Guidepost

FORGET SPY BALLOONS – THE BIGGER THREAT IS TIKTOK

After the downing of the Chinese spy balloon by U.S. Forces in early February 2023, several additional objects have been identified over U.S. and Canadian airspace. While officials have denied that these were additional spy balloons, many have questioned what information was collected by these aerial spy devices, and for what purposes. Even though this is significant to national security, most citizens aren't personally worried about this breach of privacy.

We suggest that an even greater threat to the average citizen is social media apps, specifically TikTok. Several articles have recently been published discussing the security threats of TikTok, in *Forbes*, *USAToday*, and *Wired*. In fact, recent legislation to ban TikTok across the United States has been put forth in the creatively named: Averting the National Threat of Internet Surveillance, Oppressive Censorship and Influence, and Algorithmic Learning by the Chinese Communist Party (ANTI-SOCIAL CCP) Act.

Bloomberg Law reports "more than two dozen states have taken action to remove and block the app—owned by Beijing-based ByteDance Ltd.—from government devices and networks over concerns about data access by the Chinese government." When state governments are banning use of the app, this begs the question: why? Recent class action lawsuits allege "that its in-app browser illegally tracks users' clicks and keystrokes in violation of a federal wiretap law…TikTok could become privy to private information such as a user's credit card accounts, mental health, or sexual preferences."

While several U.S. states have taken action to ban the use of TikTok, Canada's position was initially less direct. In or around December 2022, Conservative MP Michael Chong called for an investigation into TikTok, stating that the app can manipulate algorithms for foreign influence operations, and given its global reach, TikTok could present a national security threat.

On February 23, 2023, *Global News* reported that Canada's federal privacy commissioner alongside several provinces, launched a joint investigation into TikTok, to determine whether "meaningful consent is being obtained for the collection, use and disclosure of personal information" Just five days later, the Canadian federal government removed and blocked TikTok from all federal government-issued devices. A government spokesman stated that the app

"presents an unacceptable level of risk to privacy and security." Canadian provinces and several municipalities have since enacted similar policies.

The collection and use of data is certainly concerning, but so too is what users are uploading, without regard to privacy. We have conducted digital vulnerability assessments for many clients, and a consistent area of focus in our reports includes reviews of TikTok accounts of the clients' children. In most instances, privacy settings are not utilized, and videos are easily accessible online for anyone to review. Kids and teens post videos from inside their homes, discuss upcoming vacations or trips, share lamentations over parents, highlight favorite places to visit, and flaunt their family's wealth – all neatly organized on a single website and updated as often as the user posts.

Experts on digital surveillance and Chinese interference have concerns that the app could provide Beijing with a gold-mine of data on individuals and groups in the West. They fear the app could be used as a tool to manipulate public thinking, by delivering misinformation onto TikTok, or censoring material. Further, experts worry that TikTok could use hidden software tools to pry into other mobile apps to collect yet more information.

Social media is a common means of communication and sharing in today's society; however, oversharing in the digital world poses many risks to our privacy, safety, and physical security.

Consider the following protective measures when utilizing social media:

1. **Review Privacy Policies:**

Review the privacy policies of social media platforms and apps prior to joining and understand what information the organization is collecting, where the information is stored and how it is being used, and whether the information is being disclosed to a third-party.

2. **Customize Your Privacy Settings:**

Select the most restrictive security setting available and do not share any personal information, such as phone numbers, addresses, current location, birthdays etc. Ensure to review your privacy setting regularly as social media sites are consistently updating their settings.

3. **Manage Your Usernames and Passwords:**

Consider the use of a pseudonym instead of your legal name. Use strong and unique passwords that are at least twelve characters in length and contain upper and lowercase letters, numbers, and/or symbols. Consider utilizing a multi-factor authentication if available. Delete data and close unused accounts; data may remain on the organizer's server if an account is simply deactivated.

4. **Avoid Oversharing and Limit What Information to Share:**

Do not share information that identifies your location and do not disclose personal details. Sharing personal

information can leave you vulnerable to threats, including identity fraud and theft. Additionally, consider what other users, including friends and family share about.

The TikTok issue is not an outlier, and the Facebook-Cambridge Analytica scandal reminds us that although privacy settings are important, they are not a silver bullet for privacy protection. Information posted on digital platforms can persist in various places and leave a permanent footprint that can be difficult if not impossible to remove. Prior to sharing information on social media sites/apps, consider the risks to your data privacy, personal safety, physical security, and reputation.

Mandy Yousif

Mandy Yousif is the chief operating officer of Specialty Risk & Intelligence Services Inc., overseeing all operational aspects of the company. She has several years of experience conducting investigation, compliance intelligence and risk assessment consultation.

CODY SHULTZ PCI, CCI

Director, Investigations + Private Client Protection

Cody Shultz serves as a director of investigations and private client protection for Guidepost Solutions and is based in the D.C. office. Having served with the Central Intelligence Agency, he is now sought out as an expert on reputation and identity management for ultra-high net worth clients and family offices. He holds a Professional Certified Investigator certification through ASIS International and is a Certified Cryptocurrency Investigator.