

DOW JONES, A NEWS CORP COMPANY

DJIA 2519.38 0.08% ▲

S&P 500 2732.22 0.04% ▲

Nasdaq 7239.47 -0.23% ▼

U.S. 10 Yr 0/32 Yield 2.875% ▼

Crude Oil 61.61 0.44% ▲

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.

<https://www.wsj.com/articles/chinas-vpn-crackdown-may-aid-government-surveillance-1516189155>

ASIA

China's VPN Crackdown May Aid Government Surveillance

It threatens to make emails and data transmissions by foreign companies more vulnerable, security analysts say.



People use computers at a Beijing internet cafe. PHOTO: HOW HWEE YOUNG/EUROPEAN PRESSPHOTO AGENCY

By Liza Lin in Shanghai and Yoko Kubota in Beijing

Updated Jan. 17, 2018 11:36 a.m. ET

China's clampdown on the cyber tunnels used to burrow through its Great Firewall may do more than further restrict internet access—it also threatens to make emails and data transmissions by foreign companies more vulnerable to government surveillance, security analysts say.

Companies, institutions and individuals use virtual private networks, or VPNs, to send secure emails, transmit data and access websites blocked in China. The country's Ministry of Industry and Information Technology served notice last year that access to non-licensed VPNs will be blocked on March 31.

That will force companies and others to choose from a limited number of approved VPN providers, including ones run by China's state-owned telecom companies—making it easier for the government to target and monitor VPN communications, according to the analysts.

“Telecom companies, not just those in China, have the capability to see their information flowing through their lines,” said Carly Ramsey, an associate director at consulting firm Control Risks Group, underscoring the need for data encryption before such transfers.

Since it was first announced last year, the VPN clampdown has been seen largely as a campaign to patch holes in China's Great Firewall, the figurative term used to describe Beijing's efforts to restrict access to Internet content such as pornography, certain foreign news outlets and social networks including Facebook.

But forcing companies to use state-approved VPNs may also serve to strengthen China's state surveillance, which uses sophisticated technology such as facial recognition and cloud computing to monitor what people and companies say and do online.

“If someone wants to access your data, be it a state actor or otherwise, it makes it easier to do so,” Randy Phillips, Asia Managing Partner at Mintz Group in Beijing, said Wednesday.

The ministry didn’t immediately reply to a request for comment.

Internet access in China is tightening in advance of the March 31 cutoff. Last year, Apple said it removed nearly 700 VPN applications from its App Store in China in response to the new restrictions.

More recently, Telecom providers have begun sending letters to foreign customers, advising them that data transmission ports—communication points that allow computers to manage internet traffic—will also be blocked without a proper license. Late last year, China Telecom’s Shanghai office sent letters to customers asking them to register for access to certain ports used for email and file sharing, according to a copy reviewed by The Wall Street Journal.

Forcing firms to register these ports would allow Chinese authorities to monitor and identify the sources of data traffic, said Han Lai, who oversees China for tech services firm KLDDiscovery. That allows the government to spot unauthorized encrypted traffic, he said.

Foreign embassies are also feeling the squeeze. France and Portugal experienced disruptions to their VPN services used to communicate with outside companies they contract with for visa services, according to a letter the European Union sent last month to Chinese authorities, said diplomats who saw a copy.

France and Portugal did not immediately respond to requests for comment.

Several in Greater China’s foreign diplomatic corps say they have become resigned to the Chinese government peering over their shoulders.

“Nothing is really confidential,” said one diplomat. “Our hypothesis is that everything can be read when we are in China.” All declined to be named due to the sensitivity of the situation.

U.S. and other foreign companies and institutions doing business in China are increasingly concerned about the clampdown. They have reached out to trade groups including the U.S.-China Business Council and European Chamber of Commerce and for clarifications on the impact of the new restrictions, which will force many VPN users to switch to new providers.

“Access to the worldwide web has become a major frustration for companies operating in China,” said Mats Harborn, president of the European Chamber.

Some members at the U.S.-China Business Council have also reported disruptions to cross-border file sharing and attempts to access email servers from outside the U.S., Jake Parker, vice president at the Council, said Wednesday.

One foreign industry group said its monthly communications bill is set to double as it plans to switch from a disrupted VPN service to a dedicated line that goes through an international gateway provided by state-run telecom operators.

The crackdown is also taking a toll on expatriates working in China. An executive at a Japanese electronics maker said China’s internet controls have started to impact his daily routine and access to his favorite sites.

Access to these websites has become increasingly difficult in the last few months, he said.

“It’s a headache since even Yahoo Japan can’t be used as a search engine these days without VPN, and I can no longer read the Nikkei business newspaper without VPN either,” the executive said.

Write to Liza Lin at Liza.Lin@wsj.com and Yoko Kubota at yoko.kubota@wsj.com

Corrections & Amplifications

Some members at the U.S.-China Business Council have also reported disruptions to cross-border file sharing and attempts to access email servers from outside the U.S., Jake Parker, vice president at the Council, said Wednesday. An earlier version of this article incorrectly stated Mr. Parker’s title and the location for attempts to access email. (Jan. 17, 2018)

Copyright ©2017 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.