Are TikTok "Bans" a Bill of Attainder?

Terence Check*

Are the growing number of TikTok "bans" prohibited under the Bill of Attainder Clause of the U.S. Constitution? Probably not, but this conclusion is not as obvious as one might think. Accordingly, this brief Article examines one of the most pressing national security issues of the current moment: increasing legislative activity at federal and state levels to ban TikTok, and whether such bans would comport with the Constitution's prohibitions against "bills of attainder." TikTok is a hugely popular social media application owned by ByteDance, a technology company located in the People's Republic of China (PRC). Due to these deep ties to the PRC, a growing number of legislators, governors, and federal government agencies have taken steps to limit the reach of TikTok within the United States on security grounds. The security concerns used to justify the bans fall into two general categories. First, there is the risk of misuse of the personal, demographic, and social data gathered by TikTok. Second, there is the opportunity that TikTok provides to the PRC to disseminate Chinese Communist Party (CCP) propaganda. Within the United States, these concerns pit state and federal government interests against the extensive economic activity of a $400 billion corporate behemoth, making for a potential legal battle of great societal significance.

The particularity of these government actions regarding TikTok may seem to raise questions about the Constitution's Bill of Attainder Clause, which is designed to prevent such punishments that arose in an unseemly era of legislative pronouncements of guilt motivated by the caprice of kings and politicians. This Article examines whether TikTok bans would constitute bills of attainder by analyzing Kaspersky Laboratory v. DHS*, which reviewed a Congressional ban on using Kaspersky Labs products by the federal government.*[1] Kaspersky *is a leading case in bill of attainder jurisprudence. It presents a similar fact pattern involving foreign technology and government action to prevent security threats and accordingly has great significance for the current moment. This Article concludes that not only are TikTok bans as currently conceived not bills of attainder (because they do not punish) but also that the ahistorical and atextual judicial expansion of the range of laws covered by the Bill of Attainder Clause may become untenable in an age of complex nation-state competition where nimble legislative interventions for security matters beyond TikTok may become increasingly necessary.*

* © 2024 Terence Check. Senior Counsel, Cybersecurity and Infrastructure Security Agency; Adjunct Professor, Cleveland State University College of Law; LL.M., American University; J.D., Cleveland State University. All statements are made in the author's personal capacity and do not reflect any position of any institution or agency.

1. As this Article was being readied for publication, Congress and President Biden enacted the Protecting Americans from Foreign Adversary Controlled Applications Act of 2024. As widely expected, TikTok has challenged the Act on Constitutional grounds, alleging a violation of the First Amendment. Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec., 909 F.3d 446, 450 (D.C. Cir. 2018).

I. INTRODUCTION

In this hyper-partisan world, the hugely popular social media app TikTok has the misfortune of becoming one of the few issues around which a bipartisan consensus has begun to form.[2] Republican legislators and university administrators do not often agree, but increasing numbers of them have concluded that TikTok poses a threat to security.[3] These security concerns vary, but most stem from the fact that TikTok belongs to ByteDance, a technology giant headquartered in the People's Republic of China (PRC).[4] Entrusting the sheer quantity and quality of data created, stored, and analyzed by TikTok to further access and processing by entities within the PRC has raised urgent security concerns.[5] Even though TikTok originally came under federal government scrutiny in 2020, a flurry of legislative and executive activity regarding the application has brought renewed attention to the highly engaging and controversial social media platform.[6]

The current raft of state and federal legislative activity to ban TikTok arises in part from the lack of clarity regarding federal authority to

2. Cristiano Lima & Aaron Schaffer, *Businesses and Schools are Facing Pressure to Drop TikTok, Too*, WASH. POST (Jan. 18, 2023, 9:11 AM), https://www.washingtonpost.com/politics/2023/01/18/businesses-schools-are-facing-pressure-drop-tiktok-too/.

3. *See generally* Bernard Horowitz & Terence Check, *TikTok v. Trump and the Uncertain Future of National Security-Based Restrictions on Data Trade*, 13 J. NAT'L SEC. L. & POL'Y 61 (2022) (examining the 2020 TikTok ban by President Trump and subsequent litigation).

4. *Id.* at 64.

5. *Id.* at 89-90 (quoting Tiktok v. Trump, 507 F. Supp. 3d 92, 98-99 (D.D.C. 2020)).

6. *Id.* at 64.

regulate cross-border data trade in the interest of national security. As exposed by a D.C. district court decision that overturned a Trump Administration-era "ban" of TikTok under the International Emergency Economic Powers Act (IEEPA), the President's authority to restrict the operation of social media apps, even if such apps pose significant security threats in the views of relevant experts, appears to be in flux—or, more realistically, highly limited under recent case law.[7] Accordingly, Republican governors in multiple states have taken executive action to prohibit the use of TikTok on state government networks and devices, and the federal government has pursued a similar policy that has received bipartisan support.[8] Even though many of the concerns identified—data theft, espionage, foreign propaganda—all might exist to some extent with any major social media or technology company, the executive orders and bills referenced above all call out TikTok with specificity: these bans would apply to TikTok and only TikTok.[9]

This Article examines whether this particularity raises any Constitutional concerns, ultimately concluding that such legislative and executive actions targeting TikTok do not constitute bills of attainder. This Article begins with historical background of the bill of attainder and how TikTok "bans" rose to prominence over the course of the past several years. With this foundation laid, this Article examines the viability of legislative bans on TikTok by examining *Kaspersky Laboratory v. DHS*, one of the leading recent cases addressing bills of attainder in the unique context of legislative bans on companies and software the pose a threat to U.S. national security.

Current trends indicate that if TikTok wants to remain in the U.S. market, it appears likely that TikTok must either choose between divestiture or some other restructuring to shed its PRC connections or take the matter to court.[10] In anticipation of the latter course (TikTok has challenged a ban once before), this Article hopes to answer whether TikTok bans are bills of attainder; to hopefully avoid drawn out litigation

7. *Id.* at 97.

8. Aaron Schaffer, *There Are TikTok Bans in Nearly Two Dozen States*, WASH. POST (Jan. 10, 2023, 7:16 AM), https://www.washingtonpost.com/politics/2023/01/10/there-are-tiktok-bans-nearly-two-dozen-states/.

9. *See*, *e.g.,* Averting the National Threat of Internet Surveillance, Oppressive Censorship and Influence, and Algorithmic Learning by the Chinese Communist Party Act, S. 347, 118th Cong. (2023).

10. Matt Perault & Samm Sacks, *Project Texas: The Details of TikTok's Plan to Remain Operational in the United States*, LAWFARE (Jan. 26, 2023, 8:01 AM), https://www.lawfareblog.com/project-texas-details-tiktoks-plan-remain-operational-united-states [https://perma.cc/8XZE-ZV5V].

or circuit splits over this interesting issue; and to pave the way for future legislative attempts to regulate cross-border data flows in the interest of national security.

II. BACKGROUND: TIKTOK DANCES AND ENGLISH NOBLES

By their very nature, bills of attainder single out individual persons for punishment. Thus, legislative acts singling out TikTok appear to implicate, at least theoretically, the Bill of Attainder Clause. This Part examines how the Bill of Attainder Clause came to be and how American courts have since interpreted the scope of the provision. Following that overview, this section considers how TikTok came to be singled out in this way and how it specifically poses a threat to U.S. national security.

A. The Origins of the Prohibitions on the "Bill of Attainder"

Article I, Section 9, Clause 3 of the Constitution states that "[n]o Bill of Attainder . . . shall be passed."[11] This constitutional provision has rarely been examined by courts, but the prohibition of such bills represents a key substantive protection of human rights and liberties against legislatively-enacted tyranny.[12]

Seemingly quaint by today's standards, bills of attainder originated in medieval England as a way for kings to pronounce guilt and exact penalties through acts of Parliament.[13] Usually, "attainder" meant legislation that targeted a specific individual, levied the death penalty (typically by beheading or drawing and quartering), and included the further humiliation of "attainting" the condemned's heirs by stripping them of nobility, civil rights, and the ability to inherit.[14]

Historically, the Supreme Court also extended the Clause to cover lesser legislatively delivered punishment, known as "bill of pains and penalties."[15]

While courts maintain that bill of attainder cases hinge upon their "own highly particularized context," all bills of attainder share a few central elements. "[A] law is prohibited under the bill of attainder clause 'if it (1) applies with specificity, and (2) imposes punishment.'"[16]

11. U.S. CONST. art. I, § 9. A similar provision prohibiting states from passing bills of attainder appears in Article I, Section 10.

12. Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec., 909 F.3d 446, 453 (D.C. Cir. 2018).

13. United States v. Brown, 381 U.S. 437, 441 (1965).

14. *Id.* at 441-42.

15. *Id.* at 441.

16. *Kaspersky*, 909 F.3d at 454 (citing Flemming v. Nestor, 363 U.S. 603, 616 (1960)).

Regarding the second criteria, the clause especially applies to laws that impose punishment without judicial review.

In addition to protecting the rights of individual people who might unfairly catch the ire of the legislature in the "heat of the current moment," the bill of attainder provision also prevents the "aggrandizement" of the legislature.[17] The goal of the clause, therefore, is as much functional as it is philosophical: curtailing the ability of other branches of government to pronounce guilt is as much a check on the legislative branch as it is a way to protect human rights.[18] Thus, even if there is no longer threat of an English potentate beheading disfavored nobles, the separation of powers and the need for checks and balances still animate the Bill of Attainder Clause.

These structural, political aspects of the bill of attainder provision seem to shine forth in landmark Supreme Court cases from the Civil War era. *Missouri v. Cummings* related to the enforcement of statutes requiring loyalty oaths of various professional classes with the stated purpose of excluding from the ranks of clergy, lawyers, and politicians any who "ever given aid, comfort, countenance, or support to persons engaged in any such hostility; or has ever, in any manner, adhered to the enemies, foreign or domestic, of the United States."[19]

Between the Civil War and the Cold War, the Supreme Court did not shy away from broadening the scope of the Bill of Attainder Clause beyond its original historical context in three distinct ways regarding (1) the severity of criminal punishment, (2) the degree of specificity required in the bill itself, and (3) the examination of civil harms in addition to criminal punishments.

First, the Supreme Court in *Cummings* expanded the scope of the type of punishment that would constitute a bill of attainder. In striking down a Missouri law imposing a fine or a short prison sentence for any clergy who refused to take an oath of loyalty to the United States, the Court held that "[i]t has been decided that bills of pains and penalties, which inflict a milder degree of punishment, are included within bills of attainder, which refer to capital offences."[20] The *Cummings* decision extended the reach of the Clause to those lesser bills, and it did so without citing authority or the views of the Founders.

17. John J. Cavaliere, III, *The Bill of Attainder Clauses: Protections from the Past in the Modern Administrative State*, 12 AVE MARIA L. REV. 149, 153 (2014).

18. *Id.*

19. Cummings v. Missouri, 71 U.S. 277, 279 (1866).

20. *Id.* at 296.

Second, the *Cummings* court also struck down legislation that did not specifically name one person, as traditional bills of attainder usually did, and instead struck down a law that applies to a class of individuals. The Court wrote: "If these clauses, instead of mentioning his name, had declared that all priests and clergymen within the State of Missouri were guilty of these acts, or should be held guilty of them, and hence be subjected to the like deprivation, the clauses would be equally open to objection."[21] Additionally, courts have assumed, without deciding, that the Clause also extends to corporations as well as natural persons.[22] This extension seems particularly ahistorical—it's difficult to behead a company, after all. But circuit courts have not examined the issue closely.

In a third expansion, the Supreme Court further stretched the Clause roughly a century later in *United States v. Lovett*, which considered the validity of an appropriations provision that prohibited paying federal employees deemed as "subversive."[23] Depriving a federal employee of salary payments, however inconvenient to that employee's pocketbook, seems to pale in comparison to the traditional sorts of punishments common to the court of Henry VIII and reflects a certain willingness by the Court to significantly depart from the historical context of the Clause.[24] In the words of the Court in *United States v. Brown*, another Cold War era decision:

> [T]he bill of attainder clause was intended not as a narrow, technical (and therefore soon to be outmoded) prohibition, but rather as an implementation of the separation of powers, a general safeguard against legislative exercise of the judicial function, or more simply-trial by legislature.[25]

Despite the judicial expansion of the Clause, elsewhere, legislative acts of specific applicability seem to persist. For example, the Constitution still contemplates some possibility of an "attainder" issued by Congress, specifically in the context of treason. Article III, Section 3 reads:

---

21. *Id.* at 324.

22. Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec., 909 F.3d 446, 453 (D.C. Cir. 2018) ("This court has previously assumed without deciding that the Bill of Attainder Clause's protection applies to corporations such as Kaspersky.").

23. 328 U.S. 303, 307, 314-15 (1946).

24. *See* Communist Party of U.S. v. Subversive Activities Control Bd., 367 U.S. 1, 86 (1961) (finding that a registration requirement for certain political groups was not a bill of attainder because it didn't apply to specific organizations but regulated conduct by imposing punishment only after an administrative hearing (reviewable by a court) and did not have retroactive application to past conduct).

25. United States v. Brown, 381 U.S. 437, 442 (1965).

> The Congress shall have Power to declare the Punishment of Treason, but no Attainder of Treason shall work Corruption of Blood, or Forfeiture except during the Life of the Person attainted.[26]

This indicates that Congress could "attaint" someone, perhaps through a legislative act (noting the word "declare") but unlike English attainders, their American equivalents would only punish the person condemned and not her heirs or assigns (i.e., "Life of the Person attainted").[27]

Further, the Court found that a specific congressional law targeting the papers and records of President Nixon was not a bill of attainder, and in doing so the Court articulated the three-part test for determining whether a legislative act "punishes" extrajudicially.[28] As the U.S. Congress's Annotated Constitution summarizes:

> The *Nixon* Court then proceeded to lay out three tests for assessing whether a law imposes punishment: (1) historical, (2) functional, and (3) motivational. The historical test looks to "[t]he infamous history of bills of attainder" to determine whether the law was one of a limited set of legislative actions that were deemed to be bills of attainder before the Founding and in prior Supreme Court cases.[29]

The need to balance the interests of the state against the rights of individuals illuminates the history and practice of bill of attainder jurisprudence. It is perhaps no accident that courts and legislatures examine these questions in periods of heightened political tension and perceived (or real) threats to state security: for example, during the civic and geopolitical turmoil of Tudor England, the Reconstruction era, and the Cold War. This Article now turns to the issue of TikTok and whether it shares, in this respect, the company of English nobles, former Confederates, and postwar Communists.

B. The Factual Origins of TikTok "Bans"—Why is TikTok a Threat?

The legislative interest in TikTok did not appear out of thin air. Instead, the growing alarm over TikTok's data practices arose against the

---

26. U.S. CONST. art. III, § 3.

27. *Id.* Furthermore, bills of attainder seemed to persist in pre-Constitutional governments. For example, in 1778, Thomas Jefferson drafted, and the Virginia House of Delegates passed, a bill of attainder targeting a man accused of offenses including treason, murder, and arson. 2 THOMAS JEFFERSON, THE PAPERS OF THOMAS JEFFERSON 189-91 (Julian P. Boyd ed., Princeton Univ. Press 2018).

28. Nixon v. Adm'r of General Servs., 433 U.S. 425, 429 (1977).

29. *ArtI.S9.C3.2 Bills of Attainder Doctrine*, CONSTITUTION ANNOTATED, https://constitution.congress.gov/browse/essay/artI-S9-C3-2/ALDE_00013187/.

backdrop of ever-increasing economic and political tensions between the U.S. and the PRC. Interestingly, even though both countries have differing geopolitical interests, both economies remain undeniably intertwined, including through cyberspace where billions of bytes of information transit the fiber optic cables linking both countries every second. Accordingly, one must understand the current TikTok situation against the backdrop of broader explosion of personal data processing and data transfers which now underlie much of the global economy.[30]

This change in the economic order—relying on flows of data just as much as flows of goods—has grown alongside another fundamental development. Just as the internet disrupted nearly every industry, so too has it disrupted the work of intelligence and national security professionals. Unlike the Cold War, where difficult-to-acquire covert information reigned supreme, the internet and the rise of publicly available data sources has inverted the practice of intelligence—by some estimates, eighty percent of intelligence information is derived from "open source" or OSINT."[31] Under these conditions, social media applications are quite the treasure trove for foreign government security agencies.

While social media companies like TikTok have garnered the most recent attention, other PRC-based companies have also faced scrutiny in the U.S.. Recent legal scholarship states:

> In 2018, the U.S. Intelligence community warned the public at large (rather than merely the private sector) that Huawei and ZTE presented a threat not merely because of traditional cyber foreign economic collection of national security information but because of their wider, more general collection of quotidian U.S. person information on behalf of the Chinese Communist Party.[32]

Nevertheless, social media applications raise their own specific concerns because even though consumers "give continued assent to data processing in these circumstances, begrudgingly making more of their data available despite increasing general distrust of social media platforms: these platforms are simply too practical to quit."[33]

Much ink has been spilled over TikTok's data collection practices, including the prospect of a TikTok US Data Security subsidiary, referred

30. Horowitz & Check, *supra* note 3, at 81.
31. *Id.* at 81-82.
32. *Id.* at 85.
33. *Id.*

to generally as "Project Texas."[34] TikTok collects an extremely comprehensive range of data on its users, which will likely persist regardless of whether one looks at TikTok in its current version or a hypothetical U.S.-specific version.[35] TikTok's own Terms of Service confirms the scope and scale of the bulk collection of the following types of data, which importantly includes biometric data.[36]

The scope of the data collection, aside from concerns about diffusion of PRC propaganda into the United States, animates the growing concerns over the app.

> TikTok's core value to users lies in its ability to transmit data like "text, images, video and audio," all of which constitute "bulk data" that . . . might be used by China "to train algorithms for facial and voice recognition" (and while the D.C. District Court used the word 'might,' the prediction soon came true). . . . TikTok's Terms of Service and Privacy Policy . . . allow TikTok to collect and share a user's information with the . . . People's Republic of China to respond to "government inquiries."[37]

Not only does TikTok collect expansive categories of data, but such data can also make its way directly into the hands of the PRC government.

C. The Legal Origins of TikTok Bans—The Trump Administration's Approach

Given the scope of data collection by TikTok, the Trump Administration began to focus on the app in 2019, culminating in the issuance of Executive Order 13942, citing concerns that the "automated collection of personal information, including internet browsing patterns, could enable the Chinese government to . . . . track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage."[38]

> Based on this assessment, the executive branch took two sets of actions. The first prohibited 'transactions' under IEEPA, which effectively would result in a ban on downloads and updates of the TikTok app within the United States. The second set of actions

34. Perault & Sacks, *supra* note 10.

35. *Cf. Id.* (In their otherwise comprehensive evaluation of Project Texas, Perault and Sacks do not report whether TikTok intended for the new subsidiary to change the amount or type of data collected from users).

36. Horowitz & Check, *supra* note 3, at 64.

37. *Id.* at 89 (internal citations omitted).

38. *Id.* at 86 (internal citations omitted).

> focused on the use of the foreign investment review process managed by CFIUS to ensure that Bytedance, another Chinese tech company with close ties to the Chinese Communist Party, would divest itself of its ownership interest in TikTok, allowing some other company that did not pose the same national security concerns to purchase ByteDance's stake.[39]

Soon thereafter, a series of district court decisions overturned President Trump's ban of TikTok, finding that the ban exceeded the jurisdictional scope of IEEPA.[40] To summarize, these courts concluded that because TikTok is a social media application, its contents were "informational materials" or "personal communications which do[] not involve anything of value" that fell outside the President's power to ban transactions under IEEPA.[41] This charitably characterized reasoning fell short in significant ways and disposed of two key fundamental issues in a few lightly cited paragraphs. This case law, which remains valid as of this writing, limits the U.S. government of the use of IEEPA to regulate cross-border data flows in the interest of national security.[42] Other regulatory frameworks, such as reviews by the Committee on Foreign Investment in the United States (CFIUS) or Federal Trade Commission enforcement, have major gaps.[43] For now, Bytedance's purchase of Musical.ly (now TikTok) remains under CFIUS review, and the outcome appears uncertain.[44]

Unsurprisingly, many state governments have thus banned TikTok from their own government networks and devices. These states include: Alabama, Georgia, Idaho, New Hampshire, North Dakota, Utah, Texas, Maryland, South Dakota, South Carolina, and Nebraska.[45] Many states have also taken action to investigate TikTok's effects on the American public based on non-security related concerns as well. More than forty state attorneys general have launched a bipartisan effort to examine TikTok's mental health impacts on children and teenagers.[46] With the

39. *Id.*
40. *Id.* at 92-93.
41. *Id.* at 93.
42. *Id.* at 105.
43. *Id.* at 110.
44. Perault & Sacks, *supra* note 10.
45. Giulia Hayward, *Virginia Joins Several Other States in Banning TikTok on Government Devices*, NPR (Dec. 17, 2022, 9:56 AM), https://www.npr.org/2022/12/15/1142828852/tiktok-senate-federal-ban-state-agency-governors [https://perma.cc/B2AP-V3YX].
46. Press Release, Governor Glenn Youngkin Bans TikTok and WeChat on State Devices and State-Run Wireless Networks (Dec. 16, 2022), https://www.governor.virginia.gov/newsroom/news-releases/2022/december/name-948259-en.html [https://perma.cc/Q5PA-Q2NT].

prospect of federal legislative action to ban TikTok, either in whole or from government networks and devices, this article now looks to apply bill of attainder jurisprudence to such legislative and executive actions.[47]

III. BILLS OF ATTAINDER IN AN AGE OF CYBERSECURITY AND INTELLIGENCE CHALLENGES: *KASPERSKY LABS V. CISA* AND NATIONAL SECURITY-BASED RESTRICTIONS ON SOFTWARE

Before TikTok, there was Kaspersky Labs. In 2017, the Russian-based Kaspersky Lab antivirus software became subject to a Binding Operational Directive 17-01 (BOD) issued by the Department of Homeland Security (DHS) that directed all federal government departments and agencies to remove the antivirus software from their networks.[48] Like TikTok, the government had grown concerned about the possibility that a foreign-owned technology company, this time an antivirus software, could allow to foreign governments to access important systems and steal sensitive information.[49] Congress soon codified BOD 17-01, making the government-wide ban a permanent legal requirement and not merely an executive action. Kaspersky brought a lawsuit challenging both the BOD and the enacted law, claiming the latter was a bill of attainder. On review, the D.C. Circuit Court of Appeals resoundingly concluded that the laws did not violate the Bill of Attainder Clause.

A. Why Legislative Bans on Kaspersky Lab Software Were Not a Bill of Attainder

To reiterate, bills of attainder have three major components worth recounting here in for the specific application regarding Kaspersky Labs. First, bills of attainder must pertain to a *specific* individual, or group of individuals, and—for now—this includes corporations and other legal entities.[50] Second, the bill must impose a "punishment," for which the Supreme Court's *Nixon* decision articulated a three-part examination of whether the contents of the bill fit within the historical, functional, and

47. *Id.*

48. Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec., 909 F.3d 446, 451 (D.C. Cir. 2018). The Acting Secretary invoked "her statutory authority to issue directives 'for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk' . . . ." *Id.* (quoting 44 U.S.C. § 3552(b)(1)).

49. *Id.*

50. Cummings v. Missouri, 71 U.S. 277, 296-97 (1866) ("To be obnoxious as bills of attainder, the provisions must operate against some particular delinquent, or specified class of delinquents, and not against the whole community.").

motivational meanings of punishment. Lastly, such punishment must be levied without the benefit of judicial fact-finding or judicial review.[51]

On the first criterion, the task of the *Kaspersky* court was easy: Congress passed legislation specifically naming Kaspersky Labs.[52] The statute ordered the federal government to remove Kaspersky products from government systems and restricted any further procurement of such products in the future.[53]

Kaspersky Labs' bill of attainder challenge encountered difficulties in the second prong. While courts have expanded the scope of the Clause to cover harms beyond imprisonment, execution, and loss of title, not all burdens constitute a punishment.[54] On the functional part of the punishment test, reviewing courts typically ask whether the burden resulting from the legislation is the "means to an end or an end in and of itself."[55] If there is no other extrinsic goal of the "burden," for example, the ordered removal of Kaspersky software from government systems, the more such a burden looks like punishment. Courts conduct this analysis by determining whether there is a sufficient degree of connection between the burden imposed and the legitimate "non-punitive" interest of the government. Courts differ over the standard for such connection, with some requiring only a "rational basis" between the burden and its non-punitive interests, while other courts seek a higher "clear and convincing" standard. In *Kaspersky,* the non-punitive interest in the "security of the federal government's information systems" satisfied both the higher and lower standards given that unauthorized access would jeopardize "extremely important strategic national assets."[56] On this functional factor alone, the ban on Kaspersky products passed muster under the Bill of Attainder Clause—the need to protect government systems from compromise and data from exfiltration by a highly sophisticated foreign government supplies a convincing non-punitive purpose.[57] The D.C.

51. *Id.* at 297.

52. Pub. L. No. 115-91, § 1634, 131 Stat. 1283, 1739-40 (2017).

53. *Id.*

54. Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec., 909 F.3d 446, 455 (D.C. Cir. 2018).

55. *Id.*

56. *Id.* at 457 (internal citations omitted).

57. *Id.* ("With or without Kaspersky's willing cooperation, explained the experts, the Russian government could use Kaspersky products as a backdoor into federal information systems. Then, having gained privileged and undetected access, Russia could make all manner of mischief. The Acting Secretary of Homeland Security apparently agreed with these warnings. So Congress, after hearing all of this information, decided to disallow federal use of Kaspersky hardware, software, and services.").

Circuit appeared hesitant to second guess Congressional judgment or entertain Kaspersky's proposed alternatives. "At the end of the day, the functional test does not require that Congress precisely calibrate the burdens it imposes to the goals it seeks to further or to the threats it seeks to mitigate."[58]

Failing on the functional test is more or less the end of the road, but a brief consideration of historical and motivational tests may help examine proposed bans on TikTok.[59] The D.C. Circuit examined the ban on Kaspersky products and struggled to find how such a ban would constitute one of the historical types of punishment, which ranged from the traditional execution and imprisonment to the more modern loss of employment.[60] It is worth noting here that loss of employment may be within previous jurisprudence from the Reconstruction era, but arguments that employment restrictions would violate the Clause have no clear constitutional basis and have no clear basis in English constitutional law, at least according to Blackstone's Commentaries on the Laws of England.[61] The D.C. Circuit remained unconvinced by Kaspersky's arguments of corporate harm and reputational loss, likening the ban to "run of the mill business regulations."[62] Ultimately, whether under an eighteenth or twenty-first century conception of punishment, the D.C. Circuit concluded that banning Kaspersky was not even a "close" case.[63]

The motivational test seems to be surplus. Passing the functional test, let alone the historical test, ensures the validity of the legislation because failing the motivational test by itself is "not determinative" absent clear congressional punitive intentions.[64] Proving such intent requires more than pointing to a few anodyne statements by one Senator, as Kaspersky tried to do.[65] Neither the *Kaspersky* decision nor any of the

58. *Id.* at 460.

59. *Id.*

60. *Id.* at 461-63.

61. Blackstone's Commentaries, Book 4, Ch. 29, *Lillian Goldman Law Library*, https://avalon.law.yale.edu/18th_century/blackstone_bk4ch29.asp [https://perma.cc/AMM8-AZKW] ("The confequences of attainder are forfeiture, and corruption of blood.") (sic).

62. Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec., 909 F.3d at 462.

63. *Id.* at 460 ("Although we cannot rule out the possibility that a persuasive showing on the historical or motivational tests could overcome a challenger's failure to raise a suspicion of punitiveness under the functional test, this, as we are about to explain, is not such a case—indeed, not even close.").

64. *Id.* at 463.

65. *Id.* at 463-64.

cases it cited on this point seems to conclusively demonstrate what exactly would constitute "indicia of punitive intent."[66]

Before considering how a TikTok ban might fare under the Bill of Attainder Clause, it is worth remembering that the robust judicial review—by both a district and appellate court—points against the third component of impermissible attainder bills. Because Bills of Attainder by their very nature impose punishment *without* independent judicial review, the mere fact that Kaspersky could obtain substantive constitutional review on the merits shows that even punitive bills might not be bills of attainder because of the seeming inevitability of judicial review of a wide range of government actions.[67]

B. Applying Kaspersky *to Government Bans on TikTok*

This Article examines the *Kaspersky* decision in such depth because of its clear similarities to TikTok and other technology companies operating from geopolitically sensitive countries.[68] With a solid understanding of recent bill of attainder jurisprudence in the relatively narrow sense of "bans" on certain products and companies for the federal government, this Article now examines the several different kinds of proposed bans on TikTok.

The first two types of "bans" appear well-suited to pass muster under the precedent set forth by *Kaspersky* and *Huawei*. These bans only prohibit the use or installation of TikTok on government devices. Some bans, particularly those arising at the state level, originated as an administrative action taken by a jurisdiction's chief executive.[69] Of course, state constitutions contain their own bill of attainder provisions, notwithstanding the Constitution's own prohibition on attainders passed by state legislatures.[70] Less certain, however, is the applicability of bill of attainder doctrine to acts by the Executive.[71] For example, one commentator writes: "Despite substantial development of the bill of attainder doctrine, the Supreme Court has not resolved the preliminary

66. Kennedy v. Mendoza-Martinez, 372 U.S. 144, 209 (1963).

67. *Kaspersky*, 909 F.3d at 464-65.

68. Two years after the *Kaspersky* decision, a district court in Texas evaluated whether a Congressional ban on Huawei (a Chinese telecommunications company) constituted a bill of attainder. Relying heavily on *Kaspersky*, the court found that the Huawei ban passed all three tests, even with a few sharp statements from legislators. Huawei Techs. USA, Inc. v. United States, 440 F. Supp. 3d 607, 650 (E.D. Tex. 2020).

69. *See* Press Release, Governor Glenn Youngkin Bans TikTok and WeChat on State Devices and State-Run Wireless Networks, *supra* note 48.

70. U.S. CONST. art. I, § 10.

71. Cavaliere, *supra* note 17, at 158.

issue of whether the Bill of Attainder Clauses apply to executive and administrative action."[72] Administrative bans using executive power seem to be similar to the issuance of a "binding operational directive" as in *Kaspersky v. DHS*. When governors or Presidents use their statutorily delegated or inherent powers to regulate their branch of government, such matters would seem to pass the functional test of punishment under bill of attainder jurisprudence.[73] Indeed, if the Executive determines that it is in the interests of the government—whether on security grounds, productivity, or some other legitimate purpose—striking down device-level bans on TikTok would seemingly infringe on the separation of powers, which is one of the primary goals of the Bill of Attainder Clause in the first place.[74] Such an intrusion by a court to set aside an administrative ban seems particularly radical because of the lack of punitive intent and scope—TikTok can still conduct business, just not on government devices.[75] In this regard, these administrative device-level bans appear like ordinary government rules of conduct for IT devices, such as prohibitions on accessing gambling or pornographic websites.

For similar reasons and given the precedent in *Kaspersky*, a legislatively enacted ban on TikTok from government devices would fare similarly to administrative bans. Unless challengers to a TikTok ban could distinguish the app from Kaspersky antivirus software on some factual grounds, bans tailored to government networks and devices would likely survive challenge under the Bill of Attainder Clause.

C. Banning TikTok Nationwide

The prospect of a general national ban of TikTok looks most like a bill of attainder.[76] Indeed, such a ban would exceed even the scope of the subject legislation in *Kaspersky*, which importantly applied only to the federal government's use of Kaspersky products and not use by businesses and the public writ large.[77] As of this writing, such a ban looks possible with the Biden Administration reportedly warning TikTok's

72. *Id.* (internal citations omitted).
73. *Id.* at 159.
74. *Id.* at 159-60.
75. *Id.* at 161.
76. *Id.* at 155.
77. These may be distinctions without major differences. Before it was restricted from government devices, Kaspersky did a great deal of business with the federal government. Even if not a majority of revenue, the federal government and closely affiliated contractors made up a significant portion of revenue. TikTok, on the other hand, does not provide institutionally focused services like antivirus software or cyber-threat intelligence. Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec., 909 F.3d 446, 459 (D.C. Cir. 2018).

owners in the PRC that only divestment may forestall an outright legislative ban.[78]

But if TikTok calls the administration's bluff and waits for Congress to pass legislation, would such legislation violate the Bill of Attainder Clause? Would barring a corporation from transacting business in the United States constitute a legislatively imposed punishment?

Previous legal precedent dating to the Civil War might tempt proponents of TikTok or skeptics of U.S. security interests into trying their luck. But such an attempt would likely be in vain, due to the functional and non-punitive nature of such legislation. Opponents of a ban might draw comparisons to *Cummings v. Missouri*, a Supreme Court opinion that struck down a state law that required loyalty oaths from clergy and officeholders after the Civil War, ensuring that none within the class of credentialed persons had given aid or support to the Confederates. They may also compare a TikTok ban to *Lovett v. United States*, which invalidated an appropriations act that deprived "subversive" federal employees of a salary.[79] Both Courts, decades apart, reached the same conclusion—that even minor restrictions on the ability to earn income based on legislative disapproval of political activities found to be harmful to the national interest (former Confederates and sympathizers and communists). Surely then, TikTok might incorrectly argue that a law prohibiting its operation in the United States must also be a bill of attainder?

Looking to *Lovett* and *Cummings,* as opposed to more useful precedent in *Kaspersky*, misses major differences. First of all, *Lovett* and *Cummings* belong to a different era of bill of attainder jurisprudence, an era of major expansion beyond the traditional (perhaps even the Framers') understanding of such laws.[80] Accordingly, the three-part test in *Nixon* is more likely to predict how a TikTok ban might fare, as opposed to the amorphous, unformalized approaches of earlier attainder cases.

Second, *Lovett* and *Cummings* involved laws that affected natural persons, specifically US citizens. While there is some case law that indicates that corporations might enjoy protection under the Clause, there has been little precedent examining foreign companies as part of this

78. John D. McKinnon, *U.S. Threatens Ban if TikTok's Chinese Owners Don't Sell Stakes*, W.S.J. (Mar. 15, 2023, 6:45 PM), https://www.wsj.com/articles/u-s-threatens-to-ban-tiktok-if-chinese-founder-doesnt-sell-ownership-stake-36d7295c. For an analysis on the limitations of a CFIUS-based approach to addressing the data security risks posed by TikTok and social media applications of similar origin, see Horowitz & Check, *supra* note 3.

79. United States v. Lovett, 328 U.S. 303, 310-11 (1946).

80. *Id.* at 309-11.

jurisprudence. Under *Kaspersky*, for example, the D.C. Circuit suggests that it was not even a "close" case—accordingly, foreign corporations may struggle to demonstrate that they fall within the class of persons protected by the Clause.

Third, the interests of the United States appear more pressing for a TikTok ban than either *Lovett* or *Cummings*. In *Lovett*, the appropriation act at issue targeted a handful of federal employees, described as "irresponsible" and "crackpots," for conducting nondescript "subversive" activities, but most likely because of their links to Communist organizations.[81] Even though Congress passed the law in 1943, little in the *Lovett* decision indicates that there were dire security concerns at play, appearing more to play on notions of "fitness" for government service.[82] So too is the case in *Cummings*, handed down years after the end of the Civil War when most in American society were looking toward reconciliation, reconstruction, and restitution for enslaved persons. In both these instances, the judicial record shows that either the storm had passed or had not really been a storm at all. As described above in Section 3(a), the severity of the national security threat weighs in favor of the "legitimate non-punitive" interest of the government. In this instance, plenty of evidence suggests that TikTok poses significant threats to a number of government interests, such as the threat of misinformation, data theft, espionage, and other dangers. Unlike *Lovett* and *Cummings*, the storm has not yet passed. And that may significantly weigh against finding that a TikTok ban would constitute punishment.

Fourth, the notion of banning TikTok from conducting business in the United States strains historical conceptions of punishment. In *Cummings*, failure to take a loyalty oath could result in criminal sanction even if relatively mild (especially when compared to drawing and quartering!). In *Lovett*, the prospect of prohibiting a federal employee from ever drawing a salary for his labors looks akin to servitude and harkens back to the disinheritance and removal of titles from attainted persons. Banning TikTok from the marketplace seems different from any of these historical precedents. How might TikTok distinguish such a ban from any wide range of restrictions on business transactions, such as preventing the likes of dictators and terrorists from accessing the U.S. financial system via Office of Financial Asset Control (OFAC) or a dry county's refusal to allow a distiller to flog her wares within county lines? Both types of business restrictions frequently apply without the benefit of

81. *Id.* at 308-09.
82. *Id.* at 310-11.

bespoke judicial review and even though bills of attainder typically apply with specificity, both types of restrictions apply to clearly-defined groups of regulated persons, even if thousands strong.

Opponents of a TikTok ban might convincingly argue that such a ban may fail the motivational test of punishment. After all, the prospect of competition with the PRC and heightened tension could lead one to conclude—even if wrongly—that a legislative ban is driven by hatred and bigotry against China. News media certainly has displayed strong rhetoric on these matters. But this puts aside the hundreds and thousands of Chinese companies that transact business in the United States every day.[83] Nevertheless, perhaps this motivational argument could find a sympathetic ear in the court of public opinion. Even so, as demonstrated above, even showing a motivation to punish may not be enough if the legislation in question does not function as punishment or comport with historical understandings of punishment.

IV. CONCLUSION—BANS ON TIKTOK ARE NOT BILLS OF ATTAINDER

Specifically barring a multi-billion-dollar social media company, even if necessary to guard against severe national security concerns, seems unprecedented. In such uncharted waters, it may be tempting to look at history as a guide. Ultimately, a bill of attainder challenge to a legislative TikTok ban will rest on whether a court believes that such legislation has a legitimate, non-punitive purpose. As shown above, a TikTok ban, while drastic, does not look like any of the historical examples of punishment. Such a move, if it comes, would come after years of deliberation, fact-gathering, and analysis, and after multiple IEEPA and CFIUS reviews. Whether courts will believe this body of evidence will remain to be seen. But, where the Executive and Congress have acted in concert before to protect networks and data from adversarial foreign influence, courts have determined that even drastic action was not a bill of attainder.

83. Notably, this is not just the U.S. Several months ago, India banned TikTok, cutting off millions of users, citing national sovereignty. Paayal Zaveri, *Why India Banned TikTok and What the US Can Learn, as Pressure Mounts for Biden to Follow Suit*, BUS. INSIDER (Jan. 8, 2023, 1:31 PM), https://www.scmp.com/news/asia/article/3205994/why-india-banned-tiktok-and-what-us-can-learn-pressure-mounts-biden-follow-suit.