

United States Senate

WASHINGTON, DC 20510

February 7, 2019

Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Washington, D.C. 20528

Dear Director Krebs:

We write concerning the growth of mobile applications that could expose U.S. government employees' web browsing data to third parties, heightening the risk of data interception. We are particularly concerned about the potential threat posed by foreign-made apps that are affiliated with countries of national security concern and urge you to examine the national security risk they pose.

In recent years, mobile data-saving and Virtual Private Network (VPN) apps have become popular, as consumers have grown increasingly interested in securing their internet connection and protecting their privacy. For example, mobile browsers like Dolphin, Yandex, and Opera use their own servers as an intermediary for user traffic, compressing web pages before delivering them to the user to provide data-saving functionality. Similarly, VPN providers route all user traffic through their own servers, nominally to mitigate privacy concerns.

Millions of consumers have downloaded these apps, some of which are made by foreign companies in countries that do not share American interests or values. Because these foreign apps transmit users' web-browsing data to servers located in or controlled by countries that have an interest in targeting U.S. government employees, their use raises the risk that user data will be surveilled by those foreign governments. The compromise of that data could harm U.S. national security.

The U.S. government has already recognized this threat. After investigating the national security risks posed by Chinese telecom equipment, the House Intelligence Committee recommended "the United States should view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies." Similarly, the Department of Homeland Security last year directed all federal agencies to purge their systems of products created by Kaspersky Labs, citing the Russian government's legal ability to compel Kaspersky Labs to assist Russia's intelligence gathering operations. If U.S. intelligence experts believe Beijing and Moscow are leveraging Chinese and Russian-made technology to surveil Americans, surely DHS


should also be concerned about Americans sending their web browsing data directly to China and Russia.

In light of these concerns, we urge you to conduct a threat assessment on the national security risks associated with the continued use by U.S. government employees of VPNs, mobile data proxies, and other similar apps that are vulnerable to foreign government surveillance. If you determine that these services pose a threat to U.S. national security, we further request that you issue a Binding Operational Directive prohibiting their use on federal government smartphones and computers.

Sincerely,



Ron Wyden
U.S. Senator



Marco Rubio
U.S. Senator