[ORAL ARGUMENT SCHEDULED FOR SEPTEMBER 16, 2024]

IN THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

TIKTOK INC., et al., Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States.

Respondent.

Nos. 24-1113, 24-1130, 24-1183

REPLY IN SUPPORT OF MOTION TO FILE PORTIONS OF THE RESPONSE BRIEF AND THREE DECLARATIONS UNDER SEAL AND EX PARTE AND RESPONSE TO PETITIONERS' CROSS-MOTION FOR APPOINTMENT OF A SPECIAL MASTER

The Court should grant the government's motion for leave to file classified material *ex parte*. As the government has explained, these petitions for review involve challenges to a statute that resulted from the weighing by Congress and the Executive Branch of the national-security threat posed by the operation of TikTok as currently structured within the United States. There is no basis for requiring this Court to conduct its review of that statute without considering the classified information that informed the evaluation of that threat by the Executive and Legislative branches.

In response, petitioners do not dispute that this Court has inherent authority to consider classified information *ex parte*. Instead, they largely argue that this Court should decline to exercise that authority here. But this national-security case falls squarely within the rare circumstances in which *ex parte* consideration is appropriate and justified. And the government has made the bulk of its submissions on the public record, as petitioners acknowledge, such that the legal claims at issue can be publicly litigated to the extent consistent with the government's compelling interest in shielding highly sensitive information from public disclosure.

Petitioners use strident rhetoric to try to impugn the integrity of the government's filings, but their actual criticisms raise highly technical points that are at best debatable on their own terms. Petitioners cannot contest the crucial facts—that an entity founded and based in China and subject to Chinese laws controls TikTok's recommendation algorithm and can access sensitive information of millions of Americans—but they nonetheless suggest that asserted imprecision in the government's unclassified filings somehow calls into question the Court's capability to assess the relevance of the classified submissions. Petitioners' own declaration, for example, characterizes ByteDance as a "major Chinese compan[y]," App.772, while petitioners now state that "the assertion that TikTok is owned by a Chinese company is false," Opp'n 16. And, in any event, petitioners' criticisms of unclassified filings provide no reason for this Court not to consider

the classified information that informed the political branches' assessment of the need for the challenged legislation.

The Court should also deny petitioners' alternative request to appoint a special master, which would cause delay and complication for little apparent benefit. After asking the Court to expedite this case and jointly agreeing to certain procedures for the handling of the parties' factual submissions, petitioners now ask the Court at this late stage to appoint a special master to recommend procedures to handle the limited *ex parte* information. This Court is fully capable of assessing the classified evidence for itself, as it routinely does in analogous cases. Petitioners' motion should be denied.

- I. THE COURT SHOULD GRANT LEAVE TO FILE THE CLASSIFIED RESPONSE BRIEF AND CLASSIFIED DECLARATIONS UNDER SEAL AND EX PARTE
 - A. This Case Warrants this Court's Review of the Classified Record Supporting an Important Act of Congress

Petitioners challenge the constitutionality of the recently enacted Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, 138 Stat. 895 (2024) (Act). They primarily contend that the Act violates their First Amendment rights. As the government has explained, *see* Mot. 1-2; Gov't Br. 11, before Congress enacted the Act, it received several classified briefings and conducted one classified hearing, at which the Executive Branch provided extensive information—including substantial classified information—on

the national-security risks posed by TikTok's continued operations in the United States under its current ownership structure. The classified information gathered by the Executive Branch and shared with Congress informed the judgment that these national-security risks are sufficiently great to require the Act's restrictions.

Although Congress received substantial classified information before enacting the Act, Congress and the Executive have publicly articulated for years the primary risks that TikTok poses. First, TikTok collects vast amounts of data on its U.S. users—and, through those users, on non-users—and that data collection threatens to allow the Chinese government access to sensitive information that could be used to undermine the security of the United States. Second, TikTok relies on a proprietary recommendation algorithm to determine the videos sent to users, and various features of that algorithm threaten to allow the Chinese government to covertly control the content consumed by American users in ways detrimental to U.S. interests. See Gov't Br. 7-11. Even before the government filed its brief and declarations, petitioners were well aware of those concerns, and filed a declaration in this case focused on those two issues. See App.762. The classified information discussed in the government's brief provides the additional, highly sensitive, and non-public context and grounding that helped Congress and the Executive Branch properly evaluate the magnitude and gravity of those publicly articulated risks. This Court should have the same opportunity.

By seeking to prevent this Court's ex parte consideration of classified information, petitioners attempt to require either that this Court evaluate the constitutionality of an important national-security statute on the basis of an artificially circumscribed record or that the government reveal highly sensitive classified information. Neither of those options is tenable, and nothing in this Court's precedent or petitioners' filing justifies forcing such a choice.

Although the government recognizes that the use of ex parte information in litigation is the exception rather than the rule, this case presents exactly the situation where this Court regularly relies on ex parte classified information. The government acted partially on the basis of such sensitive information, and petitioners now challenge the factual basis for that action, urging that the government's national-security judgments were not "supported by hard evidence," TikTok Br. 48-49, and were unduly "speculative," id. at 52-53. In such a scenario, this Court properly exercises its "inherent authority to review classified material ex parte, in camera as part of its judicial review function." Olivares v. TSA, 819 F.3d 454, 462 (D.C. Cir. 2016) (quotations omitted); see also Mot. 7-8 (collecting cases). Any attempt to adjudicate petitioners' claims without considering that information would unduly hamper the Court's ability to engage in its judicialreview function, leaving the Court with an artificially limited record that would not reflect the full scope of reasons underlying the Act.

As noted, the government's two core justifications for the Act are public, as is much of the supporting information. By petitioners' own estimation (Opp'n 1), nearly 85% of the government's brief and 70% of the government's declarations are unredacted. Likewise, for purposes of transparency and completeness, even though the government did not rely on it in its brief, the government recently made available unclassified portions of the transcript of a committee hearing related to the Act. *See* Notice of Filing Redacted Transcript (Aug. 9, 2024). The government is not trying to litigate in secret, but rather to litigate in public to the greatest extent possible, while still providing the Court with access to the classified information that informed the government's national-security judgments that are central to this litigation.

There is thus no basis for requiring this Court to adjudicate this case without access to classified information. And the government also cannot properly be forced to reveal the highly classified information to outside parties. As this Court has recognized, "[f]orcing the executive branch to disclose information that it has validly classified would 'compel a breach in the security which that branch is charged to protect." Fares v. Smith, 901 F.3d 315, 324 (D.C. Cir. 2018) (quoting National Council of Resistance of Iran v. Department of State, 251 F.3d 192, 208-09 (D.C. Cir. 2001)). This case involves information classified at the "Secret" and "Top Secret" levels. Disclosure could thus be expected to cause "serious" (Secret)

or "exceptionally grave" (Top Secret) "damage to the national security." Exec. Order No. 13,526, 75 Fed. Reg. 707, 707-08 (Dec. 29, 2009). The government has concluded that it would be inappropriate to divulge that information to the public or to petitioners, and petitioners are not entitled to second-guess that national-security conclusion. *See also Twitter, Inc. v. Garland*, 61 F.4th 686, 710 (9th Cir. 2023) ("[T]he government might have a legitimate interest in shielding the materials even from someone with the appropriate security clearance." (quotations omitted)); *United States v. Daoud*, 755 F.3d 479, 484 (7th Cir. 2014) (rejecting the argument that disclosing classified information "to cleared lawyers could not harm national security"). Indeed, petitioners do not seriously suggest that they should be given access to highly classified information, merely citing the possibility as something a special master might order after further consideration. *See* Opp'n 36.

In similar circumstances, as noted, this Court has repeatedly permitted the filing and consideration of *ex parte* classified information that justifies challenged government action. Petitioners, conversely, identify no remotely comparable case in which the Court has refused to consider classified information. Instead, they rely on cases that stand for the general—and uncontroverted—proposition that adversary presentation is the general rule and preferred when possible. When they address the cases in which this Court has held that consideration of classified information was warranted, they seem to suggest that this case is different because

of the nature of the interests involved. But the Court has never suggested that the government's ability to submit classified information *ex parte* turns on a questionable "distinction between, or hierarchy among, constitutional rights." *Caplin & Drysdale, Chartered v. United States*, 491 U.S. 617, 628 (1989). And although petitioners repeatedly emphasize the scope of the TikTok platform, the platform's immense size illustrates the size of the unprecedented national-security threat. There is no basis for disregarding evidence that demonstrates the scope of that threat.

B. Petitioners' Remaining Arguments Against Submitting Materials Ex Parte Are Without Merit

1. Petitioners are mistaken to assert (at 5-8) that the evidence in the government's declarations is "not relevant." As an initial matter, this argument, even if credited, would largely constitute an argument on the merits that the government cannot prevail based on the classified information, rather than an argument that the Court cannot review the classified evidence and determine for itself how much weight it should receive.

But the argument is, in any event, wrong on its own terms. The government responded in its merits brief, citing binding precedent, to petitioners' argument that this Court's review is limited to congressional findings. *See, e.g.*, Gov't Br. 66.

And there is no dispute that Congress held multiple classified briefings and a classified hearing; petitioners' desire to question how the information from those

USCA Case #24-1113

briefings and hearings was disseminated within the Legislative Branch before the vote bears no resemblance to the relevant inquiry on judicial review of a duly enacted statute. *See* Newman Decl. ¶¶122, 124-26; Blackburn Decl. ¶5; App.10-12 (describing multiple classified legislative proceedings); Members of Congress Amicus Br. 7-9 (explaining that the Act was "the product of extensive legislative factfinding going back decades").

The suggestion that the evidence the government put before this Court is somehow distinct from the national-security judgments that underlie the Act does not withstand even the most cursory scrutiny. The declarations provide the U.S. Intelligence Community's assessments of the potential threats to U.S. national security posed by ByteDance and TikTok. *See* Blackburn Decl. ¶9; Vorndran Decl. ¶4; Newman Decl. ¶5-7. As explained in the government's brief (at 18-79), those assessments directly inform the compelling interest that the Act is appropriately tailored to serve.

2. Petitioners erroneously assert (at 18) that the government's public submissions include "factually incorrect and misleading statements" that warrant denying the government's motion to file classified material *ex parte*. Those arguments fail at every level.

As an initial matter, while petitioners take issue with certain phrasing in the government's brief and declarations, they ultimately do not cast doubt on the

fundamental points. For example, TikTok does not actually dispute that it collects information about U.S. users' locations; as explained below, petitioners merely deny doing so in one particular manner. And it is beyond debate that there is a risk that China can gain access to such data, along with the vast swaths of other sensitive and personal data that the application collects. Gov't Br. 8-9, 18, 27; Blackburn Decl. ¶9. Likewise, petitioners stress (Opp'n 17) that TikTok US's "ultimate owner is the Cayman-incorporated ByteDance Ltd.," but they fail to grapple with the uncontested fact that operating entities of ByteDance are headquartered in Beijing and thus subject to broad forms of control by the Chinese government. Nor does the abstract question of where TikTok's proprietary contentrecommendation algorithm physically resides change the critical point that ByteDance could be expected to comply with demands by the Chinese government to manipulate the algorithm. Blackburn Decl. ¶69. The purported inaccuracies that petitioners claim to identify do not call into question the Act's justifications, much less preclude the Court from making its own judgment about the unclassified and classified submissions that support the Act's passage.

Petitioners' specific claims are, in any event, unfounded. Petitioners take issue with the notion that "the TikTok application collects 'precise location' data from its U.S. users," responding with a carefully worded statement that "current versions of the application do not collect GPS location information." Opp'n 14-15.

The government did not say anything about "GPS location information," in particular, but instead stated more generally that TikTok collects U.S. users' location information. There is no dispute that TikTok collects such information in ways other than through GPS location, such as by using internet protocol (IP) addresses. See, e.g., United States v. Tolbert, 92 F.4th 1265, 1269 (10th Cir. 2024) (describing the use of "open-source searches" to connect an IP address to a particular location); cf. Newman Decl. ¶101. Indeed, as the government's brief explained, Gov't Br. 28-29, public reporting indicated that ByteDance employees "accessed TikTok user data and IP addresses to monitor the physical locations of specific U.S. citizens." App.8 & n.45 (citing Emily Baker-White, EXCLUIVE: TikTok Spied on Forbes Journalists, Forbes (Dec. 22, 2022)); Newman Decl. ¶98; Vorndran Decl. ¶29. Petitioners can disagree about whether the information that enabled them to perform that monitoring is better described as "precise" location data or by some other adjective, but they are wrong to portray any such dispute as "a material factual inaccuracy in the government's submission, plain and simple," Opp'n 15. Moreover, petitioners' need to use the phrase "current versions of the application" in their denial reflects that GPS information is collected from users who still use an old version of the application. See Privacy Policy, TikTok (last updated July 1, 2024), https://perma.cc/AA4E-LH5U, cited in Opp'n 15 n.2.

Petitioners fare no better in denying that "TikTok is owned by a Chinese company." Opp'n 16. Petitioners emphasize that "TikTok Inc. is ultimately owned by ByteDance Ltd., a Cayman Islands-incorporated holding company." Id. But the relevant national-security consideration is the degree to which the Chinese government may exercise control over the entity's operations. That inquiry would naturally focus not on the location of the holding company's incorporation but on the "operating entities," which are "in China," according to petitioners' own declaration. App. 769 n. 24. Petitioners' declaration goes on to refer to the "corporate group" generally as "ByteDance," id., and to justify the fact that "ByteDance reportedly employs certain [Chinese Communist Party] members" on the ground that "virtually all major Chinese companies are required to maintain internal committees comprised of [Chinese Communist Party] members," App. 772. Given that petitioners' own declarant refers to ByteDance as a "major Chinese compan[y]," petitioners can hardly complain that the government similarly refers to TikTok's being owned by a Chinese company—particularly because petitioners have not alleged that TikTok has been sufficiently divested from control by a foreign adversary to render the statute inapplicable, see Act § 2(g)(6). A House Committee's apparent imprecision in describing the intricacies of ByteDance's corporate structure, repeated in the government's brief, does not alter that reality, regardless of whether that description is inaccurate in some particular. See Gov't

Br. 7 (asserting, citing App.3, that TikTok Ltd. is owned by Beijing ByteDance Technology).

Petitioners also object (at 15) to the government's references to TikTok's content-recommendation algorithm's being "located in China." The question of where an algorithm composed of lines of computer code physically resides is somewhat abstract, and the government adopted a customary shorthand to convey that the recommendation engine is based in China and subject to manipulation by the Chinese government. See, e.g., Gov't Br. 16-17. Petitioners concede that "[t]he source code for TikTok's recommendation engine was originally developed by ByteDance engineers based in China," App.817, and that Chinese law accordingly prohibits the export of such "technolog[y] developed in China," TikTok Br. 24; see also App.413-14, 659. When attempting to address the government's nationalsecurity concerns through a national security agreement, petitioners' own proposal provided that the "source code supporting the TikTok platform, including the recommendation engine, w[ould] continue to be developed and maintained by ByteDance subsidiary employees, including in the United States and in China." App.829.

Contrary to petitioners' suggestion (at 15-16), their declarant does not show the absence of Chinese influence merely because the "U.S. recommendation engine is stored in the Oracle cloud" and "deploy[ed] . . . in the United States" by a

3. Petitioners do not advance their argument by seeking to second-guess the government's determinations about which disclosures would harm national security. As the Supreme Court has recognized, decisions regarding the risk of releasing particular information "are worthy of great deference," as it is the responsibility of Executive Branch officials "to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an

unacceptable risk of" harm. CIA v. Sims, 471 U.S. 159, 179-80 (1985); see also, e.g., Center for Nat'l Sec. Studies v. U.S. Dep't of Justice, 331 F.3d 918, 927 (D.C. Cir. 2003) (noting, in the context of the Freedom of Information Act, that the Court has "consistently reiterated the principle of deference to the executive . . . when national security concerns are implicated").

The specifics of petitioners' criticisms here underscore why that is the case here. They question why an intelligence community official's "bottom-line conclusions must be redacted," Opp'n 18-19, but these sorts of "predictive judgments" and "assessment[s]" strike at the core of national-security interests, Trump v. Hawaii, 585 U.S. 667, 708 (2018). Petitioners also cite instances in which references to public sources have been redacted, ignoring that the context in which a public source is discussed could be classified even when the source itself is not. See, e.g., Exec. Order No. 13,529, 75 Fed. Reg. 707, 711 (Dec. 29, 2009) (providing for when "[c]ompilations of items of information that are individually unclassified may be classified"); Sims, 471 U.S. at 178 (upholding authority "to withhold superficially innocuous information"). And petitioners critique the government's lifting of limited redactions after further consideration, an act that demonstrates the government's commitment to transparency.

4. Petitioners mistakenly contend (at 30-31) that the government should not be permitted to rely on classified information here because Congress did not

provide express statutory authority for doing so. This Court has permitted the government to rely on classified information ex parte in a host of contexts that did not rest on express statutory authorization. See, e.g., Abdellatif v. U.S. Dep't of Homeland Sec., No. 20-1298, 2024 WL 3546140, at *7 (D.C. Cir. July 26, 2024); Jifry v. FAA, 370 F.3d 1174, 1181-82 (D.C. Cir. 2004). It would be odd to suggest that Congress intended to force the Executive Branch to defend the enactment here, which was premised in substantial part on classified information, based on an artificially weakened record. And petitioners get matters backwards in suggesting that Congress must not have intended for the government to submit classified information to defend the Act's designation of TikTok because the government must submit "a classified annex" to Congress when designating foreign adversary controlled applications under the Act, see $\S 2(a)(2)(B)$, (g)(3)(B). That provision instead highlights Congress's understanding that classified information is an integral part of the type of national-security judgment at issue here.

Petitioners' reliance on the Classified Information Procedures Act, which applies only "in criminal cases," Opp'n 31, is misplaced. The procedures designed for that very different context may be instructive in some circumstances, but by their own terms do not govern here. And even the case on which petitioners chiefly rely made clear that those procedures are not required. *See Kashem v. Barr*, 941

F.3d 358, 390 (9th Cir. 2019); see also Parhat v. Gates, 532 F.3d 834, 849 (D.C. Cir. 2008) (describing those procedures as an example to borrow from).

5. The government's request to submit classified information *ex parte* complies with due process. Petitioners barely acknowledge the wealth of public sources and information that have enabled them to make their case. Instead, they suggest that the government cannot rely on ex parte materials because of the "private interests" associated with expressive activities on TikTok. Opp'n 22-23. Even putting aside that those expressive activities are not the Act's target and that those activities may continue on other social-media platforms or on TikTok itself following a proper divestment from ByteDance, see Gov't Br. 60-65, petitioners err in giving short shrift to the weighty public interest that supports submitting a limited class of classified materials ex parte. The Act reflects weighty interests in national security, and the government has a "compelling interest in withholding national security information from unauthorized persons." Department of the Navy v. Egan, 484 U.S. 518, 527 (1988) (quotations omitted).

Petitioners do not contest those public interests, instead contending that the government's interest in *relying on* classified information is "weak at best," again questioning the relevance or probative value of that information. Opp'n 19-21, 23-24, 29; *see also* pp. 8-9 *supra*. This Court can make that judgment based on the evidence itself.

Given the compelling government interests in protecting national security and safeguarding classified information, the government's proposal to submit limited classified information ex parte sufficiently ensures basic fairness and is reasonably and appropriately designed to protect against erroneous deprivation of petitioners' private interests. As explained, see Mot. 6-8, this Court has permitted the government to file classified information ex parte in a number of cases, where it has rejected due process challenges to relying on that information in an ex parte setting. See, e.g., Jifry, 370 F.3d at 1182-84; People's Mojahedin Org. of Iran v. Department of State, 327 F.3d 1238, 1242 (D.C. Cir. 2003). This Court has recognized that even when defending a designation with "a dire effect on a designee's private interests," due process can be satisfied by a "short unclassified summary" that, although "not highly fact-specific," provides "the who, what, when and where of the allegations." Bello v. Gacki, 94 F.4th 1067, 1075-76 (D.C. Cir. 2024) (quotations omitted). The government has presented here its core rationales, much of the supporting evidence, and comprehensive legal argument on the public record—amounting to much more than the "summaries" that the Court has endorsed in other cases.

THE COURT SHOULD DENY PETITIONERS' CROSS-MOTION TO APPOINT A II. SPECIAL MASTER

After agreeing several months ago to procedures "govern[ing] these original actions," Joint Mot. to Set Briefing and Oral Argument Schedule 3 (May 17, 2024), petitioners now request that the Court appoint a special master to "recommend" additional procedures. Opp'n 33. Petitioners have long been on notice that the government may seek to submit evidence ex parte, see Joint Mot. 4, and they could have proposed procedures to handle those materials when the parties jointly proposed how the Court should adjudicate this case. Not only did they not propose any such procedures then, they do not propose any now, instead asking the Court to appoint a special master, who would review the information and make a proposal to this Court.

Petitioners urge the Court to introduce unnecessary complexity and delay by appointing a special master and necessitating further briefing. They never explain how those procedures are compatible with the expedited nature of this case where argument is a month away, nor why this Court is incapable of assessing the comparatively slim amount of classified information in this case. Petitioners rely (Opp'n 34) on a case in which this Court held that the district court did not abuse its discretion by appointing a special master to examine over 14,000 pages of classified documents to identify a representative sample for the district court to adjudicate disclosure requests under the Freedom of Information Act. In re U.S.

Department of Defense, 848 F.2d 232, 236 (D.C. Cir. 1988). But petitioners fail to explain why this Court should face any similar difficulty examining the government's brief and declarations here, which are less than 350 pages and overwhelmingly unclassified. The cases petitioners cite involving the appointment of a special master to adjudicate contempt proceedings—none of which involved ex parte evidence—are even further afield. See Opp'n 35 n.14.

Petitioners' request for a temporary injunction is similarly baseless. As explained in the government's brief (at 86-88), petitioners' cursory argument makes no effort to establish the requisite showing for such an "extraordinary remedy." Chaplaincy of Full Gospel Churches v. England, 454 F.3d 290, 297 (D.C. Cir. 2006) (quotations omitted). Certainly, any delay occasioned by petitioners' belated request to create additional procedural complexity would not provide additional justification for such substantive relief.

CONCLUSION

For the foregoing reasons, we respectfully request that the Court grant the government leave to file its response brief and three declarations in this matter under seal for the Court's *ex parte* and *in camera* review; and we respectfully request that the Court deny petitioners' request to appoint a special master or grant a temporary injunction.

Respectfully submitted,

Filed: 08/15/2024

BRIAN M. BOYNTON

Principal Deputy Assistant Attorney

General

BRIAN D. NETTER

Deputy Assistant Attorney General

MARK R. FREEMAN SHARON SWINGLE DANIEL TENNY

/s/ Casen B. Ross
CASEN B. ROSS
SEAN R. JANDA
BRIAN J. SPRINGER
Attorneys, Appellate Staff
Civil Division, Room 7270
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530
(202) 514-1923
casen.ross@usdoj.gov

CERTIFICATION OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), I hereby certify this filing complies with the requirements of Fed. R. App. P. 27(d)(1)(E) because it has been prepared in 14-point Times New Roman, a proportionally spaced font, and that it complies with the type-volume limitation of D.C. Circuit Rule 27(c), because it contains 4,414 words, according to the count of Microsoft Word.

/s/ Casen B. Ross

Filed: 08/15/2024

Casen B. Ross

CERTIFICATE OF SERVICE

I hereby certify that on August 15, 2024, I electronically filed the foregoing through the appellate CM/ECF system. Service was accomplished on registered counsel through the CM/ECF system.

/s/ Casen B. Ross

CASEN B. ROSS