

1 MICHAEL W. BIEN – 096891
ERNEST GALVAN – 196065
2 VAN SWEARINGEN – 259809
BENJAMIN BIEN-KAHN – 267933
3 ALEXANDER GOURSE – 321631
AMY XU – 330707
4 ROSEN BIEN
GALVAN & GRUNFELD LLP
5 101 Mission Street, Sixth Floor
San Francisco, California 94105-1738
6 Telephone: (415) 433-6830
Facsimile: (415) 433-7104
7 Email: mbien@rbgg.com
egalvan@rbgg.com
8 vswearingen@rbgg.com
bbien-kahn@rbgg.com
9 agourse@rbgg.com
axu@rbgg.com

10 KELIANG (CLAY) ZHU – 305509
11 DEHENG LAW OFFICES PC
7901 Stoneridge Drive #208
12 Pleasanton, California 94588
Telephone: (925) 399-5856
13 Facsimile: (925) 397-1976
Email: czhu@dehengsv.com

14 ANGUS F. NI – Admitted *Pro Hac Vice*
15 AFN LAW PLLC
502 Second Avenue, Suite 1400
16 Seattle, Washington 98104
Telephone: (773) 543-3223
17 Email: angus@afnlegal.com

18 Attorneys for Plaintiffs

19 UNITED STATES DISTRICT COURT

20 NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

21 U.S. WECHAT USERS ALLIANCE,
CHI HUO INC., BRENT COULTER,
22 FANGYI DUAN, JINNENG BAO, ELAINE
PENG, and XIAO ZHANG,

23 Plaintiffs,

24 v.

25 DONALD J. TRUMP, in his official capacity
as President of the United States, and
26 WILBUR ROSS, in his official capacity as
Secretary of Commerce,

27 Defendants.

THOMAS R. BURKE – 141930
DAVIS WRIGHT TREMAINE LLP
505 Montgomery Street, Suite 800
San Francisco, California 94111-6533
Telephone: (415) 276-6500
Facsimile: (415) 276-6599
Email: thomasburke@dwt.com

DAVID M. GOSSETT – Admitted *Pro Hac Vice*
DAVIS WRIGHT TREMAINE LLP
1301 K Street N.W., Suite 500 East
Washington, D.C. 20005-3366
Telephone: (202) 973-4216
Facsimile: (202) 973-4499
Email: davidgossett@dwt.com

JOHN M. BROWNING – *Pro Hac Vice*
forthcoming
DAVIS WRIGHT TREMAINE LLP
1251 Avenue of the Americas, 21st Floor
New York, New York 10020-1104
Telephone: (212) 603-6410
Facsimile: (212) 483-8340
Email: jackbrowning@dwt.com

Case No. 3:20-cv-05910-LB

**DECLARATION OF MICHAEL W. BIEN
IN SUPPORT OF PLAINTIFFS’
OPPOSITION TO DEFENDANTS’
MOTION TO STAY PENDING APPEAL
OF ORDER GRANTING MOTION FOR
PRELIMINARY INJUNCTION**

Date: October 15, 2020
Time: 9:30 a.m.
Crtrm.: Remote

Judge: Hon. Laurel Beeler
Trial Date: None Set

1 I, Michael W. Bien, declare:

2 1. I am an attorney duly admitted to practice before this Court. I am a partner
3 in the law firm of Rosen Bien Galvan & Grunfeld LLP, counsel of record for Plaintiffs. I
4 have personal knowledge of the facts set forth herein, and if called as a witness, I could
5 competently so testify. I make this declaration in support of Plaintiffs' Opposition to
6 Defendants' Motion to Stay Pending Appeal of Order Granting Motion for Preliminary
7 Injunction.

8 2. Attached hereto as **Exhibit A** is a true and correct copy of an email sent by
9 my partner Van Swearingen on September 30, 2020 to opposing counsel in this case. The
10 email requests that opposing counsel provide a non-classified summary or description of
11 the classified materials filed with the Motion to Stay. As of 4:30 p.m. (PST) today,
12 opposing counsel has not responded to this email.

13 3. Attached hereto as **Exhibit B** is a true and correct copy of an August 5, 2020
14 news article, updated on August 7, 2020, by Heather Kelly of the Washington Post titled
15 "Facebook, Twitter penalize Trump for posts containing coronavirus misinformation,"
16 *available at:* <https://www.washingtonpost.com/technology/2020/08/05/trump-post-removed-facebook/> (last accessed September 29, 2020).

18 4. Attached hereto as **Exhibit C** is a true and correct copy of a October 11,
19 2017 article by Aziz Huq of Fortune titled "How the Justice Department's Facebook
20 Subpoenas Threaten Free Speech," *available at:*
21 <https://fortune.com/2017/10/11/departement-of-justice-facebook-subpoena-free-speech-privacy/> (last accessed September 29, 2020).

23 5. Attached hereto as **Exhibit D** is a true and correct copy of a September 18,
24 2020 press release issued by the U.S. Department of Commerce titled "Commerce
25 Department Prohibits WeChat and TikTok Transactions to Protect the National Security of
26 the United States," *available at:* <https://www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect>
27 (last accessed September 29, 2020).

1 6. Attached hereto as **Exhibit E** is a true and correct copy of a July 22, 2019
2 article by James B. Cutchin of the Los Angeles Times titled “How U.S. video game
3 companies are building tools for China’s surveillance state,” *available at*:
4 [https://www.latimes.com/business/story/2019-07-21/american-game-developers-china-](https://www.latimes.com/business/story/2019-07-21/american-game-developers-china-surveillance)
5 [surveillance](https://www.latimes.com/business/story/2019-07-21/american-game-developers-china-surveillance) (last accessed September 29, 2020).

6 7. Attached hereto as **Exhibit F** is a true and correct copy of a December 10,
7 2018 article by Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, and Aaron
8 Krolik of the New York Times titled “Your Apps Know Where You Were Last Night, and
9 They’re Not Keeping It Secret,” *available at*:
10 <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>
11 (last accessed September 29, 2020).

12 8. Attached hereto as **Exhibit G** is a true and correct copy of a September 6,
13 2018 article by Avie Schneider of NPR titled “Twitter Bans Alex Jones And InfoWars;
14 Cites Abusive Behavior,” *available at*:
15 [https://www.npr.org/2018/09/06/645352618/twitter-bans-alex-jones-and-infowars-cites-](https://www.npr.org/2018/09/06/645352618/twitter-bans-alex-jones-and-infowars-cites-abusive-behavior:%20)
16 [abusive-behavior:%20](https://www.npr.org/2018/09/06/645352618/twitter-bans-alex-jones-and-infowars-cites-abusive-behavior:%20) (last accessed September 29, 2020).

17 9. Attached hereto as **Exhibit H** is a true and correct copy of a July 8, 2020
18 article, updated on July 10, 2020, by Davey Alba of the New York Times titled “Facebook
19 Removes Roger Stone for Ties to Fake Accounts,” *available at*:
20 <https://www.nytimes.com/2020/07/08/technology/roger-stone-facebook.html> (last accessed
21 September 29, 2020).

22 10. Attached hereto as **Exhibit I** is a true and correct copy of a October 30, 2018
23 article by Taylor Hatmaker of TechCrunch titled “Facebook bans the Proud Boys, cutting
24 the group off from its main recruitment platform,” *available at*:
25 <https://techcrunch.com/2018/10/30/facebook-proud-boys-mcinnis-kicked-off/> (last
26 accessed September 29, 2020).

27 11. Attached hereto as **Exhibit J** is a true and correct copy of a June 9, 2018
28 news release issued by China Oceanwide Holdings Group Co., Ltd. and Genworth

1 Financial, Inc. titled “Committee on Foreign Investment in the United States Completes
2 Review of Proposed China Oceanwide and Genworth Financial Transaction,” *available at:*
3 [http://investor.genworth.com/investors/news-releases/archive/archive/2018/Committee-on-
6 Foreign-Investment-in-the-United-States-Completes-Review-of-Proposed-China-
7 Oceanwide-and-Genworth-Financial-Transaction/default.aspx](http://investor.genworth.com/investors/news-releases/archive/archive/2018/Committee-on-
4 Foreign-Investment-in-the-United-States-Completes-Review-of-Proposed-China-
5 Oceanwide-and-Genworth-Financial-Transaction/default.aspx) (last accessed September
8 30, 2020).

9 12. Attached hereto as **Exhibit K** is a true and correct copy of an email sent on
10 October 1, 2020 at 7:43 a.m. (PST) by Department of Justice attorney Dennis Fan to me.
11 The email gives notice that Defendants plan to file a notice of appeal tomorrow, October 2,
12 2020, in the United States Court of Appeals for the Ninth Circuit, and that they also intend
13 to file an emergency motion for a stay of this Court’s preliminary injunction order. This
14 email string includes a response by my partner Ernest Galvan on October 1, 2020 at 2:42
15 p.m. (PST), explaining that Plaintiffs will oppose any such application.

16 I declare under penalty of perjury under the laws of the United States of America
17 that the foregoing is true and correct, and that this declaration is executed at San Francisco,
18 California this first day of October, 2020.

19 */s/ Michael W. Bien*
20 _____
21 Michael W. Bien
22
23
24
25
26
27
28

Exhibit A

From: Van Swearingen
Sent: Wednesday, September 30, 2020 12:05 PM
To: Orloff, Serena M (CIV); Drezner, Michael L. (CIV); Robinson, Stuart J. (CIV)
Cc: Michael W. Bien; Clay Zhu; Angus Ni; Thomas Burke; Gossett, David
Subject: U.S. WeChat Users Alliance v. Trump - classified materials [IWOV-DMS.FID71398]

Serena,

We would appreciate a proffer from Defendants as to what the classified materials tend to show. Is there any summary or description of the classified materials that you can provide to us other than what is in Defendants' motion and supporting Costello declaration? Thank you,

Van

Van Swearingen



101 Mission Street, Sixth Floor

San Francisco, CA 94105

(415) 433-6830 (telephone)

(415) 433-7104 (fax)

VSwearingen@rbgg.com

CONFIDENTIALITY NOTICE

The information contained in this e-mail message may be privileged, confidential and protected from disclosure. If you are not the intended recipient, any dissemination, distribution or copying is strictly prohibited. If you think that you have received this e-mail message in error, please e-mail the sender at rbgg@rbgg.com.

IRS CIRCULAR 230 NOTICE: As required by United States Treasury Regulations, you should be aware that this communication is not intended by the sender to be used, and it cannot be used, for the purpose of avoiding penalties under United States federal tax laws.

Exhibit B

The Washington Post

Democracy Dies in Darkness

Facebook, Twitter penalize Trump for posts containing coronavirus misinformation

The social media companies have made it clear in recent months that they will not tolerate misinformation on the global pandemic.

By **Heather Kelly**

August 7, 2020 at 11:25 a.m. PDT

Correction: Twitter penalized Team Trump, the president's campaign account. An earlier version of this article said that Twitter penalized President Trump's account.

Facebook and Twitter on Wednesday took extraordinary action against President Trump for spreading coronavirus misinformation after his official and campaign accounts broke their rules, respectively.

Facebook removed from Trump's official account the post of a video clip from a Fox News interview in which he said children are "almost immune" from covid-19. Twitter required his Team Trump campaign account to delete a tweet with the same video, blocking it from tweeting in the interim.

In the removed video, President Trump can be heard in a phone interview saying schools should open. He goes on to say, "If you look at children, children are almost — and I would almost say definitely — but almost immune from this disease," and that they have stronger immune systems.

The twin actions came roughly three months before the elections in which Trump's performance on coronavirus is a key issue, and the social media companies have made it clear in recent months that they will not tolerate misinformation on the global pandemic.

The decision represents something of an about-face for Facebook, whose chief executive, Mark Zuckerberg, has long been a proponent of free speech on his site. Zuckerberg under pressure in late June said the company will remove posts that incite violence or attempt to suppress voting — even from political leaders — and that the company will affix labels on posts that violate its hate speech or other policies.

Twitter, meanwhile, has taken a more aggressive stance, flagging several of Trump's tweets for misinformation and even blocking his son Donald Trump Jr. from tweeting for 12 hours for breaking its coronavirus misinformation rules.

Twitter said it hid the campaign's post and that the account would not be able to tweet again until the message is deleted, although the campaign can appeal the decision. The account was active again late Wednesday night. Trump's personal account also reshared the video originally posted by Team Trump, but it was removed after the original tweet was blocked.

Twitter spokeswoman Liz Kelley said the tweet "is in violation of the Twitter Rules on COVID-19 misinformation. The

Facebook spokesman Andy Stone said, "This video includes false claims that a group of people is immune from COVID-19 which is a violation of our policies around harmful COVID misinformation."

A Trump campaign spokesman did not immediately respond to a request for comment.

While many children have had milder symptoms from the virus, researchers have found they are still able to catch and spread it to other people, including adults at home and in school settings, such as teachers.

"They get it and can transmit it, but they get it less and transmit it less than adults," said Theodore Ruel, chief of the Division of Pediatric Infectious Diseases and Global Health at the University of California at San Francisco. He said the word "immunity" is incorrect in this context but that children, especially younger ones, are less of a risk than adults.

More than 240,000 children in the United States have been documented to have covid-19, the disease caused by the novel coronavirus, according to the federal Centers for Disease Control and Prevention. Around 300 children have contracted a rare inflammatory disease due to covid-19 called multisystem inflammatory syndrome, and six have died.

Ruel said that with proper protocols, including masking and social distancing, and a working testing and contact-tracing program, schools for younger children could be safe enough to reopen.

"A well-run school is going to be just as safe if not safer than a grocery store," he said. "But we have to make it safe for both [teachers and kids], and we have to recognize it is a risk for both if we want to reopen schools."

As the start of the school year rolls around, school districts across the country have been torn on how to proceed. With rising covid-19 case numbers across the country, many large districts have decided to start the year virtually, with online classes. Others have opted to go ahead with in-person classes, like in Georgia.

Teachers are being ordered to report for work at Gwinnett County Public Schools, the state's largest school district, ahead of a digital semester. It has reported that 260 district employees had tested positive for the virus or been exposed to someone who had.

Facebook previously deactivated dozens of ads placed by President Trump's reelection campaign that included a symbol once used by the Nazis to designate political prisoners in concentration camps.

The company has faced increasing pressure to better moderate its site. More than 1,000 advertisers have joined a boycott regarding its civil rights record, including Disney and Verizon. And nearly two dozen state attorneys general sent a letter criticizing the company earlier Wednesday.

The shifts are at least a partial retreat from the company's traditional deference to speech it deems "newsworthy." That includes Facebook's decision to not label or remove a post by Trump that said, "when the looting starts, the shooting starts."

Twitter, which affixed a warning label on a similar post, has been more forceful about responding to what it deemed to be policy violations, including from politicians.

Twitter has labeled several tweets from the president for being misleading, including on mail-in ballots being fraudulent. Twitter late last month ordered the president's son to delete a misleading tweet with hydroxychloroquine misinformation and limited the account for 12 hours.

Zuckerberg faced tough questions from lawmakers a week ago while testifying on Capitol Hill along with other big tech CEOs on antitrust issues. Several Republicans asked him pointed questions regarding whether the company censors conservative voices.

Rep. Matt Gaetz (R-Fla.) asked Zuckerberg about specific incidents in which the lawmaker alleged that Facebook executives may have used the service to downplay conservative viewpoints.

Zuckerberg said the company aims “to be a platform for all ideas” and that he does not want Facebook to be ideologically biased.

Faiz Siddiqui contributed to this report.

Updated August 5, 2020

Big tech battles the U.S. government

In the wake of a historic antitrust hearing, big tech finds itself in the war path of local and federal government officials.

The leaders behind **Amazon, Apple, Facebook and Google** testified before the House Judiciary subcommittee on antitrust, commercial and administrative law.

Read the testimony: [Amazon](#) | [Facebook](#) | [Google](#) | [Apple](#)

Five takeaways from the historic big tech hearing.

What were the **biggest lies** the Big Tech CEOs told Congress — and us?

Rep. David N. Cicilline (D-R.I.), the leader of the House’s antitrust subcommittee:

The **“Internet is broken.”**

A letter from 20 state attorneys general demands Facebook improve its civil rights record.

Facebook and Twitter have made it clear in recent months that they will not tolerate misinformation on the coronavirus pandemic - even from the president.

[Sign in to join the conversation](#)

[Comments](#)

Exhibit C

Most Popular



One major Asian economy besides China is set for growth this year—and its GDP just rose 2.6%



Who won last night's presidential debate? Biden in a landslide, oddsmakers say



M
ir
e
c
t

COMMENTARY • FREEDOM OF SPEECH

How the Justice Department's Facebook Subpoenas Threaten Free Speech

BY AZIZ HUQ

October 11, 2017 7:31 AM PDT



A woman stands and checks her smartphone whilst framed against an illuminated wall bearing Facebook Inc.s 'Thumbs Up' symbol in this arranged photograph in London, U.K., on Wednesday, Dec. 23, 2015.

CHRIS RATCLIFFE/BLOOMBERG VIA GETTY IMAGES



In recent months, the U.S. Justice Department has issued subpoenas against Facebook (FB) and web host DreamHost for records of thousands, perhaps millions, of citizens who expressed interest in protesting President Trump's inauguration. Such requests, while perhaps well-intentioned, impinge on constitutional values embodied in the First, Fourth, and Fifth amendments. And worryingly, there is no good way now to ensure such values are respected.

Prosecutors often subpoena businesses for personal and revealing documents in white-collar and criminal cases. During the Whitewater investigation in 1998, Independent Counsel Kenneth Starr demanded records from the Washington, D.C. bookstore Kramerbooks respecting President Clinton's purchases. Five years earlier, Senate investigators subpoenaed Sen. Bob Packwood's diaries. And the reporter who obtained Judge Robert Bork's video rental records in 1987 could as easily have been a zealous prosecutor.

Social media and web-hosted platforms generate business records much like bookstores, libraries, and video stores—just at a much higher rate, and entangling many more people. The Justice Department's request to DreamHost, for example, potentially swept in 1.3 million people.

Prosecutors often have legitimate interests in these records. The ongoing Las Vegas investigation into gunman Stephen Paddock, for example, will properly reach records of his online activity. Many terrorist investigations hinge on tracking suspects' interactions with online radicalizers, necessitating the acquisition of records.

At the same time, subpoenas pose challenges to privacy and political freedom. First, the specter of wide-ranging government power to acquire records of online interactions might alter people's behavior, allowing government to subtly influence the shape of public debate. Second, subpoenas respecting online conduct allow government to identify those with divergent views—and to target them for harassment or punishment.

These are precisely the concerns that led to James Madison's drafting of provisions in the Bill of Rights in 1791 to protect not just a right of free speech, but also rights against unreasonable searches and seizures and compelled self-incrimination under the Fourth and Fifth amendments, respectively.

A key case that the Bill of Rights' framers knew well was the 1763 decision in *Wilkes v. Wood*. Parliamentarian John Wilkes was a loud critic of the prime minister. After Wilkes published an especially stinging pamphlet, his home was raided for

inculpatory papers. In a case closely watched in the colonies, Wilkes then sued for damages—and won.

In 1886, the Supreme Court faced its first important case on the meaning of Fourth and Fifth amendments. Edward Boyd, a glass merchant, challenged a government subpoena for documents related to alleged evasion of customs duties. Drawing on the Wilkes case and other Founding era precedent, the Court held that a subpoena for “a man’s private papers,” apparently including business records, was per se a violation of the Fourth and Fifth amendments.

In the first half of the 20th century, the Court retreated from this formulation in the face of growing demands by the emerging New Deal regulatory state for more investigative powers. In 1976, it withdrew Fourth Amendment protection for private papers held by a third party. In 1973 and 1976, it held that subpoenas for documents from third parties no longer raised a Fifth Amendment issue. The *Boyd* rule, once thought the foundation of civil liberty, was dead.

Although some justices have lately registered some awareness of the important constitutional issues raised by data held by third-party online intermediaries, the Court has so far failed to reconsider its abandonment of *Boyd’s* rule.

In this vacuum, Congress might have stepped in. True, it did respond to the Bork videos story by enacting the Video Privacy Protection Act in 1988. And, it passed the

Stored Communications Act (SCA) in 1986, which now provides a primitive framework for regulating government acquisition of online-related data. But the SCA—written for the Internet circa 1986—is now about as technologically up to date as Judge Bork’s VCR.

The net result is that there are no reliable guideposts to help even well-meaning government lawyers manage these competing concerns. The failure means that there’s no sure way to ensure that both legitimate investigative ends and constitutional values are respected in the current Facebook/DreamHost investigation. It’s a failure we can’t blame the Framers for—only Congress and the Court.

Aziz Huq is the Frank and Bernice J. Greenberg Professor of Law at the University of Chicago Law School.

Rankings

40 Under 40	Most Powerful Women
100 Best Companies	World’s Greatest Leaders
Fortune 500	World’s Most Admired Companies
Global 500	See All Rankings

Sections

Automotives	The Ledger	Health	Retail
Careers	Venture	International	Sports
Design	Finance	Leadership	Technology
Executive Travel	Energy & Environment	Lifestyle	Commentary
		Luxury	

Customer Support

Frequently Asked Questions

Exhibit D

Coronavirus Updates for Department Employees



MENU

Search

U.S. Department of Commerce

[Home](#) » [News](#) » [Press releases](#)

Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States

Wilbur Ross

In response to President Trump's Executive Orders signed August 6, 2020, the Department of Commerce (Commerce) today announced prohibitions on transactions relating to mobile applications (apps) WeChat and TikTok to safeguard the national security of the United States. The Chinese Communist Party (CCP) has demonstrated the means and motives to use these apps to threaten the national security, foreign policy, and the economy of the U.S. Today's announced prohibitions, when combined, protect users in the U.S. by eliminating access to these applications and significantly reducing their functionality.

"Today's actions prove once again that President Trump will do everything in his power to guarantee our national security and protect Americans from the threats of the Chinese Communist Party," **said U.S. Department of Commerce Secretary Wilbur Ross**. "At the President's direction, we have taken significant action to combat China's malicious collection of American citizens' personal data, while promoting our national values, democratic rules-based norms, and aggressive enforcement of U.S. laws and regulations."

FOR IMMEDIATE RELEASE
Friday, September 18, 2020

Office of Public Affairs
(202) 482-4883
publicaffairs@doc.gov

While the threats posed by WeChat and TikTok are not identical, they are similar. Each collects vast swaths of data from users, including network activity, location data, and browsing and search histories. Each is an active participant in China's civil-military fusion and is subject to mandatory cooperation with the intelligence services of the CCP. This combination results in the use of WeChat and TikTok creating unacceptable risks to our national security.

As of September 20, 2020, the following transactions are prohibited:

1. Any provision of service to distribute or maintain the **WeChat or TikTok** mobile applications, constituent code, or application updates through an online mobile application store in the U.S.;
2. Any provision of services through the **WeChat** mobile application for the purpose of transferring funds or processing payments within the U.S.

As of September 20, 2020, for WeChat and as of November 12, 2020, for TikTok, the following transactions are prohibited:

1. Any provision of internet hosting services enabling the functioning or optimization of the mobile application in the U.S.;
2. Any provision of content delivery network services enabling the functioning or optimization of the mobile application in the U.S.;
3. Any provision directly contracted or arranged internet transit or peering services enabling the function or optimization of the mobile application within the U.S.;
4. Any utilization of the mobile application's constituent code, functions, or services in the functioning of software or services developed and/or accessible within the U.S.

Any other prohibitive transaction relating to WeChat or TikTok may be identified at a future date. Should the U.S. Government determine that WeChat's or TikTok's illicit behavior is being replicated by another app somehow outside the scope of these executive orders, the President has the authority to consider whether additional orders may be appropriate to address such activities. The President has provided until November 12 for the national security concerns posed by TikTok to be resolved. If they are, the prohibitions in this order may be lifted.

The notices for these actions will be posted on the Federal Register at approximately 8:45AM EDT on Friday, September 18, 2020.

Background:

On August 6, 2020, President Trump signed Executive Orders (E.O.) 13942, Addressing the Threat Posed by TikTok, and E.O. 13943, Addressing the Threat Posed by WeChat. In the E.O.s, the President determined that the apps capture vast swaths of information from U.S. users, leaving the data

vulnerable to CCP access for nefarious purposes. Commerce, at the Direction of the President, was required to identify transactions within 45 days to protect national security and the private data of millions of people across the country. Today's announced prohibitions fulfill the President's direction and mitigate national security risks.

LEADERSHIP

[Wilbur Ross](#)

TAGS

 [National security](#)

▼ Explore

[Issues](#)

[News](#)

[Data and reports](#)

[Work with us](#)

▼ About us

[Our mission](#)

[Strategic plan](#)

[Bureaus and offices](#)

[Privacy program](#)

▼ Get in touch

[Contact us](#)

[Staff directory](#)

Exhibit E



ADVERTISEMENT

BUSINESS

How U.S. video game companies are building tools for China's surveillance state



Software developers at American gaming companies are getting roped into building the tools of the Chinese social control state. (Josh Lefkowitz/Getty Images)

By JAMES B. CUTCHIN

JULY 22, 2019 | 4 AM



Last October, software developers at Riot Games in Santa Monica fielded an unusual request. As with other video game makers, Riot’s success depends on its ability to make games that are compulsively playable, like its global hit “League of Legends.” But Tencent, the Chinese tech giant that owns Riot, needed a way to force some of its most enthusiastic customers to play less.

While it has owned a controlling stake in Riot since 2011, Tencent has generally been hands-off when it comes to the company’s products. But facing increasing pressure from Chinese state media and regulators over its role in a supposed epidemic of video game addiction, Tencent needed a way to track how much time individual gamers in China

spent playing “League of Legends” — and kick out minors who exceeded two hours per day. If Riot engineers didn’t supply an “anti-addiction system” for “League of Legends,” they might lose access to the Chinese market altogether.

For the record:

10:00 PM, Jul. 29, 2019 *This article describes Sesame Credit’s service as a private pilot program for a national social credit system. Ant Financial, the program’s operator and an affiliate of the Chinese tech giant Alibaba, says the program is “in no way contracted to run or affiliated with China’s social credit system.”*

Within weeks, an update brought these features to the Chinese version of “League of Legends.”

Over the last year, one game company after another has quietly acceded to Chinese government demands to limit the amount of time young people spend on their games. Chinese players of American hits such as “League of Legends,” “Fortnite” and “World of Warcraft” are having their playtime tracked according to their national ID number. Those younger than 18 face heavy in-game penalties or outright expulsions if they play too long.

ADVERTISEMENT

Although it’s Chinese policy driving the restrictions, data privacy advocates say that for Americans to participate in the creation of these tools represents the crossing of a concerning new threshold. They view the moves as part of a [problematic trend](#) of Western technology firms redesigning their services to create China-friendly versions aligned with the country’s tighter social controls.

“For American companies, it really comes down to deciding whether or not you are willing to participate in this type of surveillance,” said Matt Erickson, executive director

of the Digital Privacy Alliance. “If they do choose to take part, it makes these companies not unwitting but full-blown accomplices in the Chinese police state.”

Access to the world’s second-largest market is a powerful incentive, but for some companies, supporting Chinese censorship and social control efforts is not a matter of choice. As Chinese giants buy up American tech companies, from West Hollywood-based gay dating app Grindr to Motorola’s mobile phone business, [regulators are raising questions](#) about companies’ autonomy and ability to push back on requests that might violate their ethical principles.

Internal documents from Riot Games obtained by The Times offer a rare glimpse into how the Chinese government exercises influence over companies beyond its borders.

ADVERTISEMENT

Tencent is the world’s largest game publisher and owns large or controlling stakes in a range of industry-leading developers including “Clash of Clans” maker Supercell and “Fortnite” developer Epic Games. Its self-developed title, “Honor of Kings,” was the world’s [highest-grossing mobile game](#) of 2018. The game’s success made it a lightning rod for growing Chinese government concerns of gaming addiction among Chinese youth, prompting Tencent to build its first ID-tracking playtime restriction system and pledge to incorporate similar systems on all of its games in 2019.

A digital presentation circulated via email among developers at Riot’s Santa Monica headquarters called for an “AAS [anti-addiction system] upgrade” for “League of Legends” in China. The presentation, authored in China, framed the request alongside accounts of growing Chinese government criticism of the gaming industry, official media attacks on Tencent, and a stark reminder that “League of Legends” “cannot [be] free from regulation.”

The request specified the need for features tagging teenage players in accordance with “future AAS regulation.” It also asked for the ability to kick certain players from the

game at specified times and restrict time-based in-game rewards. The presentation's author included mock-ups of "anti-addiction warning" pop-ups on "League of Legends," with messages telling players they had reached their daily gaming limits or were forbidden to play between particular hours (9 p.m. to 8 a.m.).

It did not take developers long to produce the requested features. In a December 2018 [post](#) on Chinese social media site QQ, Riot China announced an update to "League of Legends" including most of the changes.

ADVERTISEMENT

When asked about the U.S.-based staff's level of involvement with the development of the ID-tracking and playtime restriction systems, Riot Games said in a statement, "Our lead engineers, based in California, are aware of every feature that we create for 'League of Legends.' We develop market-specific features collaboratively, with representatives from our engineering teams around the world."

Tencent referred questions to an outside PR agency, which declined to provide responses.

While such systems are becoming standard in China, Jay Stanley, a policy analyst at the American Civil Liberties Union, said they constitute a granular privacy invasion that runs counter to American norms.

"American companies are part of American society and should be institutions that we can trust, abiding by American values," Stanley said. "If these companies are running overseas and participating in authoritarian regimes, then it's a real problem."

ADVERTISEMENT

Stanley acknowledged that it would be difficult for businesses like Riot to refuse to implement these systems at the cost of being locked out of the [\\$36.5-billion Chinese](#)

[gaming market](#), but said that failing to do so would help normalize invasive surveillance internationally. “This is going to put a lot of businesses in a bind, but we as a country need to defend American values,” Stanley said.

U.S. tech giants such as Google and Facebook have faced similar difficult choices about whether to create censored versions of their platforms in order to gain access to China. Google [left the country in 2010](#) amid disputes over censored search results and a major hacking incident. Last year’s revelation that the company had secretly begun work on a censor-compliant Chinese search engine, code-named [Project Dragonfly](#), sparked an outcry from Google employees and U.S. politicians. (A Google official told Congress last week that it has [terminated the project](#).) Facebook has [reportedly given up on entering China](#) after years of courting Beijing failed to win the company a reprieve from a 2009 ban. Meanwhile, U.S. lawmakers have begun to call for an end to American investor money being [channeled toward development of Chinese surveillance systems](#) used in the repression of religious and ethnic minorities.

The anti-addiction regulations referenced in the Riot documents appear to refer to a [Chinese Ministry of Education statement](#) released last year. In it, the ministry said it would take steps to control the number of online games available, explore age-based restrictions and limit the amount of time adolescents spend gaming. No specifics or timeline were given, but many major game publishers in China rolled out their own solutions in anticipation of government action.

Tencent started requiring mandatory age and ID authentication on its top-grossing mobile game “Honor of Kings” in 2018, making players provide their Chinese national ID information for [verification against police databases](#). The company has said the checks will be applied to all of its games this year and has been conducting trials of additional verification methods including mandatory [facial recognition checks](#).

The Shenzhen-based firm, which also owns China's largest social media platform, WeChat, is under intense pressure to address Chinese government concerns around the negative effects of gaming. Tencent's market value fell by a [record-breaking](#) \$271 billion last year partly because of a complete freeze on new game approvals from March through December of 2018. (The stock [has since rallied](#) as regulators began working through the backlog.) The halt came amid a flurry of official criticism blaming excessive gaming for everything from increasing rates of nearsightedness among youth to potential national security vulnerabilities from [mobile gaming addiction among military personnel](#).

Lisa Cosmas Hanson, founder of Asia-focused gaming market intelligence firm Niko Partners, said that the freeze on game approvals and the resulting backlog have hurt many game companies in China, forcing some smaller operations to shut down. Although approvals have resumed, the process has become more difficult, she said.

"Publishers in China have told me things like that it used to be a 20-page application and now it's 300," Hanson said. According to research by her firm, only 75 imported games have been approved so far this year, down from 467 in 2017.

Although real-ID verification systems are relatively new, features designed to limit the amount of time Chinese gamers spend online have been around for more than a decade. Irvine-based Blizzard Entertainment put a three-hour playtime limit on the Chinese server for its massively multiplayer online role-playing game, "World of Warcraft," in 2006. Gamers got around the restrictions by creating multiple accounts and switching between them, but the system has since been upgraded to require age and identity verification through a national ID.

ADVERTISEMENT

"Fortnite," which has held the title of the world's largest and highest-grossing free-to-play online game for most of the last year, [rolled out similar ID verification and playtime](#)

[tracking](#) restrictions in China earlier this year. Neither “Fortnite” publisher Epic Games, based in Cary, N.C., nor Blizzard Entertainment responded to requests for comment.

Looming over all this is China’s planned rollout of a [social credit system](#), which will assign citizens a score incorporating both standard financial metrics, such as debt repayment, and more personal information such as shopping habits and online behavior. Once a nationwide system debuts in 2020, a citizen with a low score could reportedly face penalties such as losing the right to buy plane and high-speed rail tickets, take out loans or purchase property. Excessive time spent playing video games is one specific [behavior that could lower your score](#) with Sesame Credit — one of the system’s main private pilot programs. This applies not only to minors but gamers of all ages.

While there have as yet been no indications of ID-linked tracking systems being used for anything beyond limiting minors’ gaming time, some people remain concerned about the potential for future misuse, particularly because Tencent has already conducted its own [short-lived pilot of a social credit system](#) last year.

“There is no right to privacy in China,” said Erickson, of the Digital Privacy Alliance. “Any information collected to make sure kids aren’t playing too many video games will definitely be used by the government and the police for whatever purpose they see fit.”

ADVERTISEMENT

Jack Poulson, founder of the advocacy group Tech Inquiry, says American tech workers — lacking visibility into executive-level decisions and other divisions of their sprawling conglomerates — aren’t always aware when they are participating in projects that might go against their values. “There’s no real protection in place to ensure that employees have an understanding of what they are helping build,” he said.

Poulson served as a senior scientist at Google’s research and machine intelligence department before [publicly resigning](#) last year in the wake of the Project Dragonfly



Your guide to our new economic reality.

Get our free business newsletter for insights and tips for getting by.

Enter Email Address

SIGN ME UP

You may occasionally receive promotional content from the Los Angeles Times.



James B. Cutchin



Twitter

James B. Cutchin was a USC Annenberg Media, Economic & Entrepreneurship fellow in the Business section in 2019.

MORE FROM THE LOS ANGELES TIMES

HOT PROPERTY

Heather Graham sells Hollywood Hills haunt she bought after 'Boogie Nights'

2 hours ago

BUSINESS

U.S. layoffs remain elevated as 837,000 seek jobless aid

1 hour ago

revelations. He founded Tech Inquiry to help tech workers push back on unethical requests. He said the first step to ensuring that staff aren't corralled into work they find morally objectionable is having a clear understanding of a project's end goals, but he acknowledged that in Riot's case the murky distinction between the Chinese public and private sectors makes this easier said than done.

"How do you even get a sense of what the likely uses of this data could be? It could be a government decision, it could be Tencent," Poulson said. "With something like this, it's obviously more complicated."

Riot Games and surveillance



L.A. Times Today airs Monday through Friday at 7 p.m. and 10 p.m. exclusively on Spectrum News 1.

ADVERTISEMENT

BUSINESS

TECHNOLOGY

WORLD & NATION

Exhibit F

Every moment of every day, mobile phone apps collect detailed location data.



Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret

Dozens of companies use smartphone locations to help advertisers and even hedge funds. They say it's anonymous, but the data shows how personal it is.

By JENNIFER VALENTINO-DeVRIES, NATASHA SINGER, MICHAEL H. KELLER and AARON KROLIK DEC. 10, 2018

The millions of dots on the map trace highways, side streets and bike trails — each one following the path of an anonymous cellphone user.

One path tracks someone from a home outside Newark to a nearby Planned Parenthood, remaining there for more than an hour. Another represents a person who travels with the mayor of New York during the day and returns to Long Island at night.

Yet another leaves a house in upstate New York at 7 a.m. and travels to a middle school 14 miles away, staying until late afternoon each school day. Only one person makes that trip: Lisa Magrin, a 46-year-old math teacher. Her smartphone goes with her.

An app on the device gathered her location information, which was then sold without her knowledge. It recorded her whereabouts as often as every two seconds, according to a database of more than a million phones in the New York area that was reviewed by The New York Times. While Ms. Magrin's identity was not disclosed in those records, The Times was able to easily connect her to that dot.

The app tracked her as she went to a Weight Watchers meeting and to her dermatologist's office for a minor procedure. It followed her hiking with her dog and staying at her ex-boyfriend's home, information she found disturbing.

"It's the thought of people finding out those intimate details that you don't want people to know," said Ms. Magrin, who allowed The Times to review her location data.

Like many consumers, Ms. Magrin knew that apps could track people's movements. But as smartphones have become ubiquitous and technology more accurate, an industry of snooping on people's daily habits has spread and grown more intrusive.

At least 75 companies receive anonymous, precise location data from apps whose users enable location services to get local news and weather or other information, The Times found. Several of those businesses claim to track up to 200 million mobile devices in the United States — about half those in use last year. The database reviewed by The Times — a sample of information gathered in 2017 and held by one company — reveals people's travels in startling detail, accurate to within a few yards and in some cases updated more than 14,000 times a day.

[Learn how to stop apps from tracking your location.]

These companies sell, use or analyze the data to cater to advertisers, retail outlets and even hedge funds seeking insights into consumer behavior. It's a hot market, with sales of location-targeted advertising reaching an estimated \$21 billion this year. IBM has gotten into the industry, with its purchase of the Weather Channel's apps. The social network Foursquare remade itself as a location marketing company. Prominent investors in location start-ups include Goldman Sachs and Peter Thiel, the PayPal co-founder.

Businesses say their interest is in the patterns, not the identities, that the data reveals about consumers. They note that the information apps collect is tied not to someone's name or phone number but to a unique ID. But those with access to the raw data — including employees or clients — could still identify a person without consent. They could follow someone they knew, by pinpointing a phone that regularly spent time at that person's home address. Or, working in reverse, they could attach a name to an anonymous dot, by seeing where the device spent nights and using public records to figure out who lived there.

Many location companies say that when phone users enable location services, their data is fair game. But, The Times found, the explanations people see when prompted to give permission are often incomplete or misleading. An app may tell users that granting access to their location will help them get traffic information, but not mention that the data will be shared and sold. That disclosure is often buried in a vague privacy policy.

“Location information can reveal some of the most intimate details of a person's life — whether you've visited a psychiatrist, whether you went to an A.A. meeting, who you might date,” said Senator Ron Wyden, Democrat of Oregon, who has proposed bills to limit the collection and sale of such data, which are largely unregulated in the United States.

“It's not right to have consumers kept in the dark about how their data is sold and shared and then leave them unable to do anything about it,” he added.

Mobile Surveillance Devices

After Elise Lee, a nurse in Manhattan, saw that her device had been tracked to the main operating room at the hospital where she works, she expressed concern about her privacy and that of her patients.

“It's very scary,” said Ms. Lee, who allowed The Times to examine her location history in the data set it reviewed. “It feels like someone is following me, personally.”

The mobile location industry began as a way to customize apps and target ads for nearby businesses, but it has morphed into a data collection and analysis machine.

Retailers look to tracking companies to tell them about their own customers and their competitors'. For a web seminar last year, Elina Greenstein, an executive at the location company GroundTruth, mapped out the path of a hypothetical consumer from home to work to show potential clients how tracking could reveal a person's preferences. For example, someone may search online for healthy recipes, but GroundTruth can see that the person often eats at fast-food restaurants.

"We look to understand who a person is, based on where they've been and where they're going, in order to influence what they're going to do next," Ms. Greenstein said.

Financial firms can use the information to make investment decisions before a company reports earnings — seeing, for example, if more people are working on a factory floor, or going to a retailer's stores.

Health care facilities are among the more enticing but troubling areas for tracking, as Ms. Lee's reaction demonstrated. Tell All Digital, a Long Island advertising firm that is a client of a location company, says it runs ad campaigns for personal injury lawyers targeting people anonymously in emergency rooms.

"The book '1984,' we're kind of living it in a lot of ways," said Bill Kakis, a managing partner at Tell All.

Jails, schools, a military base and a nuclear power plant — even crime scenes — appeared in the data set The Times reviewed. One person, perhaps a detective, arrived at the site of a late-night homicide in Manhattan, then spent time at a nearby hospital, returning repeatedly to the local police station.

Two location firms, Fysical and SafeGraph, mapped people attending the 2017 presidential inauguration. On Fysical's map, a bright red box near the Capitol steps indicated the general location of President Trump and those around him, cellphones pinging away. Fysical's chief executive said in an email that the data it used was anonymous. SafeGraph did not respond to requests for comment.

More than 1,000 popular apps contain location-sharing code from such companies, according to 2018 data from MightySignal, a mobile analysis firm. Google's Android system was found to have about 1,200 apps with such code, compared with about 200 on Apple's iOS.

The most prolific company was Reveal Mobile, based in North Carolina, which had location-gathering code in more than 500 apps, including many that provide local news. A Reveal spokesman said that the popularity of its code showed that it helped app developers make ad money and consumers get free services.

To evaluate location-sharing practices, The Times tested 20 apps, most of which had been flagged by researchers and industry insiders as potentially sharing the data. Together, 17 of the apps sent exact latitude and longitude to about 70 businesses. Precise location data from one app, WeatherBug on iOS, was received by 40 companies. When contacted by The Times, some of the companies that received that data described it as “unsolicited” or “inappropriate.”

WeatherBug, owned by GroundTruth, asks users’ permission to collect their location and tells them the information will be used to personalize ads. GroundTruth said that it typically sent the data to ad companies it worked with, but that if they didn’t want the information they could ask to stop receiving it.

The Times also identified more than 25 other companies that have said in marketing materials or interviews that they sell location data or services, including targeted advertising.

[Read more about how The Times analyzed location tracking companies.]

The spread of this information raises questions about how securely it is handled and whether it is vulnerable to hacking, said Serge Egelman, a computer security and privacy researcher affiliated with the University of California, Berkeley.

“There are really no consequences” for companies that don’t protect the data, he said, “other than bad press that gets forgotten about.”

A Question of Awareness

Companies that use location data say that people agree to share their information in exchange for customized services, rewards and discounts. Ms. Magrin, the teacher, noted that she liked that tracking technology let her record her jogging routes.

Brian Wong, chief executive of Kiip, a mobile ad firm that has also sold anonymous data from some of the apps it works with, says users give apps permission to use and share their data. “You are receiving these services for free because advertisers are helping monetize and pay for it,” he said, adding, “You would have to be pretty oblivious if you are not aware that this is going on.”

But Ms. Lee, the nurse, had a different view. “I guess that’s what they have to tell themselves,” she said of the companies. “But come on.”

Ms. Lee had given apps on her iPhone access to her location only for certain purposes — helping her find parking spaces, sending her weather alerts — and only if they did not indicate that the information would be used for anything else, she said. Ms. Magrin had allowed about a dozen apps on her Android phone access to her whereabouts for services like traffic notifications.

But it is easy to share information without realizing it. Of the 17 apps that The Times saw sending precise location data, just three on iOS and one on Android told users in a prompt during the permission process that the information could be used for advertising. Only one app, GasBuddy, which identifies nearby gas stations, indicated that data could also be shared to “analyze industry trends.”

More typical was theScore, a sports app: When prompting users to grant access to their location, it said the data would help “recommend local teams and players that are relevant to you.” The app passed precise coordinates to 16 advertising and location companies.

A spokesman for theScore said that the language in the prompt was intended only as a “quick introduction to certain key product features” and that the full uses of the data were described in the app’s privacy policy.

The Weather Channel app, owned by an IBM subsidiary, told users that sharing their locations would let them get personalized local weather reports. IBM said the subsidiary, the Weather Company, discussed other uses in its privacy policy and in a separate “privacy settings” section of the app. Information on advertising was included there, but a part of the app called “location settings” made no mention of it.

The app did not explicitly disclose that the company had also analyzed the data for hedge funds — a pilot program that was promoted on the company’s website. An IBM spokesman said the pilot had ended. (IBM updated the app’s privacy policy on Dec. 5, after queries from The Times, to say that it might share aggregated location data for commercial purposes such as analyzing foot traffic.)

Even industry insiders acknowledge that many people either don’t read those policies or may not fully understand their opaque language. Policies for apps that funnel location information to help investment firms, for instance, have said the data is used for market analysis, or simply shared for business purposes.

“Most people don’t know what’s going on,” said Emmett Kilduff, the chief executive of Eagle Alpha, which sells data to financial firms and hedge funds. Mr. Kilduff said responsibility for complying with data-gathering regulations fell to the companies that collected it from people.

Many location companies say they voluntarily take steps to protect users’ privacy, but policies vary widely.

For example, Sense360, which focuses on the restaurant industry, says it scrambles data within a 1,000-foot square around the device’s approximate home location. Another company, Factual, says that it collects data from consumers at home, but that its database doesn’t contain their addresses.

Some companies say they delete the location data after using it to serve ads, some use it for ads and pass it along to data aggregation companies, and others keep the information for years.

Several people in the location business said that it would be relatively simple to figure out individual identities in this kind of data, but that they didn’t do it. Others suggested it would require so much effort that hackers wouldn’t bother.

It “would take an enormous amount of resources,” said Bill Daddi, a spokesman for Cuebiq, which analyzes anonymous location data to help retailers and others, and raised more than \$27 million this year from investors including Goldman Sachs and Nasdaq Ventures. Nevertheless, Cuebiq encrypts its information, logs employee queries and sells aggregated analysis, he said.

There is no federal law limiting the collection or use of such data. Still, apps that ask for access to users' locations, prompting them for permission while leaving out important details about how the data will be used, may run afoul of federal rules on deceptive business practices, said Maneesha Mithal, a privacy official at the Federal Trade Commission.

"You can't cure a misleading just-in-time disclosure with information in a privacy policy," Ms. Mithal said.

Following the Money

Apps form the backbone of this new location data economy.

The app developers can make money by directly selling their data, or by sharing it for location-based ads, which command a premium. Location data companies pay half a cent to two cents per user per month, according to offer letters to app makers reviewed by The Times.

Targeted advertising is by far the most common use of the information.

Google and Facebook, which dominate the mobile ad market, also lead in location-based advertising. Both companies collect the data from their own apps. They say they don't sell it but keep it for themselves to personalize their services, sell targeted ads across the internet and track whether the ads lead to sales at brick-and-mortar stores. Google, which also receives precise location information from apps that use its ad services, said it modified that data to make it less exact.

Smaller companies compete for the rest of the market, including by selling data and analysis to financial institutions. This segment of the industry is small but growing, expected to reach about \$250 million a year by 2020, according to the market research firm Opimas.

Apple and Google have a financial interest in keeping developers happy, but both have taken steps to limit location data collection. In the most recent version of Android, apps that are not in use can collect locations "a few times an hour," instead of continuously.

Apple has been stricter, for example requiring apps to justify collecting location details in pop-up messages. But Apple's instructions for writing

these pop-ups do not mention advertising or data sale, only features like getting “estimated travel times.”

A spokesman said the company mandates that developers use the data only to provide a service directly relevant to the app, or to serve advertising that met Apple’s guidelines.

Apple recently shelved plans that industry insiders say would have significantly curtailed location collection. Last year, the company said an upcoming version of iOS would show a blue bar onscreen whenever an app not in use was gaining access to location data.

The discussion served as a “warning shot” to people in the location industry, David Shim, chief executive of the location company Placed, said at an industry event last year.

After examining maps showing the locations extracted by their apps, Ms. Lee, the nurse, and Ms. Magrin, the teacher, immediately limited what data those apps could get. Ms. Lee said she told the other operating-room nurses to do the same.

“I went through all their phones and just told them: ‘You have to turn this off. You have to delete this,’” Ms. Lee said. “Nobody knew.”

Adam Satariano contributed reporting.

Related Coverage

- [How Game Apps That Captivate Kids Have Been Collecting Their Data](#) SEPT. 12, 2018
- [Service Meant to Monitor Inmates’ Calls Could Track You, Too](#) MAY 10, 2018
- [Hundreds of Apps Can Empower Stalkers to Track Their Victims](#) MAY 19, 2018

Exhibit G

HOURLY NEWS

LISTEN LIVE

PLAYLIST



DONATE



MEDIA

Twitter Bans Alex Jones And InfoWars; Cites Abusive Behavior

September 6, 2018 · 5:34 PM ET

AVIE SCHNEIDER



Alex Jones of InfoWars talks to reporters outside a Senate Intelligence Committee hearing on Wednesday. Twitter has permanently suspended the conspiracy theorist, citing violations of its policy on abusive behavior.

Drew Angerer/Getty Images

Updated at 6:29 p.m. ET

Twitter on Thursday said it has "permanently suspended" conspiracy theorist Alex Jones and his InfoWars outlet, citing "new reports of Tweets and videos posted yesterday that violate our abusive behavior policy."

Last month, YouTube, Apple, Facebook and Spotify banned Jones' main platforms over concerns about his content. But Twitter only suspended some of his privileges, a move that drew criticism.

On Wednesday, Florida Sen. Marco Rubio tussled with Jones after Jones confronted and touched him outside a Senate Intelligence Committee hearing.

And at a House Energy and Commerce Committee hearing, Twitter CEO Jack Dorsey faced questions amid criticism from Republicans that big tech companies suppress conservatives online.



DIGITAL LIFE

Twitter CEO Jack Dorsey Explains Why Alex Jones Isn't Banned, In Big Tech Exception



POLITICS

Marco Rubio Clashes With Alex Jones In Capitol: 'I'll Take Care Of You Myself'

Dorsey denied that Twitter is politically selective. He tweeted: "I want to start by making something clear: we don't consider political viewpoints, perspectives, or party affiliation in any of our policies or enforcement decisions. Period. Impartiality is our guiding principle."

But on Thursday, Twitter announced in a tweet: "Today, we permanently suspended @realalexjones and @infowars from Twitter and Periscope. We took this action based on new reports of Tweets and videos posted yesterday that violate our abusive behavior policy, in addition to the accounts' past violations."

Twitter linked to its page detailing its policy on abusive behavior. That policy states, in part: "You may not engage in the targeted harassment of someone, or incite other

people to do so. We consider abusive behavior an attempt to harass, intimidate, or silence someone else's voice."

After the ban was announced, Jones said in a video posted on the InfoWars website: "I was taken down, not because we lied but because we tell the truth and because we were popular. And because we dared go to that committee hearing and stand up to Rubio and stand up to the lies of mainstream media and speak the truth. ...

"This is the deep state striking back and really pressuring these tech firms to censor," Jones added.

In August, Dorsey explained why Twitter had not banned Jones then. "He hasn't violated our rules. We'll enforce if he does," Dorsey tweeted. In an apparent reference to other tech companies that had banned Jones, he said that Twitter would not "succumb and simply react to outside pressure."



MEDIA

YouTube, Apple and Facebook Ban Infowars, Which Decries 'Mega Purge'



DIGITAL LIFE

Alex Jones Penalized By Twitter

Dorsey added, "We're going to hold Jones to the same standard we hold to every account, not taking one-off actions to make us feel good in the short term, and adding fuel to new conspiracy theories."

As NPR's David Folkenflik noted, "The ideas that Jones shares are particularly noxious, the idea that Sandy Hook massacre of schoolchildren was a hoax, the idea that 9/11 was an inside job, and other things."

Jones is facing defamation lawsuits, most centering on comments about school shootings.

After the earlier bans, Jones said that "America has been sold out," and the Infowars Twitter feed declared that the moves against his company were "communist style censorship."

infowars alex jones twitter

More Stories From NPR



NATIONAL

Anita Hill On Sexual Harassment In Hollywood And Beyond



Exhibit H

Facebook Removes Roger Stone for Ties to Fake Accounts

The social network said the fake accounts were active around the 2016 presidential election.

By Davey Alba

Published July 8, 2020 Updated July 10, 2020

[Read more on Roger Stone's sentence being commuted by President Trump.]

Facebook on Wednesday said it was removing the personal accounts of Roger J. Stone Jr., President Trump's friend and ally, because they had ties to numerous fake accounts that were active around the 2016 presidential election.

The company made the announcement as part of its monthly report on removing disinformation. Mr. Stone's personal accounts on Facebook and Instagram, which is owned by Facebook, were entwined with a U.S.-based network of accounts that had links to the Proud Boys, a group that promotes white supremacy, the company said. The social network banned the Proud Boys group in 2018.

"We first started looking into this network as part of our investigation into the Proud Boys' attempt to return to Facebook after we had designated and banned them from the platform," Nathaniel Gleicher, Facebook's head of cybersecurity policy, wrote in a company blog post announcing Facebook's takedown. "Our investigation linked this network to Roger Stone and his associates."

Mr. Stone, 67, is set to go to prison this month. In November, a jury convicted him on seven felonies, including lying to federal investigators, tampering with a witness and impeding a congressional inquiry. The charges were brought by the special counsel, Robert S. Mueller III, whose investigators scrutinized Mr. Stone's attempts during the 2016 presidential election to communicate with WikiLeaks about the release of Democratic emails that had been stolen by Russian operatives.

In a statement, Mr. Stone denied overseeing fake accounts on Facebook or Instagram. "This extraordinary active censorship for which Facebook and Instagram give entirely fabricated reasons," he said, "is part of a larger effort to censor supporters of the president, Republicans and conservatives on social media platforms. The claim that I have utilized or control unauthorized or fake accounts on any platform is categorically and provably false."

This is not the first time that Mr. Stone has been kicked off a major social media platform. In October 2017, Mr. Stone was suspended from Twitter after insulting several CNN news anchors and contributors. In July 2019, the federal judge overseeing the case brought by Mr. Mueller ordered Mr. Stone off major social media platforms. The judge said Mr. Stone had violated a gag order by using them to attack the special counsel's investigation and officials tied to it.

Mr. Stone's accounts were part of the 54 Facebook accounts, 50 pages and four Instagram accounts that Facebook said were associated with the Proud Boys network. The network, the company said, was most active in 2016 and 2017, during the run-up to the United States presidential election and immediately after. A few accounts were still active into 2020, posting primarily about Mr. Stone's court case and judgment according to Graphika, a company that specializes in analyzing social media, which released a report about Facebook's Wednesday takedown.

Many of the accounts that Facebook removed used fake personas, stole pictures of people around the internet and published posts promoting Mr. Stone, according to Graphika's analysis. The accounts publicized his books in 2016, and pushed for his legal defenses in 2019 and appeals for a pardon in 2020.



Posts about the legal process surrounding Mr. Stone’s arrest and sentencing from accounts in the network taken down by Facebook. Graphika

The accounts also posted hostile criticism of Hillary Clinton, especially in the lead-up to the 2016 election, Graphika said, and engaged in coordinated harassment against a judge who had temporarily blocked Mr. Trump’s executive order barring citizens of seven predominantly Muslim countries from entering the United States.

Facebook said it had identified the full scope of the network after hundreds of pages of search warrants and affidavits were released in response to a lawsuit filed by The New York Times and other news media organizations.

The social network said it also took down 35 Facebook accounts, 14 pages, one group and 38 Instagram accounts involved in a domestic disinformation campaign in Brazil, which were linked to “some of the employees of the offices” of President Jair Bolsonaro of Brazil and two of his sons, Congressman Eduardo Bolsonaro and Senator Flávio Bolsonaro. It was not clear whether Brazil’s president had any direct role in those accounts.

“This shows that coordinated inauthentic behavior can turn up in many places, even the offices of high-profile politicians,” said Ben Nimmo, director of investigations at Graphika. “It also shows that there’s a whole community out there hunting for this kind of operation. It’s a brain race between the influence operations and the people who hunt them, and every takedown teaches us a little more.”

Davey Alba is a technology reporter covering disinformation. In 2019, she won a Livingston Award for excellence in international reporting and a Mirror Award for best story on journalism in peril. @daveyalba

A version of this article appears in print on , Section B, Page 3 of the New York edition with the headline: Facebook Muzzles a Trump Ally

Exhibit I

The Latest

Facebook bans the Proud Boys, cutting the group off from its main recruitment platform

Taylor Hatmaker

@tayhatmaker / 5:27 pm PDT • October 30, 2018



 **Image Credits:** (Photo by Susan Watts/NY Daily News via Getty Images / Getty Images)

Facebook  is moving to ban the [Proud Boys](#), a far-right men's organization with ties to white supremacist groups. [Business Insider](#) first reported the decision. Facebook confirmed to TechCrunch the decision to ban the Proud Boys from Facebook and Instagram, indicating that the group (and presumably its leader Gavin McInnes) now meet the company's definition of a hate organization or figure.

Facebook provided the following statement:

Our team continues to study trends in organized hate and hate speech and works with partners to better understand hate organizations as they evolve. We ban these

organizations and individuals from our platforms and also remove all praise and support when we become aware of it. We will continue to review content, Pages, and people that violate our policies, take action against hate speech and hate organizations to help keep our community safe.

Facebook's policy on white supremacy plays right into a racist agenda



In an ongoing series over at Motherboard, we're learning quite a bit about how Facebook polices hate speech and hate organizations on its platform. Historically, the company has been far less than transparent about its often inconsistent censorship practices, even as white supremacist content — and plenty of other forms of hate targeted at marginalized ... [Continue reading](#)



TechCrunch



Even compared to other groups on the far right with online origins, the Proud Boys maximize their impact through social networking. The organization, founded by provocateur and Vice founder McInnes, relies on Facebook as its primary recruitment tool. As we reported in [August](#), the Proud Boys operate a surprisingly sophisticated network for getting new members into the fold via many local and regional Facebook groups. All of it relies on Facebook — the Proud Boys homepage even links out to the web of Facebook groups to guide potential recruits toward next steps.

At the time of writing, Facebook's ban appeared to affect some Proud Boys groups and not others. The profile of Proud Boys founder McInnes appears to still be functional. Facebook's decision to act against the organization is likely tied to the [recent arrest of five Proud Boys members](#) in New York City on charges including assault, criminal possession of a weapon and gang assault.

Exhibit J



Archive Details

Committee on Foreign Investment in the United States Completes Review of Proposed China Oceanwide and Genworth Financial Transaction

06/09/18

RICHMOND, Va., June 9, 2018 /PRNewswire/ -- China Oceanwide Holdings Group Co., Ltd. (Oceanwide) and Genworth Financial, Inc. (NYSE: GNW) today announced that the Committee on Foreign Investment in the United States (CFIUS) has completed its review of their proposed transaction and concluded that there are no unresolved national security concerns with respect to the proposed transaction. This satisfies one of the conditions to the closing of the proposed transaction.

In connection with the CFIUS review of the proposed transaction, Genworth and Oceanwide entered into a mitigation agreement which, among other things, requires Genworth to use a U.S.-based, third-party service provider to manage and protect the personal data of Genworth's U.S. policyholders.

The closing of the transaction remains subject to other conditions, including the receipt of required regulatory approvals in the U.S., China and other international jurisdictions. Genworth and Oceanwide are engaging with the relevant regulators regarding the pending applications.

"We are pleased that CFIUS has completed its review of our transaction and look forward to working with Oceanwide to obtain the remaining regulatory approvals needed and satisfy other conditions necessary to close the transaction as soon as possible," said Tom McInerney, president and CEO of Genworth.

Added LU Zhiqiang, chairman of Oceanwide: "Successfully concluding the CFIUS process is a major step in our efforts to complete this transaction, which will strengthen Genworth's financial position and allow us to bring Genworth's insurance expertise to China."

About Genworth Financial

Genworth Financial, Inc. (NYSE: GNW) is a Fortune 500 insurance holding company committed to helping families achieve the dream of homeownership and address the financial challenges of aging through its leadership positions in mortgage insurance and long term care insurance. Headquartered in Richmond, Virginia, Genworth traces its roots back to 1871 and became a public company in 2004. For more information, visit genworth.com.

From time to time, Genworth releases important information via postings on its corporate website. Accordingly, investors and other interested parties are encouraged to enroll to receive automatic email alerts and Really Simple Syndication (RSS) feeds regarding new postings. Enrollment information is found under the "Investors" section of genworth.com. From time to time, Genworth's publicly traded subsidiaries, Genworth MI Canada Inc. and Genworth Mortgage Insurance Australia Limited, separately release financial and other information about their operations. This information can be found at <http://genworth.ca> and <http://www.genworth.com.au>.

About China Oceanwide

China Oceanwide is a privately held, family owned international financial holding group founded by Mr. LU Zhiqiang. Headquartered in Beijing, China, China Oceanwide's well-established and diversified businesses include operations in financial services, energy, culture and media, and real estate assets globally, including in the United States.

China Oceanwide is the controlling shareholder of the Shenzhen-listed Oceanwide Holdings Co., Ltd. and Minsheng Holdings Co. Ltd.; the Hong Kong-listed China Oceanwide Holdings Limited; the privately-held Minsheng Securities, Minsheng Trust, and Asia Pacific Property & Casualty Insurance; and it is the single largest shareholder of Australia-listed CuDECO Ltd. China Oceanwide also is a minority investor in Shanghai-listed China Minsheng Bank and Hong Kong-listed Legend Holdings. In the United States, China Oceanwide has real estate investments in New York, California, and Hawaii. Businesses controlled by China Oceanwide have more than 10,000 employees globally.

Cautionary Note Regarding Forward-Looking Statements

This communication includes certain statements that may constitute "forward-looking statements" within the meaning of the federal securities laws, including Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended. Forward-looking statements may be identified by words such as "expects," "intends," "anticipates," "plans," "believes," "seeks," "estimates," "will" or words of similar meaning and include, but are not limited to, statements regarding the closing of the transaction and obtaining relevant regulatory approvals. Forward-looking statements are based on management's current expectations and assumptions, which are subject to inherent uncertainties, risks and changes in circumstances that are difficult to predict. Actual outcomes and results may differ materially from those in the forward-looking statements and factors that may cause such a difference

include, but are not limited to, risks and uncertainties related to: (i) the risk that the transaction may not be completed in a timely manner or at all, which may adversely affect Genworth's business and the price of Genworth's common stock; (ii) the parties' inability to obtain regulatory approvals, or the possibility that regulatory approvals may further delay the transaction or will not be received prior to July 1, 2018 (and either or both of the parties may not be willing to further waive their End Date termination rights beyond July 1, 2018) or that materially burdensome or adverse regulatory conditions may be imposed in connection with any such regulatory approvals (including those conditions that either or both of the parties may be unwilling to accept); (iii) the risk that a condition to closing of the transaction may not be satisfied; (iv) potential legal proceedings that may be instituted against Genworth following announcement of the transaction; (v) the risk that the proposed transaction disrupts Genworth's current plans and operations as a result of the announcement and consummation of the transaction; (vi) potential adverse reactions or changes to Genworth's business relationships with clients, employees, suppliers or other parties or other business uncertainties resulting from the announcement of the transaction or during the pendency of the transaction, including but not limited to such changes that could affect Genworth's financial performance; (vii) certain restrictions during the pendency of the transaction that may impact Genworth's ability to pursue certain business opportunities or strategic transactions; (viii) continued availability of capital and financing to Genworth before the consummation of the transaction; (ix) further rating agency actions and downgrades in Genworth's financial strength ratings; (x) changes in applicable laws or regulations; (xi) Genworth's ability to recognize the anticipated benefits of the transaction; (xii) the amount of the costs, fees, expenses and other charges related to the transaction; (xiii) the risks related to diverting management's attention from Genworth's ongoing business operations; (xiv) the impact of changes in interest rates and political instability; and (xv) other risks and uncertainties described in the Definitive Proxy Statement, filed with the SEC on January 25, 2017, and Genworth's Annual Report on Form 10-K, filed with the SEC on February 28, 2018. Unlisted factors may present significant additional obstacles to the realization of forward-looking statements. Consequences of material differences in results as compared with those anticipated in the forward-looking statements could include, among other things, business disruption, operational problems, financial loss, legal liability to third parties and similar risks, any of which could have a material adverse effect on Genworth's consolidated financial condition, results of operations, credit rating or liquidity. Accordingly, forward-looking statements should not be relied upon as representing Genworth's views as of any subsequent date, and Genworth does not undertake any obligation to update forward-looking statements to reflect events or circumstances after the date they were made, whether as a result of new information, future events or otherwise, except as may be required under applicable securities laws.

View original content: <http://www.prnewswire.com/news-releases/committee-on-foreign-investment-in-the-united-states-completes-review-of-proposed-china-oceanwide-and-genworth-financial-transaction-300663704.html>

SOURCE Genworth Financial, Inc.

Exhibit K

From: Ernest Galvan
Sent: Thursday, October 1, 2020 2:42 PM
To: Dennis.Fan@usdoj.gov; H.Thomas.Byron@usdoj.gov; Janda, Sean R. (CIV
Cc: Ben Bien-Kahn; Angus Ni; Michael W. Bien; Alex Gourse; Thomas Burke; Van Swearingen; Browning, Jack; Amy Xu; Karen Stilber; Erika Zheng; jfazio@dehengsv.com; Gossett, David; Clay Zhu
Subject: RE: US WeChat Users Alliance v Trump - CA9 Stay Motion [IWOV-DMS.FID71398]

Dear Counsel:

I will be working on any Ninth Circuit appeal. This email is to respond to yours of this morning regarding a stay application to the Ninth Circuit.
We will oppose any such application.

In addition to the lack of any need for a stay on the merits, your application is procedurally defective under the Federal Rules of Appellate Procedure. You have moved for and received a shortened schedule for briefing your stay motion to the district court. It is now set for hearing on October 15, and the district court has stated that it may advance the hearing to an earlier date. ECF No. 73. You therefore satisfy neither the FRAP 8(a)(2)(A)(i) requirement to show impracticability nor the subsection (ii) requirement that the district court denied the motion or failed to afford the relief requested.

You note that your client has not even given you permission to appeal yet, some 11 days after the preliminary injunction was issued, further confirming that there is no emergency to justify an extraordinary stay.

Best Regards,

Ernest Galvan
ROSEN BIEN GALVAN & GRUNFELD LLP
101 Mission Street, 6th Floor
San Francisco, CA 94105
(415) 433-6830 (telephone)
(415) 296-2293 (direct)
(415) 694-3606 (mobile)
(415) 433-7104 (fax)
egalvan@rbgg.com

CONFIDENTIALITY NOTICE

The information contained in this e-mail message may be privileged, confidential and protected from disclosure. If you are not the intended recipient, any dissemination, distribution or copying is strictly prohibited. If you think that you have received this e-mail message in error, please e-mail the sender at rbg@rbgg.com

IRS CIRCULAR 230 NOTICE: As required by United States Treasury Regulations, you should be aware that this communication is not intended by the sender to be used, and it cannot be used, for the purpose of avoiding penalties under United States federal tax laws.

From: Fan, Dennis (CIV) <Dennis.Fan@usdoj.gov>
Sent: Thursday, October 1, 2020 7:43 AM
To: Michael W. Bien <MBien@rbgg.com>; Alex Gourse <AGourse@rbgg.com>; Van

Swearingen <VSwearingen@rbgg.com>; Amy Xu <AXu@rbgg.com>;
angus@afnlegal.com; davidgossett@dwt.com; Thomas Burke
<THOMASBURKE@dwt.com>; jfazio@dehengsv.com
Cc: Byron, H. Thomas (CIV) <H.Thomas.Byron@usdoj.gov>; Janda, Sean R. (CIV)
<Sean.R.Janda@usdoj.gov>
Subject: US WeChat Users Alliance v Trump - CA9 Stay Motion

Dear counsel:

I hope you are well. We are reaching out to you regarding *U.S. WeChat Users Alliance v. Trump*, where, as we have stated in district court, the government intends to file a notice of appeal from the district court's preliminary injunction tomorrow, October 2, 2020, subject to the Solicitor General's authorization.

Tomorrow, we would also file in the Ninth Circuit an emergency motion to stay the preliminary injunction. Would you please inform me of plaintiffs' position on that motion no later than **close of business today**?

The attorneys copied here are the principal attorneys for the government on appeal, and if you have questions regarding the appeal please feel free to reach out to us.

Best,
Dennis

Dennis Fan
U.S. Department of Justice
Civil Division, Appellate Staff
Washington, DC
(202) 514-2494