small businesses currently "do not have a cyberattack prevention plan,"[5] yet nearly half of them have experienced at least one breach within the last year.[6] Data breaches can be particularly perilous for small businesses and new entrants, with one survey finding that 66 percent could face temporary or permanent closure if their systems are compromised.[7]

The process of putting into place clear rules requiring corporations to prevent abuse and misuse personal data is long overdue. As the agency responsible for data protection across most of the economy, the Federal Trade Commission plays a central role.

While the effort to update the Safeguards Rule is a start, its reach will be limited to certain nonbank financial institutions like Equifax, and violations don't even come with any civil penalties. Given the ongoing harms to individuals and our country, we should use every tool in our toolbox to address data security issues. The Commission has urged Congress to act, but I agree with Commissioner Rebecca Kelly Slaughter, who has argued that "we cannot simply hold our breath and wait."[8] There are many ways that we can curtail the collection, misuse, and abuse of personal data, including launching a rulemaking that broadly applies to companies across sectors so there are meaningful sanctions for violators. We have this authority today.

Commissioners Wilson and Phillips argue that we must consider the impact of data security on competition. I agree. Data security must also be top of mind in our competition enforcement work across sectors of the economy. We should be reviewing how mergers can lead to a race to the bottom on data security. We need to rigorously scrutinize data deals. Companies are being bought and sold based on the data they have and the data they can continue to collect. Acquired data is being merged into larger databases and used in ways that people may not have authorized when they signed up for the service or initially provided their information.

---

[4] Fed. Trade Comm'n v. Equifax, Case 1:19-mi-99999-UNA, U.S. District Court for the Northern District of Georgia, Atlanta Division, Complaint for Permanent Injunction and Other Relief at 7-8 (July 22, 2019), https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf

[5] Craig Lurey, *Cyber Mindset Exposed: Keeper Unveils its 2019 SMB Cyberthreat Study*, KEEPER SECURITY, (July 24, 2019), https://www.keepersecurity.com/blog/2019/07/24/cyber-mindset-exposed-keeper-unveils-its-2019-smb-cyberthreat-study/.

[6] *Hiscox Cyber Readiness Report 2019*, HISCOX LTD., (Apr. 23, 2019), https://www.keepersecurity.com/blog/2019/07/24/cyber-mindset-exposed-keeper-unveils-its-2019-smb-cyberthreat-study/.

[7] Press Release, *VIPRE Announces Launch of VIPRE Endpoint Security - Cloud Edition*, BUSINESS WIRE, (Oct. 2, 2017), https://www.businesswire.com/news/home/20171002005176/en.

[8] Last year, Commissioner Slaughter described how the FTC could use its existing authority to initiate a data protection rulemaking. *See* Rebecca Kelly Slaughter, Commissioner, Fed. Trade Comm'n, Remarks at the Silicon Flatirons Conference at the University of Colorado Law School: The Near Future of U.S. Privacy Law, (September 6, 2019), https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf

We need to continue to take a close look at what promises were made in exchange for data access and whether those promises were upheld when the data was sold. We also need to examine how companies are integrating different security systems, whether strong security standards are being maintained, and whether sensitive data is being handled appropriately.

Finally, we need to consider whether there are limits to the amount of data one company can collect and compile, the types of data one company can combine, and the ways in which data can be used and monetized. The scale and scope of data collection that large companies are engaging in has made them – and us – sitting ducks for malicious actors. Since these companies are more fixated on monetizing that data than securing it, their mass surveillance has become a national security threat. Our adversaries know that these large firms have essentially done the dirty work of collecting intelligence on our citizens, and lax security standards make it easy to steal. Ultimately, we need to fix the market structures and incentives that drive firms to harvest and traffic in our private information, so that complacent companies are punished when they don't care about our security needs or expectations.

The extraordinary step of criminal indictments of members of the Chinese People's Liberation Army announced by the Attorney General is yet another wake-up call. Until we take serious steps to curb corporate surveillance, the risks to our citizens and country will only grow as bad actors continue to steal and stockpile our data. The FTC will need to act decisively to protect families, businesses, and our country from these unquantifiable harms.