

Introducing
Dynamics 365 Copilot

Infuse your ERP and CRM with AI

SPONSORED BY MICROSOFT

Get AI-powered assistance across business functions.

LEARN MORE

It's Time to Get Real About TikTok's Risks

US lawmakers keep warning about the popular app. But until they can explain what makes it uniquely dangerous, it's difficult to tailor a resolution.

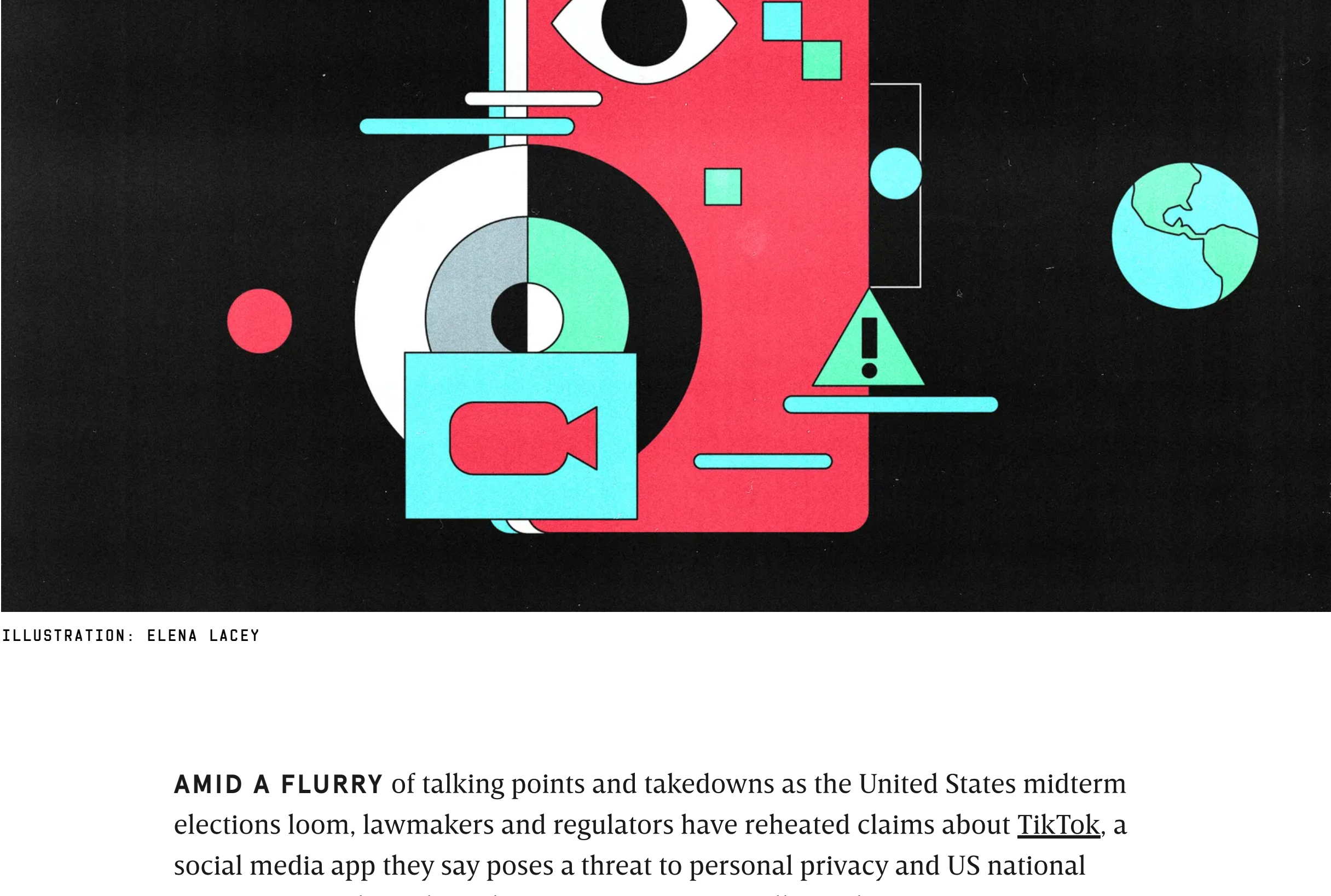


ILLUSTRATION: ELENA LACEY

AMID A FLURRY of talking points and takedowns as the United States midterm elections loom, lawmakers and regulators have reheated claims about [TikTok](#), a social media app they say poses a threat to personal privacy and US national security. Now, the Biden administration is reportedly readying its own action. But the exact scope of the problem and goals remain fuzzy. Owned by the Chinese tech giant Bytedance, TikTok has [more than a billion](#) users, including an [estimated](#) 135 million in the US, and some lawmakers, including former president Donald Trump, have warned over the past two years that the Chinese government could use the app to collect data on Americans or launch influence operations through the platform.

WIRED SECURITY

It's Time to Get Real About TikTok's Risks

00:00

10:02

Spotify

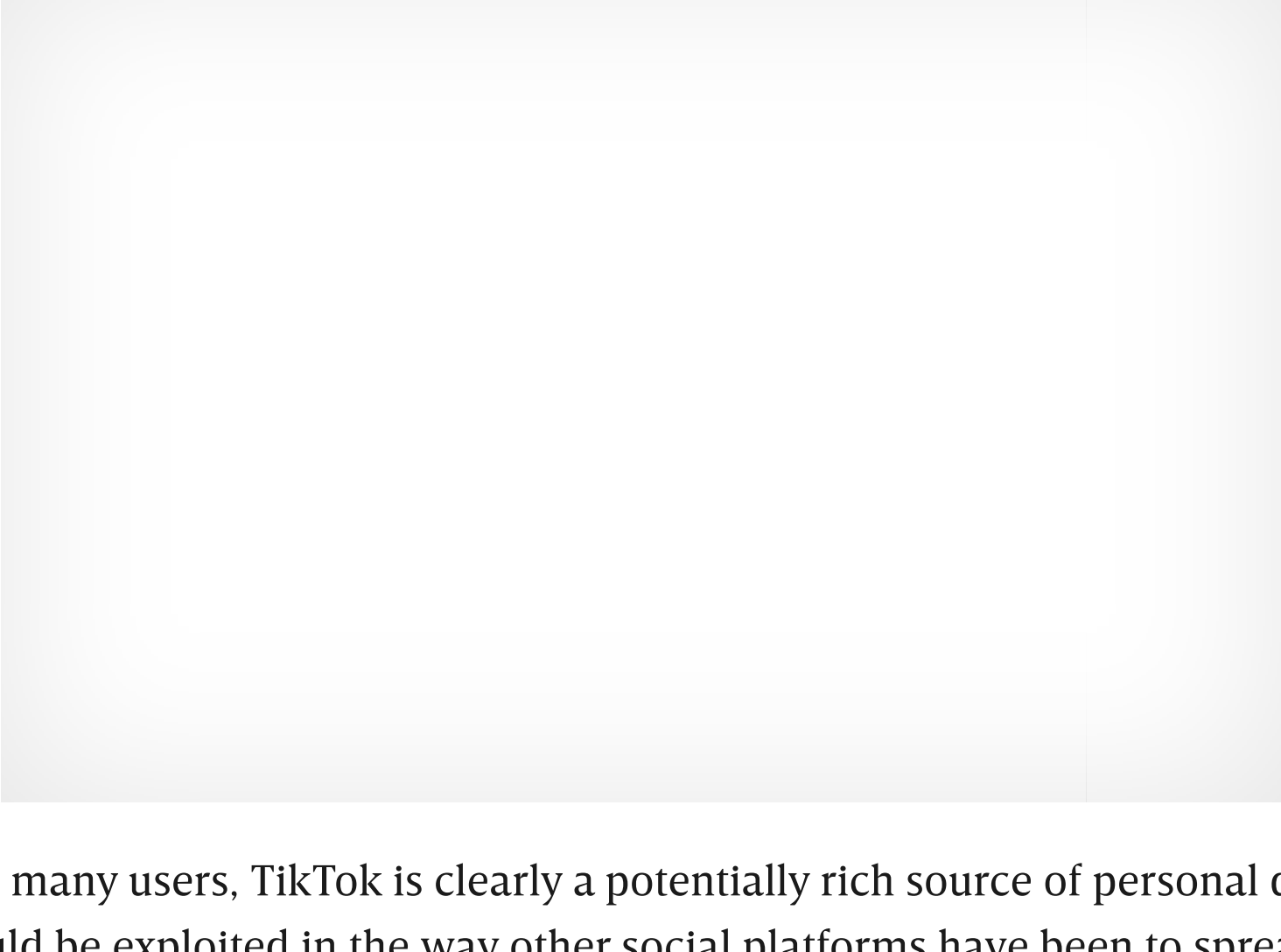
YouTube

Apple

Amazon

Google

The US military banned its members from using TikTok on government devices or at all in late 2019 and early 2020, as did the Transportation Security Administration and some other federal agencies. Just last month, the chief administrative officer for the US House of Representatives [warned lawmakers](#) against installing TikTok due to the data it can collect. This followed a June 17 [BuzzFeed News report](#), which found that ByteDance employees can and do gain access to US TikTok users' data in some situations. But for the general public, warnings from legislators and regulators this summer have continued to be vague and amorphous, underscoring broader ambiguity about where lawmakers' precise concerns lie.



With so many users, TikTok is clearly a potentially rich source of personal data and could be exploited in the way other social platforms have been to spread disinformation or promote influence operations. But the reason TikTok has been singled out is less clear. Huge quantities of sensitive data about people living in the US are already available in various forms for purchase or the taking through other public social media platforms, the digital marketing industry, data brokers, and leaked stolen data troves. And long before the rise of TikTok, China was already notorious on the global stage for stealing massive quantities of data about Americans and others from governments and companies around the world. So, is it protectionism? Xenophobia? Special insight into US national security?

A report [published by Senafor](#) on Friday indicates that the Biden administration is preparing a series of executive orders to address TikTok and the Chinese tech sector's access to Americans' data more broadly. The report says the White House's actions could significantly curtail US investment in China, while other potential measures may limit what technology can be sold to Chinese clients and specifically limit the data Chinese tech companies can collect about US citizens.

Such steps would be less dramatic than the approach to TikTok taken by Biden's predecessor but would have a larger scope and wider set of potential ramifications. In the waning months of the Trump administration, the White House [attempted to block TikTok from US app stores](#) if ByteDance didn't sell the company to a US-based firm. Though the move failed, TikTok took steps to silo itself from its Chinese owners and announced in June that all US user traffic would be routed in the US. The company is still working on deleting all user data from its own servers in favor of processing everything in Oracle's cloud. The company stores data backups in the US and Singapore.

"The thing about TikTok is that a lot of people use it!" says Rui Zhong, a researcher at the Kissinger Institute on China and the United States. "The Trump administration also tried to ban WeChat, which is not just a communication platform but a technology platform that vacuums up reams of your data—more so than TikTok. But WeChat is almost exclusively used in the US by the Chinese diaspora, whereas TikTok is just broadly popular with Americans."

She adds that while, from a US national security perspective, the existential threats are worth acknowledging, there wasn't enough information available about concrete concerns when the TikTok ban was on the table a couple of years ago or in remarks this summer. US officials still don't seem, at least publicly, to have a smoking gun illustrating the urgency of the threat. "It needed a better case built around it, and at the time in 2019 they just didn't seem to have that case," Zhong says. "Whether they will have something they can show Americans in the future or not, I can't say."

(Ad)

ADVERTISEMENT

All Access. \$1.50/week.

The New York Times

On June 24, days after the BuzzFeed report, a group of Republican senators led by Tom Cotton of Arkansas [sent a letter](#) to Treasury Secretary Janet Yellen "to inquire about the Biden administration's delayed response to the national security and privacy risks posed by TikTok." On June 28, a different group of nine Republican senators [sent a letter](#) to TikTok's CEO, Shou Zi Chew, laying out questions about the company's data management practices and relationship with ByteDance given that the company has always maintained that they will not share US user data with the Chinese government. On July 5, a bipartisan duo from the Senate Select Committee on Intelligence—democrat Mark Warner of Virginia and Republican Marco Rubio of Florida—[sent a letter](#) to the Federal Trade Commission urging the agency to investigate TikTok and ByteDance for "repeated misrepresentations by TikTok concerning its data security, data processing, and corporate governance practices."

In a series of responses this summer both [to lawmakers](#) and [the public](#), TikTok has staunchly maintained that it does not and would never share US user data with the Chinese government, and that it is a separate US-based entity subject to US laws. The company does not report publicly on [government data requests](#), but it does publish a twice-annual report about [government requests to remove content](#) from the service. The latter report indicates that the company has never fulfilled a removal request from China.

The bottom line, though, is that TikTok is owned by ByteDance. And some ByteDance employees can access TikTok user data. Does that mean the ruling Chinese Communist Party (CCP) can get that data too? In his June 30 response to the nine Republican senators, TikTok's Chew said, "Employees outside the US, including China-based employees, can have access to TikTok US user data subject to a series of robust cybersecurity controls and authorization approval protocols overseen by our US-based security team." He described at length the layers of classification and restriction that protect user data from being accessed casually or without oversight. Chew and TikTok have long maintained that it they "have not provided US user data to the CCP, nor would we if asked." When WIRED asked TikTok how this squares with the reality that ByteDance has access and could be compelled to exercise it under Chinese law, spokesperson Maureen Shanahan said, "TikTok is provided in the United States by TikTok Inc., which is incorporated in California and subject to US laws and regulations."

Still, it is unclear whether TikTok poses a unique and specific threat to US national security or if it is simply a convenient proxy through which lawmakers are grappling with larger issues of data security and privacy, disinformation, content moderation, and influence in a globalized tech market. Similarly, the Chinese telecom giant Huawei faced controversy over whether the US should incorporate [Chinese-made hardware into domestic 5G infrastructure](#), which was ultimately banned.

"There are definitely signs that Chinese influence efforts are likely to grow, linked to the Chinese government's strategy more broadly of digital authoritarianism," says Kian Vesteinsson, a research analyst for the nonprofit digital rights think tank Freedom House. "But it's important for us to acknowledge that the US government has its own shadowy national security surveillance authorities. And in recent years, US government agencies have monitored social media accounts of people coordinating protests in the US and done things like searched electronic devices throughout the country and at the border. These sorts of tactics undermine the idea that this is only a foreign threat."

Then there's the power imbalance TikTok may create. One thing about TikTok, in particular, is that its popularity and proliferation within the US could make it a one-stop shop for the Chinese government to mine the data of US users and launch influence operations in the US. Meanwhile, the US government may feel that it lacks a comparable mechanism through which it can so directly pull Chinese user data and work to sway public opinion in China.

See What's Next in Tech With the Fast Forward Newsletter

A weekly dispatch from the future by Will Knight, exploring AI advances and other technology set to change our lives. Delivered every Thursday.

Your email

Enter your email

SUBMIT

By signing up you agree to our [User Agreement](#) (including the [class action waiver and arbitration provisions](#)), our [Privacy Policy](#) & [Cookie Statement](#) and to receive marketing and account-related emails from WIRED. You can unsubscribe at any time.

"Let's assume for a second that US intelligence has access to WeChat. They would have to fight hard for that access, and it would constantly be at risk of discovery and neutralization. China, on the other hand, doesn't have to fight for access to TikTok: they have it by statutory authority," says Jake Williams, director of cyber-threat intelligence at the security firm Scythe and a former National Security Agency hacker. "By itself, I don't think that the TikTok app on people's devices is a significant threat, but the potential for Chinese data collection across the platform is a larger concern, especially when combined with other data already acquired by Chinese state actors."

Given its immense popularity, its ownership, and the fact that the bulk of TikTok activity is public by nature, there is no clear technical solution to boxing China out of the service. The question is whether the US government wants to devise a business solution or incentivize development of an appealing alternative platform. Still, privacy violations, security concerns, and foreign influence operations against US residents through social media are problems the US government has yet to solve. And neither technology bans nor countersurveillance will make them go away.

"One thing that we really should escalate here is that the US should be leading by example," Freedom House's Vesteinsson says. "When we talk about expanding the US government's surveillance powers, that sets a really bad example for governments around the world."

Get More From WIRED

- Get the best stories from [WIRED's iconic archive](#) in your inbox
- Our new [podcast](#) wants you to [Have a Nice Future](#)
- My balls-out quest to achieve [the perfect scrotum](#)
- [Please recycle this building](#) when not in use
- How the plane helped me [fall back in love with tech](#)
- [An ominous heating event](#) is unfolding in the oceans
- "Everybody's so creative!" and the [rise of recipe reactions](#)
- Embrace the new season with the Gear team's best picks for best [tents](#), [umbrellas](#), and [robot vacuums](#)

Lilly Hay Newman

A senior writer at WIRED focused on information security, digital privacy, and hacking. She previously worked as a technology reporter at Slate magazine and was the staff writer for Future Tense, a publication and project of Slate, the New America Foundation, and Arizona State University. Additionally... [Read more](#)

SENIOR WRITER

TOPICS

CHINA

SURVEILLANCE

PRIVACY

SECURITY

TIKTOK

MORE FROM WIRED

Chinese Cops Ran Troll Farm and Secret NY Police Station, US Says

Three criminal cases detail China's alleged attempts to extend its security forces' influence online—and around the globe.

ANDY GREENBERG

The High-Stakes Scramble to Stop Classified Leaks

All tools? A porn filter, but for Top Secret documents? Just classifying less stuff? US lawmakers are full of ideas but lack a silver bullet.

MATT LASLO

Leaked Pentagon Documents May Herald a New Era of Revelations

The bizarre release of sensitive US government materials soon after their creation signals a potential shift to near-real-time unauthorized disclosures.

LILLY HAY NEWMAN

Popular Chinese Shopping App Pinduoduo Is Laced With Malware

Plus: 119 arrested during a sting on the Genesis dark-web market, the IRS aims to buy an online mass surveillance tool, and more.

LILLY HAY NEWMAN

Security Roundup: Leak of Top-Secret US Intel Risks a New Wave of Mass...

Plus: Hackers claim to have stolen 10 TB from Western Digital, a new spyware has emerged, and WhatsApp gets a fresh security feature.

DHIRVY NEHRTRA

Montana's Looming TikTok Ban Is a Dangerous Tipping Point

The state is poised to be the first in the US to block downloads of the popular app, which could ignite a precarious chain reaction for digital rights.

LILLY HAY NEWMAN

Cops Just Revealed a Record-Breaking Dark Web Dragnet

Operation Specter likely drew on leads from multiple dark web market busts, including the secret takedown of Monopoly Market in 2021.

ANDY GREENBERG

LinkedIn Will Finally Offer Ways to Verify Your Job

To beat back fake accounts, the professional social network is rolling out new tools to prove you work where you say you do and are who you say you are.

LILLY HAY NEWMAN