

United States Senate

May 31, 2019

Secretary Wilbur Ross
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, D.C. 20230

Secretary Steven Mnuchin
U.S. Department of the Treasury
1500 Pennsylvania Avenue, N.W.
Washington, D.C. 20220

Trade Representative Robert Lighthizer
Office of the U.S. Trade Representative
600 17th Street, N.W.
Washington, D.C. 20508

Dear Secretaries Ross and Mnuchin and Trade Representative Lighthizer:

I am writing to call your attention to an emerging concern to U.S. consumer privacy— the proliferation of wearables (*e.g.*, smartwatches and fitness trackers) sold by Chinese companies to U.S. consumers.

China's industrial policy plans recognize that wearable devices sold by Chinese companies may continuously collect a user's information, including sensitive health data, facial and voice recognition, always-on microphones, geolocation, electronic payment, access control for mass transit systems and smart locks, social media usage, and other sensitive data.¹ The data of U.S. consumers who use these devices may end up on Chinese servers where it may be shared with, or accessed by, authorities pursuing Chinese industrial policy and political objectives.

China's major wearables brands, especially Huawei and Xiaomi, undercut U.S. companies in the market by selling low cost devices on razor thin margins with a strategy of rapidly expanding their user base in order to amass and monetize user data. Huawei shipments in particular have increased by 147 percent year-over-year, resulting in a 5.2 percent increase in global market share from the first quarter of 2017 through the first quarter of 2018.² As with similarly structured industrial policies in other sectors (*i.e.*, 5G telecommunications equipment), China intends to develop several large, national enterprises on a global scale, which it will then utilize to accomplish its national objectives. In the hands of companies closely linked to China's government, this information could even have serious implications for U.S. national security and the privacy of U.S. citizens.

¹ The 2017 Made in China 2025 Bluebook (2017)

² IDC Reports Strong Growth in the Worldwide Wearables Market, Led by Holiday Shipments of Smartwatches, Wrist Bands, and Ear-Worn Devices, <https://www.idc.com/getdoc.jsp?containerId=prUS44901819>

We know that one of the Chinese government's most important, long-term objectives under *Made in China 2025* and related industrial policies is collecting and utilizing big data.³ In this context, wearables are important to Chinese industrial policy less as "things" to be sold, and more as a means of achieving an array of other economic and strategic objectives that have broader implications for U.S. consumer privacy and national security. For example, U.S. consumers' data derived from their use of Chinese wearables that include always-on microphones, voice recognition and geolocation could be used to broaden the reach of China's "Sky Net" surveillance system (currently based on facial recognition data), which, according to Chinese media, "can scan China's population in a second" with 99.8 percent accuracy.⁴

I strongly believe we need to think of the access we allow companies who we highly suspect are controlled by foreign governments to American consumers and their personal data with a similar caution as with Huawei providing telecommunications infrastructure here in the U.S. At a minimum, we have a duty to make U.S. consumers aware of the privacy risks of buying a wearable from a Chinese company. I encourage you to take steps to ensure the safety of Americans as the Administration continues negotiate with China on behalf of U.S. consumers and our domestic industries.

Sincerely,

A handwritten signature in blue ink that reads "Bill Cassidy, M.D." The signature is written in a cursive, slightly slanted style.

Bill Cassidy, M.D.
United States Senator

³ The 2017 Made in China 2025 Bluebook (2017)

⁴ Zhao Yusha, "Sky Net" Tech Fast Enough to Scan Chinese Population in One Second: Report (Global Times (Mar. 25, 2018)); Paul Mozur, Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras, New York Times (July 8, 2018).