

RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

September 30, 2020

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

Dear Director Krebs:

I write to ask that you assess the national security risk posed by U.S. government employees and other Americans using web browser software tools made by foreign companies in countries with a history of conducting hostile foreign intelligence activities against the United States.

As you know, the major web browsers — Google's Chrome, Mozilla's Firefox, Apple's Safari, and Microsoft's Edge — allow users to download and install third-party software, known as browser extensions, which add additional functionality to the browser. Browser extensions, particularly ad blockers, are extremely popular and these software tools have been downloaded by tens of millions of Americans.

While many browser extensions are legitimate, cyber criminals, fraudsters and shady businesses have frequently exploited control over browser extensions to gain access to Americans' computers and then steal personal data and conduct advertising fraud. According to media reports, millions of consumers have been tricked into downloading and installing nefarious browser extensions. Investigative journalists have also exposed how ownership and control of popular, legitimate browser extensions has been quietly sold, after which the new owners pushed automatic updates to unsuspecting users containing malicious code that, among other things, spied on users' web browsing activity.

The companies that dominate the market for shady browser extensions are often foreign firms. For example, my office has been investigating Genimous Technology, a Chinese company that, through a series of shell companies in offshore jurisdictions like Cyprus and Cayman Islands, controls a network of web browser extensions used by more than 10 million consumers. Genimous' subsidiaries offer dozens of browser extensions, which provide users with some limited, free functionality, such as weather reports or package tracking, in order to gain access to users' computers. The true purpose of Genimous' browser extensions is to change users' search engine to one offered by Verizon Media, which pays Genimous a fee for doing so.

I am concerned that the use by millions of Americans of foreign-controlled browser extensions could threaten U.S. national security. In particular, I am concerned that these browser extensions could enable foreign governments to conduct surveillance of Americans.

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

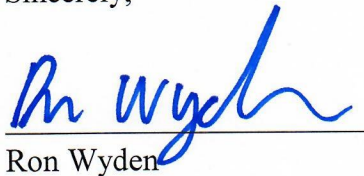
In February of 2019, Senator Rubio and I asked you to assess the national security threat posed by Virtual Private Network (VPN) services and web browsers provided by foreign companies. In your May 2019 response, you agreed with our concern, noting that “if a U.S. government employee downloaded a foreign VPN application originating from an adversary nation, foreign exploitation of that data would be somewhat or highly likely.”

The threat posed by foreign VPN services appears similar to that of foreign companies offering web browser extensions. These companies also have access to sensitive data about their users’ internet browsing and communications. This can include information collected from the web pages that users visit, such as webmail and social media accounts, which could be used to inform and supercharge foreign intelligence services’ hacking, blackmail, and influence campaigns. A malicious browser extension could also exploit vulnerabilities in a target’s web browser to install malware that steals sensitive files stored on a computer, spies on audio and video calls, or covertly activates a computer’s microphone or webcam.

To that end, I ask you to assess the threat posed by web browser extensions offered and controlled by companies in adversary nations. If you determine that these companies and their products threaten U.S. national security, please take the appropriate steps to protect U.S. government employees and government systems.

Thank you for your attention to this important issue. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator