LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What Attorneys Should Consider Before Using TikTok

By **Anna Sanders**

Law360 (February 10, 2023, 4:34 PM EST) -- Trademark attorney Ana Juneja admits she knew little of the cybersecurity threats posed by TikTok in June 2021 when she used her own cellphone to upload her first video to the social media app, sharing tips on how to start a business.

The 41-second clip went viral — amassing more than 682,000 views — and the popularity of Juneja's content led her to quit intellectual property firm Dennemeyer & Associates and start her own law practice. Her videos have been viewed millions of times and prompted numerous client inquiries.

"So many people reached out to me that I realized that there's actually a mass amount of people on TikTok that need legal services," Juneja said. "Even if they could walk down the street to their local law firm, they don't do that. You have to meet people where they are."

However, while TikTok has helped lawyers like Juneja grow their practices, she said she's since hired a social media team to run her TikTok account and even deleted the app from all her devices.

"I don't think it's appropriate for most attorneys to have to TikTok on their work phone, or any phone with work emails," said Juneja, who now has some 142,400 followers on the social media platform. "When I started on TikTok, I had the app on my phone and I just filmed my own videos and uploaded them. I didn't really know that much about the security threats. Now I don't have the app on either of my phones anymore."

Attorneys and law firm staff must exercise extreme caution when using the app because of the risks associated with data collection and information sharing, according to cybersecurity experts. Without safeguards in place, the app could compromise attorneys, law firms and their clients.

"For the same reasons use of TikTok by government agencies is concerning, the unknown of TikTok's data-harvesting capabilities creates similar risk to law firms through use by attorneys and staff," Jessica Copeland, cybersecurity and data privacy practice chair at Bond Schoeneck & King PLLC, told Law360 in an email.

Many BigLaw firms and companies limit or outright prohibit lawyers and staff from using third-party applications like TikTok on work devices, Wi-Fi connections or systems, according to cybersecurity attorneys.

But the prevalence of home offices during the coronavirus pandemic has blurred the line between work

and play, with many attorneys and support staff using the same set of mobile devices for on and off hours. Plus, smaller law firms and solo practitioners may not have guidelines around app use.

Even if organizations ban TikTok at work, experts say using the app on personal devices is still risky for firm attorneys, in-house lawyers and other legal professionals.

"TikTok is known to collect significant amounts of data of its users' geolocation and internet activity," Copeland said. "It also may present risks to a firm's infrastructure by allowing access through its private network and vulnerability to email applications and document systems accessible through the same mobile device used for TikTok, potentially placing sensitive firm and client confidential information at risk."

Scrutiny of TikTok in the U.S. has mounted in recent months, with CEO Shou Zi Chew expected to face questions from a congressional panel in March over whether the Chinese company can safeguard American data from Beijing authorities. The app is already negotiating with the U.S. Department of the Treasury over how TikTok can continue American operations while addressing privacy and national security concerns.

Even so, several branches of the U.S. military, public universities and state governments have banned the app completely on their devices or Wi-Fi, with Texas following suit on Monday. In December, a measure prohibiting TikTok from government devices passed when it was added to Congress' year-end spending bill. The senior Republican on the Federal Communication Commission also called on Apple and Google to pull TikTok from smartphones.

Why Attorneys are Vulnerable

Experts say lawyers and other legal professionals are particularly vulnerable to security threats because they handle troves of sensitive information for American citizens and high-profile U.S. clients, companies and even government regulators.

"Cyber attackers (including in state-sponsored attacks) have increasingly targeted law firms for this reason," Anna Mercado Clark, leader of the data security, privacy, e-discovery and digital forensics practice teams at Phillips Lytle LLP, said in an email.

A Law360 Pulse analysis found that more law firms fell victim to data breaches in 2022 than in each of the prior two years. Public records showed 110 law firms reported data breaches to authorities across 17 states in 2022, exceeding the 88 breaches reported in 2021 and 46 in 2020. The 2020 data tracked the same pool of states, except for Illinois.

On Wednesday, Troutman Pepper was reportedly struck by a cyberattack.

Mercado Clark stressed that these attacks aren't "simply aiming to steal personal information that could be used to steal identities."

"Attackers are increasingly sophisticated, and can target corporate intelligence (such as about mergers) or intellectual property for financial advantage, redirect settlement payments, or target information about governments or government-related entities that are held by law firms," Mercado Clark said. "Attackers can either use this information to their own advantage or can encrypt this data or a law firm's network to disrupt or to demand ransom payments."

Mercado Clark said she couldn't comment on Phillips Lytle's own internal policies around TikTok, but that she personally doesn't use the app given these cybersecurity risks and other considerations.

The concerns over TikTok stem from what's shared by users on the app — and how the info in those videos could be used to breach accounts — as well as background data collected by the company.

"The ability for an app like that to track users, study habits, monitor behaviors, and record images, sound, and other data can be really powerful, especially when combined with personally identifiable information," Copeland said. "An entity could use that data at a micro level to understand the individual, but it could also use it at the macro level and study behaviors and trends."

Many law firms don't allow staff to have their personal emails linked with their network email account — a strategy that could be deployed when attorneys use TikTok, according to Claudia Rast, the cybersecurity group leader at Butzel Long PC and co-chair of the American Bar Association's Cybersecurity Legal Task Force.

"The best thing we can do from a law firm standpoint is say, 'We're not going to allow you to do that,'" Rast said.

At Butzel Long, the IT department and administrators must approve all third-party apps used on work devices and networks, according to Rast, who is on the firm's technology committee and would have to sign off on any requests to download TikTok.

"I would say no," Rast said.

Disquieting Data Collection

All social media applications amass scores of data on users and their habits, revealing everything from their personal preferences to whether they can be influenced into looking at something, buying a product or even adopting a political ideology. In the U.S., TikTok is viewed differently than other platforms because the app is owned by a Chinese company, ByteDance.

The app's roots in Beijing have prompted concerns over exactly where data on U.S. users is stored and processed and who within the company — or the Chinese government and Communist Party — has unfettered access to that information and what they might use it for.

TikTok has repeatedly denied that it shares U.S. data with the Chinese government or that the app takes orders from Beijing to censor content or tweak the algorithm shaping user experiences. Yet media reports last year continued to suggest that the Chinese government has "backdoor" access to nonpublic U.S. user data and that a China-based ByteDance team was planning to use TikTok to monitor the locations of American citizens.

In an attempt to appease the U.S. government, TikTok announced in June that the default storage location for American user data had been changed to servers controlled by the Silicon Valley tech company Oracle. But TikTok admitted the app would still use its own U.S. and Singapore data centers for backup.

The perception of TikTok's risk to U.S. users is at least partially driven by political considerations,

according to W. James Denvil, a Washington, D.C.-based partner at Hogan Lovells who counsels businesses on privacy and cybersecurity risks. He noted that many other companies collect data that could compromise a consumer's privacy and security.

"I would say this is a concern about China as opposed to a concern about TikTok," he said.

Sullivan & Cromwell LLP partner Nicole Friedlander said China "collects personal data for influence and intelligence operations to undermine the United States, and to facilitate its control of populations." Friedlander, who is also the co-head of the firm's cybersecurity practice, couldn't comment on whether the firm had any internal policies on TikTok.

"People sometimes ask why China would want to track, understand and be able to manipulate or hack young people, the predominant users of TikTok," Friedlander told Law360 in an email. "The answer is, young people grow up. Kids using TikTok today will be working in the industries and governments of tomorrow. China is well-known for playing the long game in this way."

FBI Director Christopher Wray told Congress in November that the FBI is concerned that China could leverage access to an app that's been downloaded on more than 2 billion devices to orchestrate a cyberattack or other malicious endeavor. And he warned lawmakers that China has already "stolen more Americans' personal and business data than every other nation combined."

"With TikTok, it doesn't have to steal," Friedlander said, noting that the app is "also a vehicle for China to engage in misinformation campaigns, which may be imperceptible to the viewer, but influence viewers' opinions and sow discord."

Giving Hackers What They Need

Beyond geopolitical considerations, experts say attorneys and law firm staff could put themselves, their employers and their clients directly at risk when they share videos on TikTok or other social media.

A video may inadvertently reveal names, addresses and other information about attorneys and clients that bad actors can exploit, like documents on a desk or computer screens in the background. TikTok videos can also tip someone off to an attorney's clientele based on where and when they share. So an attorney posting a seemingly innocuous video to TikTok can reveal enough information for a hacker to trick lawyers or law firm staff into clicking a nefarious link or downloading malware.

Hackers can gain access to systems, analytics, accounts or data through this so-called social engineering, a way of psychologically manipulating people to get sensitive information. Phishing is just one social engineering technique hackers use to get attorneys to click nefarious links, willfully transfer them funds or provide access to systems.

"One way China can target law firm users of TikTok is by leveraging personal data the app collects on them to craft a tailored, personal and effective phishing email," Friedlander said. "Once hackers have a foothold in the network, they work to move laterally until they find the sensitive information they have targeted."

Bad actors may also deploy data-mining algorithms or bots to process large amounts of information posted to TikTok and elsewhere to find targets for hackers — or to gather background on attorneys with access to certain clients and particular practice areas.

"Whenever you're dealing with social media — whether you're taking selfies or taking pictures of others — your audiovisual data, the photographs or videos you take, they might reveal client confidential information in the background, particularly when we're working from home," said Denvil of Hogan Lovells.

Hackers can use that information for everything from corporate espionage and blackmail to outright theft and even state-sponsored intelligence gathering.

"Law firms should — and many do — provide very particular guidelines because we are subject to professional obligations regarding confidentiality of information and are supposed to be fiduciaries for our clients' interests," Denvil said.

All attorneys and legal professionals have an ethical obligation to competently represent their clients, and some states require that they keep apprised of benefits and risks of technology as part of this duty. This year, New York became the first state to require continuing legal education in cybersecurity and data protection.

"Beyond cybersecurity concerns, there are professional concerns that should be considered when using TikTok or posting to other social media platforms, including what reflection certain posts may have on you as an attorney, professional or your law firm," Copeland noted. While she couldn't comment on whether Bond Schoeneck had any internal firm policies around TikTok, she said her concerns about the app outweigh any benefit in using the platform.

'A Great Tool'

Still, not every attorney feels the risks eclipse the app's advantages.

California attorney Mike Mandell said he began using TikTok in 2021 to "drum up business." With more than 7 million followers, Mandell now uses the platform as a "legal influencer" who educates the public about law.

"It's a great tool to market yourself," he told Law360 Pulse. "I've definitely gotten clients from it."

Mandell said he uses the app on a phone on which he also conducts business. But he added that it's important to keep private information on a more secure line and that attorneys should treat TikTok like they would any public forum where discussing client matters would be inappropriate.

"When it comes to confidential, private conversations, take the proper security measures," he said. "If you're going to meet up with your client, you wouldn't do it in a very public place and speak very loudly. Use your common sense."

Juneja said she hired a social media team to post on TikTok and interact with other users to safeguard against cybersecurity threats.

"I am very much conscious of confidentiality. I think I go a little bit overboard in that sense," she said. "My media team also knows to verify everything that's being uploaded."

How to Minimize, Not Eliminate, Risk

Experts say that attorneys who find the app helpful to their practice can minimize risk to themselves and their clients by limiting TikTok use to devices where no other work is conducted and using multifactor authentication on their accounts.

"Be mindful of what you're posting and be careful about who you're interacting with," Denvil said.

Denvil doesn't personally use TikTok. But he said Hogan Lovells has internal training and policies around the appropriate use and risks of various technologies and social media, both for law firm assets and personal devices. While TikTok is not explicitly banned, he said, the firm would likely issue more specific guidance should a particular security concern arise with TikTok or another app, such as one that allows unauthorized use or access to microphones, video or mobile locations without a user's permission.

Copeland suggested law firms and attorneys "look into controls that phone makers and operating systems place on their apps and determine if they are comfortable with trusting those measures."

"Effective cybersecurity measures help mitigate risk to an organization's network and data, but are less effective at mitigating the risk at the personal-device level, the kind of data that an app like TikTok might have access to," she said.

Attorneys downloading third-party applications "may knowingly or unknowingly be providing access to their contacts, camera, photos, microphone, geolocation, or other device information or internet activity," according to Mercado Clark of Phillips Lytle.

Butzel Long's Rast said attorneys can minimize this risk by seeking guidance from their firm's data protection team before downloading TikTok or other apps.

"I say 'minimize' because there is no absolute when we are discussing cybersecurity," she said.

Despite these risks, TikTok's reach can't be overstated. A 10-second video can be seen by millions.

"It's definitely very important to consider security concerns — it should be one of the top things you consider because it goes to really the ethics of being an attorney and protecting your clients," Juneja said. "On the flip side, TikTok is really good marketing for people who do know how to use that type of content."

--Additional reporting by Ben Kochman, Christopher Cole, Madeline Lyskawa, Xiumei Dong and Steven Lerner. Editing by Alanna Weissman and Marygrace Anderson.
