

EDWARD J. MARKEY
MASSACHUSETTS

COMMITTEES:

ENVIRONMENT AND PUBLIC WORKS

FOREIGN RELATIONS

RANKING MEMBER:

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC,
AND INTERNATIONAL CYBERSECURITY POLICY

COMMERCE, SCIENCE, AND TRANSPORTATION

RANKING MEMBER:

SUBCOMMITTEE ON
SPACE, SCIENCE, AND COMPETITIVENESS

SMALL BUSINESS AND ENTREPRENEURSHIP

CHAIRMAN:

U.S. SENATE CLIMATE CHANGE TASK FORCE

United States Senate

SUITE SD-255
DIRKSEN BUILDING
WASHINGTON, DC 20510-2107
202-224-2742

975 JFK FEDERAL BUILDING
15 NEW SUDBURY STREET
BOSTON, MA 02203
617-565-8519

222 MILLIKEN BOULEVARD, SUITE 312
FALL RIVER, MA 02721
508-677-0523

1550 MAIN STREET, 4TH FLOOR
SPRINGFIELD, MA 01103
413-785-4610

June 06, 2018

The Honorable Bob Corker
Chairman
State Foreign Relations Committee
SD-425
Washington, D.C. 20510

The Honorable Bob Menendez
Ranking Member
State Foreign Relations Committee
SH-528
Washington, D.C. 20510

Dear Chairman Corker and Ranking Member Menendez:

I write to respectfully request that you have Facebook Chairman and Chief Executive Officer Mark Zuckerberg testify before the Senate Foreign Relations Committee regarding recent revelations that the company shared private user data with Chinese companies. Unfortunately, this is yet another instance of actions by U.S. technology companies potentially impacting American national security, and it is incumbent upon our committee to exercise oversight in this regard. As the Ranking Member of the East Asia, the Pacific, and International Cybersecurity Policy Subcommittee, I strongly believe that providing information to companies linked to the Chinese Communist Party presents a potential security threat that further exacerbates the already troubling strategic challenge China's increasingly aggressive actions are causing for U.S. foreign policy.

According to reporting published yesterday in *The New York Times*, Facebook, for nearly a decade, has knowingly provided private user data, including relationship status, religion, and political preferences, to four Chinese electronics companies.¹ Facebook has indicated that it shared user information with Huawei and others to integrate Facebook features into consumers' mobile devices. What is most alarming is that U.S. defense and intelligence agencies have long identified Huawei and other Chinese companies as potential security risks.² At a February 2018 Senate Intelligence Committee hearing, Dan Coats, the director of national intelligence, said, "Chinese cyber espionage and cyber attack capabilities will continue to support China's national

¹ Michael LaForgia & Gabriel J.X. Dance, "Facebook Gave Data Access to Chinese Firm Flagged by U.S. Intelligence," *The New York Times*, June 5, 2018, <https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html>.

² U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012*, May 2012, https://www.defense.gov/Portals/1/Documents/pubs/2012_CMPR_Final.pdf.

security and economic priorities.”³ According to media reports, U.S. officials have also implicated the Chinese government in the theft of sensitive personal information from the Office of Personnel Management, which affected more than 22 million people, indicating the Chinese government’s interest in gathering data about U.S. citizens.⁴ Although Facebook officials stated that “all the information from these integrations with Huawei was stored on the device, not on Huawei’s servers,” I have serious concerns about the foreign policy implications of American companies providing such information to Chinese companies.⁵

These revelations should not be viewed in a vacuum. Given China’s additional activities that either undermine the rules-based international order or challenge U.S. interests and values, we must view this latest development in the context of the broader foreign policy challenge. To help call attention to these troubling trends, we recently introduced the Asia Reassurance Initiative Act of 2018, which outlines a long-term strategic vision and a comprehensive, multi-faceted, and principled U.S. policy for the Indo-Pacific region. The core tenets of the U.S.-backed international system are at risk, and from our position in the United States Senate, we must send a clear signal that U.S. companies must not empower China’s increasingly coercive behavior.

As the Committee with jurisdiction over foreign policy challenges to the United States, it is our responsibility to promptly gather all pertinent information regarding potential national security issue and to hold accountable any entities responsible for this episode.

I thank you for your attention to this important matter.

Sincerely,



Edward J. Markey
United States Senator

³ Doina Chiacu & Patricia Zengerle, “U.S. senators concerned about Chinese access to intellectual property,” Reuters, February 13, 2018, <https://www.reuters.com/article/us-usa-security-china/u-s-senators-concerned-about-chinese-access-to-intellectual-property-idUSKCN1FX23M>.

⁴ Devlin Barrett, “Chinese national arrested for allegedly using malware linked to OPM hack,” *The Washington Post*, August 24, 2017, https://www.washingtonpost.com/world/national-security/chinese-national-arrested-for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a_story.html?utm_term=.3746a1cbf9f0.

⁵ LaForgia & Dance, “Facebook Gave Data Access.”