Executive Order 13971—Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies

January 5, 2021

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq*.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq*.), and section 301 of title 3, United States Code,

I, Donald J. Trump, President of the United States of America, find that additional steps must be taken to deal with the national emergency with respect to the information and communications technology and services supply chain declared in Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain). Specifically, the pace and pervasiveness of the spread in the United States of certain connected mobile and desktop applications and other software developed or controlled by persons in the People's Republic of China, to include Hong Kong and Macau (China), continue to threaten the national security, foreign policy, and economy of the United States. At this time, action must be taken to address the threat posed by these Chinese connected software applications.

By accessing personal electronic devices such as smartphones, tablets, and computers, Chinese connected software applications can access and capture vast swaths of information from users, including sensitive personally identifiable information and private information. This data collection threatens to provide the Government of the People's Republic of China (PRC) and the Chinese Communist Party (CCP) with access to Americans' personal and proprietary information—which would permit China to track the locations of Federal employees and contractors, and build dossiers of personal information.

The continuing activity of the PRC and the CCP to steal or otherwise obtain United States persons' data makes clear that there is an intent to use bulk data collection to advance China's economic and national security agenda. For example, the 2014 cyber intrusions of the Office of Personnel Management of security clearance records of more than 21 million people were orchestrated by Chinese agents. In 2015, a Chinese hacking group breached the United States health insurance company Anthem, affecting more than 78 million Americans. And the Department of Justice indicted members of the Chinese military for the 2017 Equifax cyber intrusion that compromised the personal information of almost half of all Americans.

In light of these risks, many executive departments and agencies (agencies) have prohibited the use of Chinese connected software applications and other dangerous software on Federal Government computers and mobile phones. These prohibitions, however, are not enough given the nature of the threat from Chinese connected software applications. In fact, the Government of India has banned the use of more than 200 Chinese connected software applications throughout the country; in a statement, India's Ministry of Electronics and Information Technology asserted that the applications were "stealing and surreptitiously transmitting users' data in an unauthorized manner to servers which have locations outside India."

The United States has assessed that a number of Chinese connected software applications automatically capture vast swaths of information from millions of users in the United States, including sensitive personally identifiable information and private information, which would allow the PRC and CCP access to Americans' personal and proprietary information.

The United States must take aggressive action against those who develop or control Chinese connected software applications to protect our national security.

Accordingly, I hereby order:

Section 1. (a) The following actions shall be prohibited beginning 45 days after the date of this order, to the extent permitted under applicable law: any transaction by any person, or with respect to any property, subject to the jurisdiction of the United States, with persons that develop or control the following Chinese connected software applications, or with their subsidiaries, as those transactions and persons are identified by the Secretary of Commerce (Secretary) under subsection (e) of this section: Alipay, CamScanner, QQ Wallet, SHAREit, Tencent QQ, VMate, WeChat Pay, and WPS Office.

(b) The Secretary is directed to continue to evaluate Chinese connected software applications that may pose an unacceptable risk to the national security, foreign policy, or economy of the United States, and to take appropriate action in accordance with Executive Order 13873.

(c) Not later than 45 days after the date of this order, the Secretary, in consultation with the Attorney General and the Director of National Intelligence, shall provide a report to the Assistant to the President for National Security Affairs with recommendations to prevent the sale or transfer of United States user data to, or access of such data by, foreign adversaries, including through the establishment of regulations and policies to identify, control, and license the export of such data.

(d) The prohibitions in subsection (a) of this section apply except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted before the date of this order.

(e) Not earlier than 45 days after the date of this order, the Secretary shall identify the transactions and persons that develop or control the Chinese connected software applications subject to subsection (a) of this section.

Sec. 2. (a) Any transaction by a United States person or within the United States that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate the prohibition set forth in this order is prohibited.

(b) Any conspiracy formed to violate any of the prohibitions set forth in this order is prohibited.

Sec. 3. For the purposes of this order:

(a) the term "connected software application" means software, a software program, or group of software programs, designed to be used by an end user on an end-point computing device and designed to collect, process, or transmit data via the Internet as an integral part of its functionality.

(b) the term "entity" means a government or instrumentality of such government, partnership, association, trust, joint venture, corporation, group, subgroup, or other organization, including an international organization;

(c) the term "person" means an individual or entity;

(d) the term "personally identifiable information" (PII) is information that, when used alone or with other relevant data, can identify an individual. PII may contain direct identifiers (e.g., passport information) that can identify a person uniquely, or quasi-identifiers (e.g., race) that can be combined with other quasi-identifiers (e.g., date of birth) to successfully recognize an individual.

(e) the term "United States person" means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.

Sec. 4. (a) The Secretary, in consultation with the Secretary of the Treasury and the Attorney General, is hereby authorized to take such actions, including adopting rules and regulations, and to employ all powers granted to me by IEEPA, as may be necessary to implement this order. All agencies shall take all appropriate measures within their authority to implement this order.

(b) The heads of agencies shall provide, in their discretion and to the extent permitted by law, such resources, information, and assistance to the Department of Commerce as required to implement this order, including the assignment of staff to the Department of Commerce to perform the duties described in this order.

Sec. 5. *Severability*. If any provision of this order, or the application of any provision to any person or circumstance, is held to be invalid, the remainder of this order and the application of its other provisions to any other persons or circumstances shall not be affected thereby.

Sec. 6. *General Provisions*. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department, agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP

The White House,
January 5, 2021.

[Filed with the Office of the Federal Register, 8:45 a.m., January 7, 2021]

NOTE: This Executive order was published in the *Federal Register* on January 8.

Categories: Executive Orders : Chinese companies, efforts to address threat posed by applications and software developed or controlled by.

Subjects: Defense and national security : Cybersecurity :: Strengthening efforts.

DCPD Number: DCPD202100005.