ALM | LAW.COM

New York Law Journal

# Using TikTok Could Become a Federal Crime

**By Aidan P. O'Connor and Daniel Cohen**
May 3, 2024

President Joe Biden signed a law on April 24, 2024, that bans TikTok in the United States unless the company's Chinese owner, ByteDance, divests itself from the United States within the next 12 months. Bobby Allyn, "President Biden signs law to ban TikTok nationwide unless it is sold", NPR, April 24, 2024; "Why the U.S. Is Forcing TikTok to Be Sold or Banned", The New York Times, April 26, 2024. This ban has been in the works for several years, and China has already made efforts to block the divestiture by prohibiting TikTok from transferring its technology to a foreign buyer without explicit permission from the Chinese government. *See* David E. Sanger, David McCabe, & Erin Griffith, "Oracle Chosen as TikTok's Tech Partner, as Microsoft's Bid Is Rejected", The New York Times (Sept. 13, 2020).

If the Chinese government continues to block the sale and the ban ensues, Americans and American companies will have to ask what happens when the server host permits you to access their computer per their terms of service, but the government—a third party to the relationship—does not.

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. §1030, is a federal anti-hacking law creating criminal and civil penalties. The law states"[w]hoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer" violates the CFAA. §1030(a)(2)(C). In cases like *United States v. John*, 597 F.3d 263 (5th Cir. 2010), *United States v. Nosal (Nosal I)*, 676 F.3d 854, 862 (9th Cir. 2012), *Facebook v. Power Ventures*, 844 F.3d 1058, 1067 (9th Cir. 2016), and *hiQ Labs v. LinkedIn*, 938 F.3d 985 (9th Cir. 2019), federal courts of appeal have split on what constitutes "unauthorized access," taking narrow and broad views.

Courtesy photos

**Aidan O'Connor, left, and Daniel Cohen, right, of Pashman Stein Walder Hayden.**

The reason for the split is that the term "authorization" is not defined in the statute, even though a person who accesses a protected computer (*i.e.*, virtually any computer connected to the internet per 18 U.S.C. §1030(e)(2)(B)) without authorization and thereby obtains or transmits certain protected information, or who exceeds their authorization to obtain any

information from a protected computer can be criminally punished.

CFAA, §1030(a)(1), prohibits the transfer of information "that has been determined by the United States Government pursuant to an executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations" to "any person not entitled to receive it," "to the advantage of any foreign nation."

More broadly, §1030(a)(2)(C) prohibits the obtaining of "information from any protected computer" without authorization or by exceeding authorized access. Per §1030(e)(6), "the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."

The issue of authorization was brought to the U.S. Supreme Court in *United States v. Van Buren*, 593 U.S. 374 (2021), with the parties arguing the broad and narrow views. Both views seemed to assume that authorization is given by the server host, or by the owner or controller of the computer being accessed—in *Van Buren*, an employer. The Supreme Court took the narrow view, protecting millions of Americans from criminal liability for using their work computers to surf the web. But this does not address the issue of legislative intervention.

This article asks: can the government restrict a user's authorization such that CFAA liability is created for accessing a computer that he/she is otherwise privately licensed to access? Unlike Facebook, for example, who writes terms of service agreements, blocks IP addresses and sends cease-and-desist letters to protect themselves from web scrapers or cyber attackers, the federal government's ban imposes a restriction on all American users for national security reasons wholly separate from the contract between server and user.

TikTok has been conditionally banned in the United States for national security reasons. "Congress is acting to prevent foreign adversaries from conducting espionage, surveillance, maligned operations, harming vulnerable Americans, our servicemen and women, and our U.S. government personnel." Bobby Allyn, "President Biden signs law to ban TikTok nationwide unless it is sold", supra (quoting Democratic Senator Maria Cantwell, Chair of the Senate Commerce Committee).

Emphasis should be placed on "espionage" and "surveillance" here; the government has determined that public use of the app poses a national security risk through the transmission of millions of Americans' personal data to a foreign entity and/or government. *See*, Executive Order 13873 (declaring a national emergency relating to "unrestricted acquisition or use in the United States of information and communications technology or services…supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries"); Executive Order 13942 (restating that use of Chinese mobile apps poses a national security risk and calling for restrictions on the use of TikTok in the United States).

Even under the narrow view of "authorization," it is still a CFAA violation to access a computer you do not have permission to access—whether by terms of service prohibition or employment restriction. A government ban prohibiting all access to TikTok servers could plausibly be a denial of authorization, even if it does not issue from the computer's owner, TikTok.

Through §1030(a)(2)(C), CFAA broadly prohibits obtaining information from a protected computer without authorization, or by exceeding authorized access. If the federal ban revokes or otherwise interferes with the private authorization granted by TikTok, there could be federal criminal liability for TikTok users. The suite of executive orders declaring a national security emergency regarding the use of TikTok and this new statutory ban could support an argument that information transmitted to TikTok through

use of the app is protected under § 1030(a)(1) as well, assuming that TikTok is considered "not entitled to receive" such information by virtue of the ban.

TikTok itself may also face criminal liability for accessing Americans' computers in the face of the ban; if the government revokes TikTok's authorization, then despite a user's agreement to terms of service, TikTok may violate the CFAA.

Supporters of finding a CFAA violation for a concurrent violation of a government ban on a website or app may point to prosecutorial discretion, as in *Van Buren*—the idea that prosecutors would not prosecute every TikTok user who violates the ban because some users' conduct may not be egregious enough to warrant prosecution. This argument should fail because individuals should not be at the mercy of prosecutorial discretion when assessing the risk of criminal liability, and because it is difficult to distinguish the harms to national security from two users' transactions with TikTok absent certain specific facts.

The ban raises several practical technological issues as well. Consider the role of an internet service provider (ISP) or use of a virtual private network (VPN). ISPs could be required to impose traffic filters to prevent users from accessing TikTok. *See* Executive Order 13942 (prohibiting content delivery network services enabling the functioning or optimization of the TikTok mobile application in the United States).

Users often circumvent limitations on content by using a VPN—for example, to watch content on Netflix that is not available in their region—and it may be possible for users to circumvent the ban on TikTok by using a VPN. These VPN users may be violating their platform's terms of service, copyright laws or other laws already, but they raise the question: what will VPN use look like in the United States if the government enforces the TikTok ban?

VPNs often issue no-logging policies—promises not to keep records of users' activities online—and must avoid operating in certain jurisdictions where laws require certain logs. Were a ban on TikTok imposed and enforced, a related bill could require VPN providers operating in the United States to preserve certain user data to support enforcement. *See* Daniel Markuson, "Are VPNs legal? Country guide for 2024", NordVPN, Jan. 8, 2024 (demonstrating restrictions on VPN use across the globe, including logging requirements).

Certain VPNs already avoid placing servers in the United States due to data-harvesting and data-sharing practices. Ieva Bulatovaité, "Can police track your VPN activity", Surfshark, Dec. 15, 2021 ("for example, a VPN provider can't claim to be no-logs if they're under the jurisdiction of the US or any other country with laws that require providers to keep user data"). Robust enforcement of a ban could severely restrict VPN operation and use in the United States.

The proposed ban on TikTok is intended to protect Americans from mass-collection of user data by a foreign government. However, it also brings the potential for Americans who access TikTok to violate an ambiguous and broad criminal statute, the CFAA. The statute's broad prohibitions on obtaining and transferring information contained in §§1030(a)(1) and (a)(2)(C) pose a serious risk of criminal liability for Americans and American companies in the face of this new TikTok ban.

**Aidan P. O'Connor** *is co-chair of Pashman Stein Walder Hayden's Criminal Defense Practice Group and a member of its Litigation Department.* **Daniel Cohen** *is an associate in the firm's Litigation and Appellate Advocacy and Corporate & Business Law practice groups.*