Case No. 24-34

In the

United States Court of Appeals

for the

Ninth Circuit

SAMANTHA ALARIO; HEATHER DIROCCO; CARLY ANN GODDARD; ALICE HELD; DALE STOUT; TIKTOK INC.,
Plaintiffs-Appellees,

v.

AUSTIN KNUDSEN,
in his official capacity as Attorney General of the State of Montana,
Defendant-Appellant.

Appeal from the United States District Court for the District of Montana (Missoula)
Case Nos. 9:23-cv-00056-DWM and 9:23-cv-00061-DWM
The Honorable Donald W. Molloy, District Judge

BRIEF OF DIGITAL PROGRESS INSTITUTE AS *AMICUS CURIAE* SUPPORTING APPELLANT AND REVERSAL

JOEL L. THAYER
THAYER, P.L.L.C.
1255 Union Street NE, 7th Floor
Washington, D.C. 20002
Telephone: (760) 668-0934
jthayer@thayer.tech

Attorney for Amicus Curiae,
Digital Progress Institute

COUNSEL PRESS · (213) 680-2300 PRINTED ON RECYCLED PAPER

CORPORATE DISCLOSURE STATEMENT

Pursuant to Local Rule 7.5(b)(2)(B), *Amicus Curiae* Digital Progress Institute ("Institute") files this Corporate Disclosure Statement, which complies with the requirements of Federal Rule of Civil Procedure 7.1.

The Institute hereby discloses that it is a 50l(c)(4) District of Columbia organization, and has no parent corporation, nor does any publicly held corporation own 10% or more of its stock.

Dated: March 8, 2024

Respectfully submitted,

/s/ Joel L. Thayer
Joel L. Thayer
Thayer, PLLC
1255 Union Street, 7th Floor
Washington, D.C. 20002
Telephone: (760) 668-0934
Email: JThayer@thayer.tech

Attorney for Amicus Curiae,
Digital Progress Institute

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES **Page(s)**

RULES

OTHER AUTHORITIES

IDENTITY AND INTEREST OF *AMICUS CURIAE*

The Digital Progress Institute ("Institute") is a thought leader in the intersection between constitutional fidelity and Internet regulation. Its core mission is to advocate for incremental and bipartisan policies and laws in the technology and telecommunications spaces that promote a holistic approach to Internet regulation and ensure privacy for every consumer. Preventing TikTok from engaging in espionage on behalf of the Chinese government is fundamental to these stated principles.

The Institute believes that Montana's law at issue meets all of the Institute's metrics of good governance. Montana's law is not only incremental in scope and bipartisan, but it also takes a holistic approach to Internet regulation when addressing cybersecurity and is critical to the promise of privacy for all. Again, these are two foundational principles on which the Institute was built, which further informs the Institute's interest in participating as an *amicus* in this case.

DISCLOSURES

Pursuant to Federal Circuit Rule 29(c)(5), no party's counsel authored the brief in whole or in part, no party or party's counsel contributed money that was intended to fund preparing or submitting the brief, and no person other than amicus or their counsel contributed money that was intended to fund preparing or submitting the brief. All parties consent to the filing of this Brief.

INTRODUCTION AND SUMMARY OF ARGUMENT

The information wars are upon us and our enemies are leveraging our technology to get the upper hand. If this Court rules in favor of TikTok, it would open the door for known corporate affiliates of the Chinese government—like Huawei, ByteDance, and ZTE—or Russian technology companies to weaponize our Constitution to spy on our population. Because Congress and the several States must have the ability to protect the American people, reversing the District Court's decision on TikTok's Motion for Preliminary Injunction is in the public interest.

Here, the Institute explains that the First Amendment does not shield TikTok from public scrutiny and legislation. Montana's law is targeted towards TikTok's conduct, not its or its users' speech. Courts frequently uphold the constitutionality of statutes that ban the operation of communications platforms, like TikTok, to protect Americans against foreign adversaries—especially so when there are numerous alternative options.

If this Court upholds the District Court's ruling, it would create an extraordinary cybersecurity loophole. By extension, such a ruling would create a roadmap for foreign enemies to use when they seek to pilfer sensitive consumer data from our population. Worse, it would create a significant roadblock for the federal Congress to write bipartisan legislation to prohibit this type of foreign spying nationally.

Our constitutional fidelity and shared goal of preventing foreign adversaries' peering eyes into our homes, our thoughts, and our everyday lives depend on the Court getting this right.

BACKGROUND

TikTok is an online platform that enables users to share and view videos and other forms of content. So is Facebook. And Instagram. And Twitter. And Snapchat. And YouTube. And Pinterest. And LinkedIn. And Tumblr. And WhatsApp. And Foursquare. And Reddit. And Rumble. And Discord. And Signal. And Mastodon.

Tens of thousands, if not millions, of Americans use each of these platforms every month. On them all, users express their opinions and communicate with others about a wide range of social, political, and business issues. And each platform claims to have safeguards to protect the privacy and security of U.S. user data.

Concerned that these platforms were not in fact protecting the privacy and security of Montanans' data, the Montana legislature in 2023 passed and the Governor signed two bipartisan laws. The first, S.B. 384, also known as the Montana Data Privacy Act, regulates the security and privacy practices of companies that "control or process the personal data of not less than 50,000 consumers" with some limited exceptions and additions. The second, S.B. 419, targets one particular

company—TikTok—and bans its operations in Montana so long as it remains owned by ByteDance, a Chinese corporation. S.B. 419 § 1, 4.

The legislature was clear with why it targeted TikTok and TikTok alone in S.B. 419. "People's Republic of China exercises control and oversight over ByteDance, like other Chinese corporations, and can direct the company to share user information, including real-time physical locations of users." S.B. 419 Preamble. In turn, "TikTok gathers significant information from its users, accessing data against their will to share with the People's Republic of China." *Id.* That's because "the People's Republic of China is an adversary of the United States and Montana and has an interest in gathering information about Montanans, Montana companies, and the intellectual property of users to engage in corporate and international espionage." *Id.*

ARGUMENT

I. TikTok Is A Tool of Foreign Espionage for the Chinese Government

Of the more than a dozen social media platforms targeted by the Montana legislature in S.B. 384 and S.B 419, only one has been repeatedly caught endangering the security of the United States and the State of Montana—and only one is owned by the Chinese company ByteDance.

Federal Bureau of Investigation Director Christopher Wray, for example, has warned that TikTok "is a tool that is ultimately within the control of the Chinese

government—and it, to me, screams out with national security concerns." Michael Martina & Patricia Zengerle, *FBI chief says TikTok 'screams' of US national security concerns*, REUTERS (Mar. 9, 2023), https://bit.ly/45jtX3z. President Biden's Director of National Intelligence Avril Haines has said that China uses apps (like TikTok) and communication networks to "develop[] frameworks for collecting foreign data and pulling it in . . . to target audiences for information campaigns or for other things." Andrea Mitchell Report, *DNI Avril Haines: Parents 'should be' concerned about kids' privacy and data on Tik-Tok*, MSNBC (Dec. 5, 2022), https://on.msnbc.com/3OWZn97.

These concerns are in large part due to the intimate relationship between the Chinese government and large Chinese companies like ByteDance. To align with Beijing's policies, ByteDance has had an internal party committee as part of its governance structure since 2017. Yaqiu Wang, *Targeting TikTok's privacy alone misses a larger issue: Chinese state control*, HUMAN RIGHTS WATCH (Jan. 24, 2020), https://bit.ly/3EgQXEA. In 2018, ByteDance took down an app called Neihan Duanzi because, in the words of ByteDance's founder, it was incompatible with "core socialist values." Li Yuan, *TikTok Blazes New Gound. That Could Doom It.*, THE NEW YORK TIMES (Nov. 5, 2019), https://shorturl.at/efqJQ. In 2019, ByteDance agreed to promote the credibility of Chinese police for the Chinese Ministry of Public Security's Press and Propaganda Bureau. Australia Strategic Policy

Initiative, *Mapping China's Tech Giants: ByteDance* (Mar. 8, 2024), https://shorturl.at/pzFP7. And TikTok CEO Shou Zi Chew served as ByteDance's CFO for most of 2021 and before that was president of international operations for Xiaomi Technology, a software developer the Pentagon considers a "Communist Chinese military company." Jerry Dunleavy, *TikTok CEO's Chinese government ties in spotlight ahead of Capitol Hill testimony*, WASHINGTON EXAMINER (Mar. 23, 2023), https://bit.ly/44ovQuA.

Given this background, it should be no surprise that TikTok has been found to violate American privacy laws before. In 2019, for example, TikTok entered into a consent decree with the Federal Trade Commission for violating the Children's Online Privacy Protection Act paying $5.7 million—a record fine. Federal Trade Commission, *Video Social Networking App Musical.ly [now TikTok] Agrees to Settle FTC Allegations That it Violated Children's Privacy Law* (Feb. 27, 2019), https://shorturl.at/huILP. Not a year later, the Federal Trade Commission received a complaint that TikTok was already violating that consent decree. Campaign for a Commercial-Free Childhood et al., *Complaint and Request for Investigation of TikTok for Violations of the Children's Online Privacy Protection Act and Implementing Rule* (May 14, 2020), https://shorturl.at/bnzUZ. In 2022, TikTok settled a class-action lawsuit for $92 million for violating Illinois privacy law. *In re TikTok, Inc. Consumer Privacy Litigation*, MDL No. 2948, Memorandum Opinion

and Order (July 28, 2022), https://shorturl.at/jlmwY. And in early 2023, fifteen separate lawsuits alleged that TikTok illegally tracked its users in violation of the Federal Wiretap Act. Cyrus Farivar, *TikTok's In-App Browser Monitoring Violates Wiretap Law, Slew of Lawsuits Claim*, FORBES (Mar. 3, 2023), https://shorturl.at/epqtJ. That same year, a group of 46 state attorneys generals complained that TikTok had failed to preserve subpoenaed evidence and refused to produce that evidence in a readable format in a lawsuit regarding TikTok's compliance with privacy and consumer protection laws. *In re Investigation of TikTok, Inc.*, Brief of Amici Curiae The Colorado Department of Law and 45 Other States in Common Interest (Mar. 6, 2023), https://shorturl.at/exDP5.

What is more, TikTok's promises of protecting the privacy and security of American data from China's hands have proven hollow. Leaked audio from internal TikTok meetings shows that, at least through January 2022, engineers in China had access to U.S. data. Emily Baker-White, *Leaked Audio from 80 Internal TikTok Meetings Shows that US User Data Has Been Repeatedly Accessed From China*, BUZZFEEDNEWS (June 17, 2022), https://bit.ly/3QXXf3n. "Everything is seen in China," said one member of TikTok's Trust and Safety team. *Id.* And eight different U.S. employees explained having to repeatedly turn to Chinese colleagues because U.S. staff "did not have permission or knowledge of how to access the data on their own." *Id.*

Meanwhile, TikTok's parent ByteDance has admitted to tracking at least two U.S.-based journalists via TikTok, Clare Duffy, *TikTok confirms that journalists data was accessed by employees of its parent company*, CNN (Dec. 22, 2022), https://cnn.it/3KYVYFB, and reports show that ByteDance had in fact intended to use TikTok to monitor specific American citizens. Emily Baker-White, *TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens*, FORBES (Oct. 20, 2022), https://bit.ly/44sSvWw. The U.S. Department of Justice is investigating this spying. Alexander Mallin & Luke Barr, *DOJ investigating TikTok owners for possible surveillance of US journalists: Sources*, ABC NEWS (Mar. 17, 2023), https://abcn.ws/47Pr2Bm.

In short, TikTok and its owner ByteDance have a history of violating American privacy and security laws, tracking individual American users that would be of interest to the Chinese government, and transmitting that data to ByteDance in China. Given this history of misconduct, the Montana legislature adjudged that its generalized privacy law—S.B. 384—would insufficiently deter further espionage by TikTok against the citizens of Montana and adopted S.B. 419 to ban TikTok (and hence ByteDance's) operations in the state unless ByteDance divested itself of its ownership of TikTok.

II. The First Amendment Does Not Bar Conduct-Based Regulation Designed to Protect the Security Interests of Citizens of the United States and the Several States

Montana's S.B. 419 regulates conduct, not speech. It prohibits one of a more than a dozen social-media networking apps from "operat[ing] within the territorial jurisdiction of Montana." S.B. 419 § 1. It does not prohibit TikTok from speaking. It does not prohibit TikTok from publishing its views. And it does not prohibit TikTok from disseminating its views through one of the more than a dozen social-media networking apps or the literally thousands of websites that will remain available in Montana after S.B. 419 takes effect (notably, TikTok has public profiles on every major social media platform where it shares its users' content, *see*, *e.g.*, TikTok Page, Facebook, https://www.facebook.com/tiktok). Nor does the law prohibit TikTok's current users from doing any of these things. And to make that point even more clear, S.B. 419 exempts any users from being penalized if they continue to use TikTok after the prohibition takes effect.

In a similar vein, the law does not regulate the content of the TikTok platform or the content it hosts. Montana's law treats all content the same and does not favor any user content over another. Montana's law does not prevent users from posting the same content on any other social media platform; users are still free to do so after the law goes into effect. The law brooks no exception for certain types of favored

speech nor harsher treatment for disfavored speech—nor for any favored or disfavored speaker. S.B. 419 draws no such distinctions at all.

Indeed, the only distinction found in the law is the one drawing a line between TikTok on the one hand and other social-media networking platforms on the other—and the legislation makes clear why that line has been drawn: to protect the security of Montanans from the conduct of TikTok's owner, ByteDance.

The factual predicate of that distinction is clear; as shown in numerous articles, the legislative history, and the substance of the legislation itself, the threat that ByteDance's control of TikTok poses to the security and privacy interests of Montanans (and all Americans) is undeniable. The Montana legislature has a compelling interest in protecting the security and privacy of its citizens. And the legislature exercised that prerogative by regulating the conduct of TikTok, not its speech, and carved out a path forward for TikTok to ameliorate the legislature's concerns: The law makes clear that TikTok can operate in the state of Montana (with all of the same content as before) if it cuts ties with ByteDance. S.B. 419 § 4.

The First Amendment poses no bar to such regulation. Courts have consistently distinguished between conduct and speech in applying the First Amendment. In *Arcara v. Cloud Books, Inc.*, for example, the New York state government shut down an adult bookstore for health violations because its owner used his store to facilitate prostitution. 478 U.S. 697 (1986). Even though we think

of a bookstore as a quintessential venue for First Amendment activity, the Supreme Court ruled that the First Amendment did not prevent the government from shutting down the bookstore because the government was acting based on the owner's decision to engage in prohibited, non-speech conduct. *Id.* at 707.

As Justice Burger explained:

> The legislation providing the closure sanction was directed at unlawful conduct having nothing to do with books or other expressive activity. Bookselling in an establishment used for prostitution does not confer First Amendment coverage to defeat a valid statute aimed at penalizing and terminating illegal uses of premises. *Id*.

So too here. It's clear Montana's legislature is targeting TikTok's conduct. Specifically, the law takes issues with TikTok's "stealing of information and data from users" to share with ByteDance and the Chinese government, "corporate and international espionage in Montana," and "to track the real-time locations of public officials, journalists, and other individuals." S.B. 419 Preamble. Montana's legislature makes this intent even clearer through S.B. 419's "Contingent voidness" provision that "voids [the law] if TikTok is acquired by or sold to a company that is not incorporated in any other country designated as a foreign adversary . . . ." S.B. 419 § 4.

Notably, Montana is not the first to take action against a Chinese-based communications platform. For example, Congress passed the Secure and Trusted Communications Network Act of 2019, which directed the Federal Communications

Commission to remove equipment associated with national security threats from American networks. Pub. Law No. 116-124. Accordingly, the Commission relied on the views of national security experts and banned Huawei from selling any more telecommunications equipment to rural customers that rely on federal subsidies. In a similar vein, the Commission has revoked the ability of Chinese-affiliated carriers China Telecom, ComNet, and Pacific Networks from interconnecting with American telecommunications networks and operating as telecommunications carriers in the United States.

The courts have blessed these prohibitions. The Fifth Circuit turned aside Huawei's federal-law and constitutional challenges. *See Huawei Technologies USA v. FCC*, 2 F.4th 421 (5th Cir. 2021). The D.C. Circuit upheld the revocations of China Telecom, ComNet, and Pacific Networks without a scintilla of concern towards a First Amendment violation. *See China Telecom (Americas) Corp. v. F.C.C.*, 57 F.4th 256 (D.C. Cir. 2022); *Pacific Networks Corp., et al. v. F.C.C.*, 77 F.4th 1160 (D.C. Cir. 2023).

These cases are all in line with precedent that distinguishes between regulations that target the conduct of "conduits of speech" and speakers themselves. *Turner Broadcasting System, Inc. v. F.C.C.*, 512 U.S. 622 (1994). Courts traditionally view the speech the conduit hosts as being analytically immaterial to the government's regulation of the conduit's conduct—and have upheld regulations

that target a conduit's conduct. *See Turner*, 512 U.S. at 656, 667. The D.C. Circuit used that same rationale in reviewing the FCC's *Net Neutrality Order* and upholding it against First Amendment scrutiny. *U.S. Telecom v. F.C.C.*, 855 F.3d 381, 389 (2017).

That same line of cases applies here. Like the FCC, the Montana legislature has heeded the concerns of the FBI Director Christopher Wray and Director of National Intelligence Avril Haines to protect the security of its citizens. Like the FCC, the Montana legislature targeted the wrongful conduct of one actor, found its ties with China raised irreparable issues that could not be cured with a more general law like S.B. 384, and prohibited that provider from engaging in particular conduct. Like Huawei and China Telecom and ComNet and Pacific Networks, TikTok is affiliated with a Chinese company with close ties to the Chinese government and a history of improperly sharing information about American citizens with the Chinese. And like each of these prohibited companies, TikTok is merely one among many platforms for the speech of others.

Nonetheless, the District Court here rejected the application of *Arcara* for two reasons. One, the court found that S.B. 419 is "not a generally applicable law." Dist. Ct. Op. at 14. Two, the court distinguished *Arcara* because the regulated conduct there was "nonspeech" that had "absolutely no connection to any expressive activity," whereas S.B. 419 "implicates traditional First Amendment speech"

because it bans some users "preferred means of speech" as well as TikTok's ability to "select[], curate[], and arrange[] content." *Id.* at 14-15.

None of these points hold water. *First*, it's true enough that the Montana legislature targeted TikTok in S.B. 419, but that's because TikTok is the only significant social media platform in the state that is tied to a Chinese-controlled company like ByteDance and that has a history of spying on American users at the behest of that company. Had the Montana legislature used more general terms in its statute—banning any such company from operating any social media platform in the state until it divested any ties with a company that is incorporated in any other country designated as a foreign adversary—that legislation would be "generally applicable" but still have a target of one: TikTok. And legislatures need not legislate more broadly than required to address the problem they confront—in this case, TikTok's history of serving as a tool of foreign espionage.

Next, the court's attempt to distinguish *Arcara* as being about "nonspeech" similarly fails. S.B. 419 similarly regulates conduct (or nonspeech)—the operation of a social media platform—and the reason for that regulation (stopping espionage) has "absolutely no connection to any expressive activity." Indeed, the court took pains to say that the regulation merely "implicates" expressive activities, but so did the regulation in *Arcara*. As the Court explained, closing a bookstore would "have some effect on the First Amendment activities of those subject to sanction" and yet

that got the bookstore no special First Amendment scrutiny. *Arcara*, 478 U.S. at 706.

The *Arcara* court explained that First Amendment scrutiny was only appropriate where "it was conduct with a significant expressive element that drew the legal remedy in the first place" or had the "inevitable effect of singling out those engaged in expressive activity," such as a special tax on publishers. *Arcara*, 478 U.S. at 706-07 (citing *Minneapolis Star & Trib. Co. v. Minn. Com'r of Revenue*, 460 U.S. 575, 582–83 (1983)). Here, it was TikTok's espionage of behalf of ByteDance—not conduct with a significant expressive element—that drew the legal remedy in the first place. And the differential treatment did not single out all or even most Montanans engaged in expressive activity—it was narrowly targeted at the only company that regularly collected data from Montanan users and had a history of spying. *Cf. Minneapolis Star*, 460 U.S. at 585 (finding that "differential treatment, unless justified by some special characteristic of the press, suggests that the goal of the regulation is not unrelated to suppressive of expression.").

Indeed, the *Arcara* Court could not have been more clear: Applying First Amendment scrutiny (even intermediate scrutiny) to a regulation of conduct is a "misread[ing] [of] *O'Brien*, which has no relevance to a statute directed at imposing sanctions on nonexpressive activity." Here, S.B. 419 is directed at imposing

sanctions on TikTok's espionage, a nonexpressive activity. That should be the end of the First Amendment analysis.

Nonetheless, the District Court later in its ruling relies on three precedents to hold that S.B. 419 should be subject to First Amendment scrutiny. First, the court holds that the statute "directly and immediately affects" First Amendment rights by "ban[ning] a platform where people speak," citing *Boy Scouts of America v. Dale*, 530 U.S. 640, 659 (2000). Dist. Ct. Op. at 17-18. Next, the court relies on *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989), to reason that S.B. 419 "could be seen as a restriction on the time, place, or manner that a person could speak in the public forum—that is the Internet." Dist. Ct. Op. at 19. And then the court states that even if a regulation of conduct only "puts an incidental burden on speech, it must at least pass intermediate scrutiny." Dist. Ct. Op. at 19 (citing *Pac. Coast Horseshoeing Sch., Inc. v. Kirchmeyer*, 961 F.3d 1062, 1068 (9th Cir. 2020)).

Again, none of this reasoning is correct. Start with *Dale*. There the Court noted that "the Boy Scouts is an expressive association and the forced inclusion of Dale would significantly affect its expression." *Dale*, 530 U.S. at 656. And so a non-discrimination law that required the Boy Scouts to forcibly associate with someone they did not want to associate with "directly and immediately" affected the Boy Scouts' First Amendment rights. In contrast, S.B. 419 does not "directly and immediately" require anyone to speak or prohibit them from speaking—TikTok and

its users are free to express their views (or not) on any of the dozens of other social media platforms and thousands of websites still available in Montana. It only prevents the operation of the TikTok platform in Montana, the linchpin of TikTok's ability to violate the privacy and security of its users.

Next, the District Court's suggestion that banning TikTok until it is divested by ByteDance is a time, manner, and place regulation of the Internet is too clever by half.[1] By that same logic, shutting down a bookstore in Kenmore would be a time, manner, and place regulation of the state of New York—but the *Arcara* Court specifically found that *no* First Amendment scrutiny was required. A ban on operating TikTok is just what it seems to be: A ban on particular conduct by a particular actor; nothing more, nothing less.

Finally, the District Court was wrong to rely on dicta from the *Kirchmeyer* case to claim that intermediate scrutiny always applies when "incidental" burdens on speech arise. As explained above, the Supreme Court has repeatedly required more than a mere "incidental" burden to trigger scrutiny. And the *Kirchmeyer* case involved more than a merely incidental burden: The act at issue there "regulates what kind of educational programs different institutions can offer to different

[1] The analogy also begs the question of whether S.B. 384, which regulates the privacy and security practices of social media platforms, would also be subject to intermediate scrutiny as a time, manner, and place regulation of the Internet. No court, to our knowledge, has suggested that data privacy regulations are subject to such scrutiny.

students. Such a regulation squarely implicates the First Amendment." *Kirchmeyer*, 961 F.3d at 1069. S.B. 419 does no such thing: It does not prohibit TikTok or its users from offering any educational content or speaking on any subject using literally thousands of different venues; it only prohibits the operation of the one social media platform that has been repeatedly used to spy on the American people.

III. Even Under Intermediate Scrutiny, the Montana Legislature Is Likely to Prevail

Assuming for the sake of argument that S.B. 419 does trigger intermediate scrutiny, the Montana legislature should still prevail. That's because S.B. 419 advances the important governmental interest of protecting Montanans from foreign espionage, is targeted only at TikTok's operation so long as it is owned by ByteDance to minimize any burden on speech, and leaves open ample alternative channels for communications.

The District Court held otherwise. But its logic does not hold up to scrutiny (intermediate or otherwise).

First, S.B. 419 advances "the national security interest of protecting Montanans from Chinese corporate and business espionage." Dist. Ct. Op. at 22. TikTok and its users apparently agree. *Id.* As does the State. *Id.* (noting the State contends the interest is in "the protection of Montanans against TikTok's allegedly harmful data practices").

Despite this apparent consensus, however, the District Court discarded any part of the statute focused on protecting Montanans from harmful data practices (including foreign espionage) and reframed this interest as merely a "foreign policy purpose." Dist. Ct. Op. at 23. It then discarded that interest as relevant, holding that "Montana does not have constitutional authority in the field of foreign affairs." *Id.* at 25 (citing *Hines v. Davidowitz*, 312 U.S. 52, 63 (1941)). The District Court clearly erred.

Montana's law is well within the context of states' police powers. S.B. 419's preamble and its overall structure makes clear that it is a consumer protection law, not a foreign affairs regulation. Montana's primary concern was that TikTok "gathers significant information from its users, accessing data against their will to share with the People's Republic of China." *Id.* Preamble. TikTok's history of violating privacy laws, tracking the locations of Americans, sending information on journalists to China, and refusing to preserve and turn over evidence to states grounds that concern in reality. *See* Part I, *supra*. And to make clear that the Montana legislature was not seeking to overreach, S.B. 419 limits the effects of its law to the "territorial jurisdiction of Montana." S.B. 419 § 1. As this Court is aware, a State protecting its own constituents' privacy—even from the People's Republic of China—is a form of a police power that does not infringe on federal sovereignty.

The fact that S.B. 419 takes issue with TikTok's international corporate ownership is immaterial as to whether a state can impose restrictions to quell an underlying concern rooted in its own police powers. States have every right to enact laws that implicate federal jurisdiction so long as those laws are not specifically preempted. For example, this Court took no issue with California using its police power to enact its Internet Consumer Protection and Net Neutrality Act of 2018 even though the law had the undeniable effect of regulating interstate commerce. *ACA Connects v. Bonta*, 24 F.4th 1233 (9th Cir. 2022). Why? This Court held that the California law was rooted in intrastate activities and no federal law specifically foreclosed the state's ability to enact net neutrality laws. *Id.* at 1245-46. No federal law preempts state action here—indeed, Montana was acting in part on the concerns expressed by senior officials of the Biden Administration—and protecting Montanans in Montana from a platform that has consistently stolen user data is firmly rooted in intrastate activities.

What is more, the State makes clear that it takes issue with TikTok's violation of Montana's constitutionally codified right to privacy by being "a valuable tool to the People's Republic of China to conduct corporate and international espionage in Montana and may allow the People's Republic of China to track the real-time locations of public officials, journalists, and other individuals." *Id.* This Court has held that "the protection of privacy is a significant interest." *Gomez v. Campbell-*

Ewald Co., 68 F.3d 871, 876 (9th Cir. 2014). And this Court has held that states have a compelling interest in protecting individual's privacy when "substantial privacy interests are being invaded in an essentially intolerable manner." *Project Veritas v. Schmidt*, 72 F.4th 1043, 1059 (9th Cir. 2023) (citing *Cohen v. California*, 403 U.S. 15, 21 (1971)). To say that the State of Montana has no "important interest" in advancing legislation to protect that right here would be ludicrous.

Second, the District Court found that S.B. 419 was not narrowly tailored because, in effect, S.B. 384 should have been enough and additional sanctions against TikTok were not warranted because "there are many ways in which a foreign adversary, like China, could gather data on Montanans." Dist. Ct. Op. at 28-29. To be frank, these are not the types of judgments a court is equipped to make.

To start, the Montana legislature is free to decide what problems it is trying to solve and the appropriate solutions for those problems. In the context of S.B. 384 and S.B. 419, the legislature was confronting two distinct concerns: one a generalized concern that social media platforms (among others) were not properly protecting the privacy and security of Montanans and the other a specific concern that one social media platform (TikTok) had frequently and consistently broken privacy laws, stymied investigations, and repeatedly tracked Americans and sent that data back to ByteDance, a Chinese corporation. And so the legislature passed two bills: one broadly targeted at the company data practices and another specifically

targeted at the one company the legislature found it could not trust to comply with those laws because of its ongoing relationship with ByteDance. As the State explained to the District Court, that is the definition of narrow tailoring: "eliminat[ing] the exact source of evil it sought to remedy." *City of L.A. v. Taxpayers for Vincent*, 466 U.S. 789, 808 (1984).

Even if the District Court thought TikTok could be trusted with consumer data, that was not its call. This isn't, after all, a review of regulatory action under the Administrative Procedure Act. The Constitution entrusts the police powers to the legislatures and executives of the United States, not the courts. And if the State (in agreement with FBI Director Christopher Wray and Director of National Intelligence Avril Haines) is right that TikTok cannot be trusted, then of course a targeted ban on conduct is narrowly tailored to solve before the State. To find otherwise would derail State and Federal attempts to combat national security threats.

Next, the fact that China has alternative means of gathering data from Montanans is irrelevant. A legislature is not required to entirely solve every aspect of a problem in order to act; it can choose to proceed incrementally—and often must given the numerous troubles that every legislature must face. Here, the State of Montana chose to solve one specific and well-documented means of foreign espionage on the people of Montana—and that is all it was required to do. And to hold otherwise would be absurd: The District Court noted that China could

"purchas[e] information from data brokers . . . , conduct[] open-source intelligence gather, and hack[] operations like China's reported hack of the U.S. Office of Personnel Management." Dist. Ct. Op. at 29. The idea that Montana must solve *all* these problems at once in order to solve any of them is simply absurd. And upholding the District Court's ruling here would cripple both State and Federal attempts to protect the American people from foreign espionage.

Third, the District Court found S.B. 419 did not leave open ample alternative channels of communication because it "forecloses an entire medium of public expression," Dist. Ct. Op. at 30 (quoting *Project Veritas v. Schmidt*, 72 F.4th 1043, 1064 (9th Cir. 2023)), and prevents TikTok and its users from "communicating in their preferred channel of communication." Dist. Ct. Op. at 31.

While that might be true if Montana banned *all* social-networking platforms or some other "entire medium," that's not what S.B. 419 does at all. That law leaves alone the more than a dozen alternatives to TikTok now present and popular in the United States and targets the one—the only one—with ties to a Chinese company that has admitted to spying on American journalists. And even that one platform can operate in Montana if it severs its ties with ByteDance.

Consider *City of Ladue v. Gilleo*, 512 U.S. 43 (1994), the quintessential case on banning an "entire medium" of expression. There, the City of Ladue banned practically all residential signs—that's what banning an entire medium is. *Id.* at 55.

Had the City of Ladue singled out and banned just one manufacturer of residential signs—as Montana singled out and banned only one social media platform—its regulation would have met a much different fate at the Supreme Court.

Similarly, the Court's ruling strays far from settled law in suggesting that because some users prefer using TikTok to other social media, there are not ample alternative channels of communication available to them. *For one*, it has never been the law that a speaker can decide they prefer one particular channel of communication—say KFCC(AM) in Bay City Texas or the Village Books and News Store in Kenmore, New York or TikTok—and by that choice deem every other channel insufficient. Surely the owners of KFCC(AM) (and some of its listeners) thought it their "preferred channel of communication"—and yet that posed no bar to the Federal Communications Commission revoking its broadcast license for repeated misrepresentations. *See* FCC, Report No. GN 98-5, MM Docket 96-173 (Apr. 22, 1998). Surely many of the patrons of Village Books and News Store thought it their "preferred channel of communication" for adult literature—and yet the Supreme Court found that no bar to New York's decision to shut it down for facilitating prostitution. So too here.

For another, the District Court's decision appears to be based on a misreading of this Court's *Project Veritas* case. There, Oregon law generally prohibited the unannounced recording of conversations. The court found that law "functions as 'an

absolute prohibition on a particular type of expression'—the creation of unannounced audiovisual recordings." *Project Veritas*, 72 F.4th at 1065 (quoting *United States v. Grace*, 461 U.S. 171, 177 (1983)). Applying that here, the District Court found that "The State has presented no evidence that SB 419 does not 'function[] as an absolute prohibition on a particular type of expression.'" Dist. Ct. Op. at 31. But how could it? S.B. 419 bars no particular type of expression at all; TikTok and its users are free to communicate any message they want on any other short-form social media platform be it Instagram Reels, Snapchat Highlights, YouTube Shorts, Pinterest, Vigo Video, Triller, Funimate, Likee, or the pre-cursor to all of these: Vine (now incorporated into X née Twitter). Or to frame it a different way, the only way S.B. 419 bars a "particular type of expression" is if the District Court has defined the TikTok platform itself as an entire medium of expression—and how could the State possibly disprove that it is banning that platform?

In short, the District Court simply accepted TikTok's argument that the TikTok platform is a one of a kind, unique platform. And it certainly is. It's the one major social-networking platform in the United States owned by ByteDance. It's the only one that the Director of the Federal Bureau of Investigation and the Director of National Intelligence have identified as a threat to the security and privacy of all Americans. And it's the only one the Chinese have repeatedly used to track

Americans. That makes the many other social-networking platforms superior replacements, not just adequate.

* * *

In short, the First Amendment poses no bar to the implementation of S.B. 419. And allowing the District Court decision to stand would not only overturn decades of precedents but would also handcuff the ability of Congress and the several States to reign in large technology platforms that spy on the American people—hardly a result the framers of our Constitution would have envisioned.

CONCLUSION

For all of the foregoing reasons, the Institute respectfully requests that this Court reverse the District Court's order and remand the case for further proceedings.

Dated: March 8, 2024

Respectfully submitted,

/s/ Joel L. Thayer
Joel L. Thayer
Thayer, PLLC
1255 Union Street, 7th Floor
Washington, D.C. 20002
Telephone: (760) 668-0934
Email: JThayer@thayer.tech

Attorney for Amicus Curiae,
Digital Progress Institute

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 24-34

I am the attorney or self-represented party.

This brief contains 6,007 **words,** including 0 words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- ○ complies with the word limit of Cir. R. 32-1.
- ○ is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ◉ is an **amicus** brief and complies with the word limit of FRAP 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ○ is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ○ complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
  - ☐ it is a joint brief submitted by separately represented parties.
  - ☐ a party or parties are filing a single brief in response to multiple briefs.
  - ☐ a party or parties are filing a single brief in response to a longer joint brief.
- ○ complies with the length limit designated by court order dated _____.
- ○ is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature /s/ Joel L. Thayer **Date** March 8, 2024
(use "s/[typed name]" to sign electronically-filed documents)