THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KASPERSKY LAB, INC.; and KASPERSKY LABS LIMITED,	)	
Plaintiffs,	)	
v.	)	Civ. No. 18-325 (CKK)
UNITED STATES OF AMERICA	)	
Defendant.	)	

DEFENDANT'S MOTION TO DISMISS

Pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure, the Defendant respectfully moves to dismiss the Complaint in this action, which challenges Sections 1634(a) & (b) of the National Defense Authorization Act for Fiscal Year 2018, Pub. Law No. 115-91, 131 Stat. 1283 (2017) (the "NDAA"), as an unconstitutional bill of attainder. For the reasons explained in the accompanying memorandum of law, Plaintiffs have not plausibly alleged that the challenged provisions offend the Bill of Attainder Clause, and this suit should be dismissed for failing to state a claim upon which relief can be granted.

Dated: March 26, 2018

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General

ERIC R. WOMACK
DIANE KELLEHER
Assistant Branch Directors
Civil Division

/s/ Samuel M. Singer
SAMUEL M SINGER (D.C. Bar 1014022)
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave, NW
Washington, D.C. 20530
Telephone: (202) 616-8014
Fax: (202) 616-8470

Attorneys for Defendant

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KASPERSKY LAB, INC.; and KASPERSKY LABS LIMITED,	)	
Plaintiffs,	)	
v.	)	Civ. No. 18-325 (CKK)
UNITED STATES OF AMERICA	)	
Defendant.	)	

MEMORANDUM IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statues

Regulations

INTRODUCTION

Kaspersky Lab, Inc. and its affiliate, Kaspersky Labs Ltd. (collectively, "Kaspersky"), challenge Sections 1634(a) & (b) of the National Defense Authorization Act for Fiscal Year 2018, Pub. Law No. 115-91, 131 Stat. 1283 (2017) (the "NDAA"), claiming the provisions violate the Constitution's Bill of Attainder Clause. Section 1634(a) prohibits the federal government from using products or services developed or provided by Kaspersky, and Section 1634(b) requires that any such use stop by October 1 of this year. Section 1634 was enacted in response to widespread concerns among lawmakers and intelligence officials over security risks posed by the government's use of Kaspersky products and services.

Kaspersky claims that Section 1634 works an unlawful attainder by singling the company out for legislative "punishment," a prohibition that has been historically connected with laws that single out individuals or groups for imprisonment, banishment, confiscation of property, or exclusion from a particular vocation due to disloyalty. *Nixon v. Adm'r of Gen. Servs.,* 433 U.S. 425, 468 (1977). The company faults Congress for not legislating more broadly, and dismisses the security concerns underlying this statute as "vague and inflammatory" allegations by a single Senator looking "to be seen as reacting to the apparent Russian interference in the 2016 presidential elections." Compl., 1:18-cv-00325 ¶ 3, Dkt No. 1. Those allegations, Kaspersky asserts, have not been "test[ed]" or "substantiated" by congressional "fact-finding" (a term it uses repeatedly in the complaint but never defines). *Id.* ¶¶ 38, 41, 42.

Kaspersky's bill of attainder claim should be dismissed. Section 1634 bears no resemblance to historically forbidden attainders, and the provision is neither a determination of guilt nor a condemnation of Kaspersky's past conduct as meriting punishment. It reflects, rather, the response of Congress and the President to an entirely legitimate national security concern about the

government's current and future use of products or services that could make U.S. networks vulnerable to Russian cyber intrusion. And Kaspersky's suggestion that Congress failed to "test[]" its concerns before "hastily" adopting Section 1634 is baffling. Congress is not required to "test" anything before it legislates, but even if it were, this statute's passage followed *months* of congressional investigation and information-gathering into the government's use of Kaspersky products and services, and came on the heels of actions the executive branch took to address similar concerns. By the time this legislation reached the floor, there was broad agreement among lawmakers and cybersecurity officials in the executive branch that the security risks posed by the use of Kaspersky products and services were intolerably high, and strong bipartisan support for taking preventive action against those risks.

Kaspersky's claim misapprehends the scope of the constitutional prohibition on bills of attainder. The Supreme Court has made clear that Congress can impose economic burdens on named parties without offending the Bill of Attainder Clause, and has rejected claims indistinguishable from the ones Kaspersky presses here. The touchstone of the Bill of Attainder analysis is not whether a party has been singled out in legislation in any way, but whether it has been specifically singled out for *punishment*. As long as a statute is furthering a non-punitive end, Congress may identify the object of legislation with whatever specificity it sees fit.

Kaspersky's contrary argument—which does not consider the seriousness of the threat, the quantum of proof underlying the threat, or the uniformity of expert opinion that the threat requires decisive governmental action—would leave Congress powerless to directly address threats to national security whenever the person or entity posing that threat is specifically identifiable. No court has ever reached that conclusion, no doubt because the Bill of Attainder Clause has never been understood to impose such an arbitrary constraint on the ability of Congress to legislate in

defense of national security. The provision at issue is entirely lawful. This Court should decline to invalidate it.

BACKGROUND[1]

Kaspersky provides an account of the congressional record—deriding it as "thread-bare" and bereft of "fact-finding"—that reflects a warped view of the legislative process and relevant facts. The complaint traces the history of Section 1634 from introduction to enactment, but leaves out virtually everything Congress did in the months leading up to its passage, including congressional hearings, congressional briefings (both public and classified), and congressional requests for information. The complaint also omits Kaspersky-related actions taken by the executive branch, which, while outside the legislative process, nonetheless provide crucial context for understanding the purpose and motivation behind the statute at issue. Given the centrality of congressional purpose to determining whether the provision at issue is a bill of attainder—whether it is a "punishment" for past acts or a prophylactic measure to protect the United States—the context of its passage is critical.

I. Congressional and Regulatory Activity Leading Up to the Passage of Section 1634

Section 1634 was enacted against a backdrop of widespread concern among lawmakers and intelligence officials about the presence of Kaspersky products on U.S. information systems. In the months leading up to Section 1634's enactment, various congressional committees sought information about the Kaspersky threat from witnesses, experts, and government officials.

An early public indication that lawmakers were concerned came in March 2017, during a Senate hearing on Russian cyber activities. Citing a "long history" of open-source reporting

[1] "[C]ourts may take judicial notice of matters of a general public nature . . . without converting the motion to dismiss into one for summary judgment." *Kounty v. Martin*, 530 F.Supp.2d 84, 89 (D.D.C. 2007) (citation omitted).

connecting Kaspersky to Russian security services, Senator Marco Rubio asked a panel of cybersecurity experts if they would feel comfortable using Kaspersky products on their own devices.[2] The following month, the U.S. Senate Select Committee on Intelligence (Senate Intelligence Committee) asked the Director of National Intelligence and the Attorney General to investigate Kaspersky's ties to the Russian government,[3] and two House members introduced a bill describing Kaspersky as "a company suspected of having ties with the Russian intelligence services and later caught up in a Russian espionage investigation."[4] In May, six U.S. intelligence directors, including the directors of the Central Intelligence Agency and the National Security Agency, told the Senate Intelligence Committee that they would not be comfortable using Kaspersky products on their computers. NSA Director Mike Rogers said he was "personally involved" in monitoring the Kaspersky issue, and CIA Director Mike Pompeo acknowledged that concerns about Kaspersky products "ha[d] risen to the director" level at CIA.[5]

Throughout the summer of 2017, lawmakers continued to raise questions about Kaspersky—first during a U.S. House Committee on Science, Space, and Technology (House Science

[2] *Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Panel II*, 115th Cong. 40 (March 30, 2017), https://www.gpo.gov/fdsys/pkg/CHRG-115shrg25998/pdf/CHRG-115shrg25998.pdf

[3] *See Bolstering the Government's Cybersecurity: Assessing the Risks of Kaspersky Lab Products to the Federal Government*, H. Comm. on Science, Space, and Technology, 115th Cong. (2017), https://democrats-science.house.gov/sites/democrats.science.house.gov/files/documents/10.25.17%20RM%20Beyer%20Opening%20Statemenet%20Kaspersky%20Lab%20Products%20Hearing_0.pdf

[4] H.R. Con. Res. 47, 115th Cong. (2017)

[5] *Hearing on Worldwide Threats Before the S. Select Comm. on Intelligence*, 115th Cong. (May 11, 2017), 1:11, https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-hearing-0

Committee) hearing on the lessons learned from the WannaCry attacks,[6] then during a Senate Intelligence Committee hearing on Russian interference in the 2016 elections,[7] and again during a July hearing before the U.S. House Committee on Small Business.[8]

In the ensuing months, lawmakers and executive branch agencies began taking more concrete steps to address concerns about Kaspersky products. In June, Senator Tom Cotton proposed an amendment to an Iran sanctions bill that called for the imposition of economic sanctions against Kaspersky employees in Russia.[9] In July, Representative Lamar Smith, Chairman of the House Science Committee, sent a letter to various federal agencies requesting information about their use of Kaspersky software and expressing concern that the company "is susceptible to manipulation by the Russian government."[10] Around the same time, the General Services Administration (GSA) started removing Kaspersky from the agency's lists of pre-approved vendors for contracts that cover information technology products and services and digital photographic equipment. GSA said

[6] *Bolstering the Government's Cybersecurity: Lessons Learned from Wannacry*, 115th Cong. (June 15, 2017), https://democrats-science.house.gov/legislation/hearings/bolstering-government-s-cybersecurity-lessons-learned-wannacry

[7] *Russian Interference in the 2016 U.S. Elections*, 115th Cong. (June 21, 2017), https://www.intelligence.senate.gov/sites/default/files/hearings/Russian%20Interference%20in%20the%202016%20U.S.%20Elections%20S.%20Hrg.%20115-92.pdf

[8] *Help or Hindrance? A Review of SBA's Office of the Chief Information Officer*, 115th Cong. (July 12, 2017), https://www.gpo.gov/fdsys/pkg/CHRG-115hhrg26248/pdf/CHRG-115hhrg26248.pdf

[9] 163 Cong. Rec. S3492 (2017), https://www.gpo.gov/fdsys/pkg/CREC-2017-06-14/pdf/CREC-2017-06-14-pt1-PgS3491-2.pdf

[10] Letter from Chairman Lamar Smith, July 27, 2017, at 1 https://science.house.gov/sites/republicans.science.house.gov/files/documents/072717%20Smith-Agencies%20-%20Kaspersky.pdf

its action was taken "after review and careful consideration," consistent with its priority "to ensure the integrity and security of U.S. government systems and networks."[11]

In September 2017, the Department of Homeland Security (DHS) issued Binding Operational Directive (BOD) 17-01, which directed federal agencies to identify any use of Kaspersky-branded products within 30 days, provide a plan to remove them within 60 days, and, unless directed otherwise by DHS based on information it learned during an administrative review period, to begin removing the products at 90 days. Acting Secretary Elaine Duke issued the directive after determining that the presence of Kaspersky products on federal information systems presents a "known or reasonably suspected threat, vulnerability, or risk" to federal information and information systems.[12]

In the days and weeks leading up to the passage of Section 1634, the House Science Committee held two hearings devoted exclusively to cybersecurity issues surrounding Kaspersky products. The first, an investigative hearing entitled "Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government,[13] examined "the risks associated with utilizing Kaspersky Lab products on federal government information technology systems . . . and the federal government's response to the concerns."[14] The second hearing examined the

[11] *See* Kaspersky Axed From Governmentwide Contracts, FCW, July 12, 2017, https://fcw.com/articles/2017/07/12/kaspersky-gsa-nasa-intel.aspx

[12] National Protection and Programs Directorate; Notification of Issuance of Binding Operational Directive 17-01 and Establishment of Procedures for Responses, 82 Fed. Reg. 43,782, 43,784 (Sept. 19, 2017).

[13] 163 Cong. Rec. D1125-01, https://science.house.gov/legislation/hearings/bolstering-government-s-cybersecurity-assessing-risk-kaspersky-lab-products

[14] Hearing Charter, U.S. House of Rep. Committee on Science, Space, and Technology, October 19, 2017, https://congressional.proquest.com/congressional/result/pqpresultpage.gispdfhitspanel.pdflink/$2fapp-bin$2fgis-congresearch$2f5$2fc$2f4$2f9$2fcmp-2017-tec-

federal government's implementation of the BOD.[15] In between these hearings, the House Science Committee issued a committee report on an unrelated bill citing the risks presented by Kaspersky products as one of several reasons why Congress must "take aggressive actions to support and assure a fundamentally different approach to cybersecurity that addresses the magnitude and nature of [the] growing threats."[16]

All told, by the time Section 1634 was enacted, Congress had spent months investigating and gathering information on the Kaspersky threat. At least five committees heard testimony on the subject, and two federal agencies had taken government-wide actions. This, of course, reflects only what happened on the public record. Senator Jeanne Shaheen has made it clear that she considered classified information as part of the information-gathering process, *see* Compl., Ex. C (Shaheen Op-Ed), and press accounts reveal that at least two committees received classified briefings on the Kaspersky matter.[17]

0033_from_1_to_1.pdf/entitlementkeys=1234%7Capp-gis%7Ccongresearch%7Ccmp-2017-tec-0033

[15] Hearing Charter, U.S. House of Representatives Committee on Science, Space, and Technology, October 19, 2017, https://congressional.proquest.com/profiles/gis/result/pqpresultpage.gispdfhitspanel.pdflink/$2fapp-bin$2fgis-congresearch$2ff$2f3$2f6$2fb$2fcmp-2017-tec-0039_from_1_to_1.pdf/entitlementkeys=1234%7Capp-gis%7Ccongresearch%7Ccmp-2017-tec-0039

[16] Committee Report 115-376 accompanying H.R. 1224, October 31, 2017, at 4, https://www.congress.gov/115/crpt/hrpt376/CRPT-115hrpt376.pdf. The Senate Armed Services Committee and the House Homeland Security Committee also heard testimony relating to Kaspersky in October 2017. *See Roles and Responsibilities for Defending the Nation from Cyber Attack*, Senate Armed Services Committee, 115th Cong. (October 19, 2017), https://www.armed-services.senate.gov/hearings/17-10-19-roles-and-responsibilities-for-defending-the-nation-from-cyber-attack; *Examining DHS's Cybersecurity Mission*¸ House Committee on Homeland Security, 115th Cong. (October 3, 2017), https://www.dhs.gov/news/2017/10/03/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity-and

[17] *Classified Senate Briefing Expands to Include Russian Cyber Firm under FBI Scrutiny*, ABC News, May 24, 2017, http://abcnews.go.com/Politics/classified-senate-briefing-expands-include-russian-cyber-firm/story?id=47619783; House Panel Receives Classified Briefing on Kaspersky,

II. Section 1634 of the National Defense Authorization Act

Kaspersky's account of the Section 1634's legislative history, with its focus on Senator Shaheen, ignores the role played by the U.S. Senate Armed Services Committee and its Chairman, Senator John McCain, whose efforts in advancing the provision proved instrumental to its enactment. In June 2017, during a classified Senate Armed Services Committee markup of the Senate-originated version of the 2018 NDAA bill, Senator Shaheen introduced an amendment containing a narrower version of the Kaspersky ban that would have applied only to the Department of Defense (DOD). Compl. ¶ 26, Ex. A. Senator Shaheen's amendment was agreed to, and the bill, as amended, was reported out of committee by a unanimous vote of 27-0. An executive summary of the markup prepared by the committee lists the Shaheen amendment among various security-related measures intended to "counter[] Russian aggression" and describes it as a response to "reports that the Moscow-based company might be vulnerable to Russian government influence."[18]

The following month, when the House sent its version of the NDAA bill to the Senate for consideration, Chairman McCain proposed an amendment in the nature of a substitute (or a "substitute amendment") to the House bill that reflected the various provisions the committee reported out of the June markup, including the DOD-specific Kaspersky ban. Compl. ¶ 29, Ex. D. Senator Shaheen also filed an amendment to the House bill proposing to broaden the DOD-specific provision to the entire federal government. *Id*. ¶ 27, Ex. B. But Senator Shaheen's amendment was never put to a vote, because the broader provision was accepted by Chairman McCain and included

---

Bloomberg, September 26, 2017, https://www.bloomberg.com/news/articles/2017-09-26/house-panel-is-said-to-receive-classified-briefing-on-kaspersky

[18] NDAA FY 2018, U.S. Senate Armed Services Committee, at 9-10 https://www.armed-services.senate.gov/imo/media/doc/FY18%20NDAA%20Summary6.pdf

in his modified substitute amendment. Chairman McCain's modified substitute amendment was then *unanimously* approved by the Senate, and the final NDAA that was enacted into law thus included this broader Kaspersky ban. *Id*. ¶¶ 30, 33-35.

On December 12, 2017, the President signed the NDAA, including Section 1634, into law. Section 1634(a) prohibits federal agencies from using "any hardware, software, or services developed or provided, in whole or in part, by [Kaspersky]." The prohibition requires all agencies to have discontinued use of Kaspersky products and services by October 1, 2018, the first day of the new fiscal year. NDAA § 1634(b). In the meantime, Congress directed DOD, in consultation with various federal agencies, to "conduct a review of the procedures for removing suspect products or services from the information technology networks of the Federal Government," *id*. § 1634(c)(1), and submit a report to Congress addressing a host of topics, including a description of the "Government-wide authorities that may be used to prohibit, exclude, or prevent the use of suspect products or services on the information technology networks of the Federal Government." *Id.* § 1634(c).

DISCUSSION

I. The NDAA Ban Does Not Violate the Bill of Attainder Clause.

The U.S. Constitution provides that "[n]o Bill of Attainder . . . shall be passed" by Congress. Art. 1, §9, cl.3. The Bill of Attainder Clause preserves the separation of powers, *Siegel v. Lyng*, 851 F.2d 412, 416 (D.C. Cir. 1988), barring Congress from encroaching on the functions of the judiciary by "legislatively determin[ing] guilt and inflict[ing] punishment upon an identifiable individual without provision of the protections of a judicial trial," *Nixon*, 433 U.S. at 468. The Clause's scope is narrow: it "was not intended to serve as a variant of the equal protection doctrine," but rather as a prohibition on legislative punishment of particular targeted individuals. *Id.* at 471.

On this basis, the Supreme Court has invalidated only five statutes as bills of attainder since the founding: three post-Civil War statutes barring former supporters of the Confederacy from employment or access to the courts, *Cummings v. Missouri*, 71 U.S. (4 Wall.) 277 (1866); *Ex parte Garland*, 71 U.S. (4 Wall.) 333 (1866); *Pierce v. Carskadon*, 83 U.S. (16 Wall.) 234 (1872); and two Cold War-era laws barring "subversives" and Communists from various jobs, *United States v. Lovett*, 328 U.S. 303 (1946); *United States v. Brown*, 381 U.S. 437 (1965).

Under modern case law, a law constitutes a bill of attainder "if it (1) applies with specificity, and (2) imposes punishment." *BellSouth Corp. v. FCC*, 162 F.3d 683 (D.C. Cir. 1998) ("*BellSouth II*"). The element of specificity may be satisfied if the statute singles out a person or class by name or applies to "easily ascertainable members of a group." *Lovett*, 328 U.S. at 315. As the Supreme Court has made clear, however, specificity alone does not offend the Bill of Attainder Clause. *See Nixon*, 433 U.S. at 469-73. Rather, a law may be so specific as to create a "legitimate class of one" without amounting to a bill of attainder unless it also satisfies the "punishment" element of the analysis. *Id*. at 472.

With respect to punishment, the Supreme Court has distilled a three-part inquiry that reflects the limited scope of this constitutional restriction. To determine whether a statute constitutes legislative punishment, a court considers whether a statute (1) "falls within the historical meaning of legislative punishment;" (2) whether it "further[s] nonpunitive legislative purposes;" and (3) whether the legislative record "evinces a congressional intent to punish." *Selective Serv. Sys. v. Minn. Pub. Interest Research Grp.*, 468 U.S. 841, 852 (1984) (citation omitted). These three factors are considered as a whole, and "only the clearest proof could suffice to establish the unconstitutionality of a statute" on the basis of impermissible congressional motive alone.

Flemming v. Nestor, 363 U.S. 603, 617 (1960). Even assuming Kaspersky can demonstrate that Section 1634 satisfies the specificity requirement, it fails all three prongs of the punishment test.

A. The NDAA Ban Does Not Fit the Historical Definition of Punishment.

The Supreme Court has recognized that certain types of punishment are "so disproportionately severe and so inappropriate to nonpunitive ends that they unquestionably have been held to fall within the proscription of the [Bill of Attainder Clause]." *Nixon*, 433 U.S. at 473. "The classic example is death, but others include imprisonment, banishment, the punitive confiscation of property, and prohibition of designated individuals or groups from participation in specified employments or vocations." *Consol. Edison Co. of N.Y., Inc. v. Pataki*, 292 F.3d 338, 351 (2d Cir. 2002) (citations omitted). A common thread in all of these examples of historical punishment is the initial determination by the legislature of "guilt." *See De Veau v. Braisted*, 363 U.S. 144, 160 (1960) ("The distinguishing feature of a bill of attainder is the substitution of a legislative for a judicial determination of guilt.").

Section 1634 bears no resemblance to any of the traditional forms of punishment. Section 1634 does not execute, imprison, or banish Kaspersky, and the company cannot seriously contend that Congress's decision to prohibit use of its products constitutes a punitive confiscation of property. And to the extent Kaspersky intends to liken Section 1634, which it condemns as a "punitive debarment" (Compl. ¶ 39), to a legislative bar on employment, the analogy is foreclosed by D.C. Circuit precedent. *See BellSouth Corp. v. FCC*, 144 F.3d 58, 65 (D.C. Cir. 1998) ("*BellSouth I")* (refusing to equate statute imposing restrictions "on corporations seeking to engage in specific types of commercial activity" with "traditional employment debarments"). Indeed, Section 1634's prohibition differs in crucial respects from the lifetime employment bars the Supreme Court has placed within the scope of historically forbidden attainders.

First, a restriction on a company's ability to enter a specific line of business is categorically different from the permanent exclusion of an individual from an occupation. The Bill of Attainder Clause concerns "legislative interferences[] in cases affecting personal rights," *Brown*, 381 U.S. at 444 n.18, and the Supreme Court has been willing to extend the Clause only to those bars on employment in which the ban was used as "'a mode of punishment . . . against those legislatively branded as disloyal."' *Nixon*, 433 U.S. at 474; *see also Brown*, 381 U.S. at 453; *Lovett*, 328 U.S. at 314 (noting that the purpose of the statute at issue "clearly was to 'purge' the then existing and all future lists of Government employees of those whom Congress deemed guilty of 'subversive activities' and therefore 'unfit' to hold a federal job"). The statute in *Lovett*, for example, terminated the employment of three individuals who had devoted years of service to the government, and precluded them from all future government employment. 328 U.S. at 302. The Court declared that the "permanent proscription from any opportunity to serve the Government is punishment, and of a most severe type," and "is a type of punishment which Congress has only invoked for special types of odious and dangerous crimes." *Id.* at 316.

By contrast, the prohibition challenged here has nothing to do with employment, and it certainly does not expel any individuals from their chosen profession. Instead, it has the effect of restricting a company's ability to seek discretionary contracts from one of its many sources of revenue. Kaspersky retains the right to operate in the United States, including the right to develop, market, and sell its products and services to U.S. customers not covered by Section 1634. In Section 1634, Congress has simply determined that the government will no longer use the company's products or services. While this type of "line-of-business" restriction can be costly, the burden is nothing like the penalties that have traditionally marked forbidden attainders, and the

D.C. Circuit has rejected attempts to liken line-of-business restrictions to employment bars.[19] *BellSouth I*, 144 F.3d at 65; *see also Brown*, 381 U.S. at 444 (suggesting that line-of-business restrictions do not constitute unconstitutional bills of attainder). Indeed, as line-of-business restrictions go, Section 1634 is considerably less exacting than provisions that have withstood attainder challenges in the past. *See, e.g.*, *BellSouth I*, 144 F.3d at 65 (forbidding 20 named corporations, out of more than 1,300 local exchange carriers, from entering a trade or business on the same terms as others); *Fresno Rifle & Pistol Club, Inc. v. Van de Kamp*, 965 F.2d 723, 728 (9th Cir. 1992) (rejecting bill of attainder challenge to California statute that barred specific brands of assault weapons because "[t]he type of economic punishment about which [the weapons' manufacturers] complain is not of the type 'traditionally judged to be prohibited by the Bill of Attainder Clause"). Kaspersky's assertion that Section 1634 effects a "debarment"—a penalty commonly imposed on government contractors under federal suspension and debarment regulations—only weakens the analogy to historical punishment. *See BellSouth II*, 162 F.3d at 685 (refusing to find historical punishment where the requirements imposed by the challenged statute were "no different than numerous regulatory measures aimed at particular industries that have never been held to inflict punishment").

Second, unlike the employment bars struck down by the Supreme Court, Section 1634 focuses exclusively on prospective risk. The Supreme Court has recognized a "decisive distinction"

[19] Neither the Supreme Court nor the D.C. Circuit has held that the Bill of Attainder Clause applies to corporations, and the D.C. Circuit has recognized "that there are differences between a corporation and an individual" for the purposes of the bill of attainder analysis, and that "any analogy" to prior cases involving individuals "must necessarily take into account this difference." *BellSouth II*, 162 F.3d at 684-84; *ACORN v. United States*, 618 F.3d 125, 137 (2d Cir. 2010) ("In comparison to penalties levied against individuals, a temporary disqualification from funds or deprivation of property aimed at a corporation may be more an inconvenience than punishment."); *but see Consol. Edison*, 292 F.3d at 346-49 (concluding that the Clause protects corporations).

between statutes that impermissibly punish past action and those that permissibly regulate future conduct. *Am. Commc'ns Assn, C.I.O. v. Douds,* 339 U.S. 382, 413–14 (1950). "The question in each case where unpleasant consequences are [imposed] upon an individual for prior conduct, is whether the legislative aim was to punish that individual for past activity, or whether the restriction of the individual comes about as a relevant incident to a regulation of a present situation." *Flemming,* 363 U.S. at 614. In *Nixon,* for example, the Court held that Congress's singular focus on preserving Nixon's records, at the exclusion of other Presidents, did not offend the Bill of Attainder Clause, because "*only [Nixon's] materials demanded immediate attention*." 433 U.S. at 472 (emphasis added). Nixon, in other words, "constituted a legitimate class of one," giving Congress license "to proceed with dispatch with respect to his materials while accepting the status of his predecessors' papers and ordering the further consideration of generalized standards to govern his successors." *Id*.

That is precisely what happened here. Rather than exacting punishment on Kaspersky for past action, Congress focused on excluding what it perceived to be an immediate danger (Section 1634(a)), while seeking further consideration of generalized standards to govern the removal of suspect products in the future (Section 1634(c)). And as in *Nixon*, Congress singled out Kaspersky, at the exclusion of other contractors, because at that point in time Kaspersky "demanded immediate attention." *Id*.; *see supra,* Section I (collecting legislative materials reflecting members' concerns about the Kaspersky threat). It was perfectly reasonable for Congress, facing what it judged to be an urgent and entirely singular threat to federal information systems, to "proceed with dispatch" in barring the use of Kaspersky products and services, rather than enacting a general law and waiting months, if not years for more than one hundred individual agencies to independently arrive at the very national security judgment Congress had already made. *See BellSouth II*, 162 F.3d at

689-90 (statute singling out Bell Operating Companies (BOCs) was not an unlawful attainder because of the "unique infrastructure controlled by the BOCs" which allowed them to exercise monopoly power); *SeaRiver Maritime Fin. Holdings, Inc. v. Mineta*, 309 F.3d 662, 675 (9th Cir. 2002) (Congress's concern that the Exxon Valdez posed a greater risk of spillage than other oil tankers was sufficient to justify statute excluding the vessel from Prince William Sound).

B. The NDAA Ban Plainly Furthers the Non-Punitive Purpose of Protecting Federal Information Systems.

The functional definition of punishment is satisfied only if a statute cannot "reasonably . . . be said to further nonpunitive legislative purposes." *Nixon*, 433 U.S. at 475-76. This factor, sometimes called the "functional test," "invariably appears to be 'the most important of the three,'" *BellSouth II*, 162 F.3d at 684, and indeed "compelling proof on this score may be determinative," *Foretich v. United States*, 351 F. 3d 1198, 1218 (D.C. Cir. 2003). "[E]ven measures historically associated with punishment—such as permanent exclusion from an occupation—have been otherwise regarded when the nonpunitive aims of an apparently prophylactic measure have seemed sufficiently clear and convincing." *BellSouth I*, 144 F.3d at 65 (citation omitted).

The functional inquiry rests on three questions: (1) whether the statute serves purposes that are nonpunitive, rational, and fair; (2) whether there is a nexus between means and end; and (3) whether the magnitude of the burden is in "grave imbalance" with the nonpunitive purpose. *See Foretich*, 351 F.3d at 1222. Because Section 1634 seeks to safeguard federal information systems against the threat of a Russian cyber intrusion, and does so by prohibiting the government's use of products and services it deems vulnerable to exploitation, it does not function as a punishment in any respect.

i. Nonpunitive Purpose

Section 1634 plainly serves the rational, nonpunitive purpose of protecting the U.S. government's information systems from the threat of Russian cyber intrusion. The statute is a textbook risk-management measure, and the text of the provision, together with the legislative record, shows a reasonable and coherent nexus between the burden the statute imposed and the ends it sought to achieve.

This Court need not look beyond the face of the statute to understand Congress's purpose. Section 1634 falls under a subtitle of the NDAA called "Cyberspace-Related Matters," which covers a host of preventive cybersecurity measures ranging from election security to safeguards for critical infrastructure. When read in light of its placement in the NDAA, it becomes even clearer that Section 1634 is a cybersecurity measure about the prospective risks presented by the use of Kaspersky products and services on U.S. information systems. Indeed, Section 1634(c), which calls on agencies to "conduct a review of the procedures for removing suspect products or services from the information technology networks of the Federal Government," removes any doubt that Congress believed Kaspersky products to pose such risks.

Congress's decision to prohibit the "use" of Kaspersky software, hardware, and services (including third-party products that incorporate Kaspersky code), and to thereby require federal agencies to undergo a costly and burdensome implementation process, provides further evidence of the nonpunitive purpose of prevention. If, as Kaspersky suggests, Congress's sole motivation was to punish the company, then it would have been easier, and far less costly, to simply prohibit agencies from purchasing Kaspersky products going forward, rather than requiring those agencies to undergo a time intensive and costly process to identify and discontinue all use of existing Kaspersky products in a matter of months. Indeed, if the idea was to punish Kaspersky for past

conduct, Congress could have sought to require Kaspersky to bear the costs of removing and discontinuing the use of its products. *Cf. Consol. Edison Co.*, 292 F. 3d at347 (acknowledging that a legislature may legitimately decide that a negligent power company "should bear the costs attributable to its negligence," but concluding that the challenged statute was a bill of attainder because the costs allocated to the negligent company were excessive and could not be squared with the nonpunitive purpose of prevention). By having the U.S. government assume those costs, Congress ensured that the burden imposed on Kaspersky (i.e., the loss of future government business) was related to the nonpunitive purpose of the law. *See SeaRiver*, 309 F.3d at 675 n.7 ("Congress has allocated not the past cost of the oil spill, as in *Consol. Edison*, but the risk of a future oil spill.").

Beyond the text of the statute, there is direct legislative history from the committee of jurisdiction describing the precursor to Section 1634 (the DOD-specific version Senator Shaheen offered in committee) as a response to "reports that the Moscow-based company might be vulnerable to Russian government influence."[20] The committee, in other words, was taking preventive action in response to a security threat, and it was doing so based on concerns that were widely shared among members of Congress, including Senator Shaheen, who filed her amendment "[t]o close th[e] alarming national security vulnerability" created by the presence of Kaspersky products on federal information systems. Compl., Ex. C. It was perfectly reasonable for Congress to conclude that a Moscow-based firm with unusually close ties to the Russian intelligence services poses a greater threat to federal information systems than other contractors, either because of the possibility of Kaspersky willfully facilitating a Russian cyber intrusion, or the possibility of the

[20] NDAA FY 2018, U.S. Senate Armed Services Committee at 10, https://www.armed-services.senate.gov/imo/media/doc/FY18%20NDAA%20Summary6.pdf

Russian government either compelling Kaspersky to do so or using Kaspersky's access but acting on its own.

Kaspersky does not suggest that the company's ties to the Russian government are irrelevant to the security concerns underlying Section 1634, or that a reasonable legislature would be unmoved by the evidence concerning the risk of Russian exploitation. Indeed, it makes no difference from Kaspersky's perspective whether banning its products is fully justified by the overwhelming evidence of a security threat. Instead, Kaspersky appears to argue that Congress could not legitimately rely on these concerns in enacting Section 1634 because they were not formally memorialized as legislative "fact-finding." *See* Compl. ¶ 38 (alleging that Congress "engaged in no legislative fact-finding to investigate or test the veracity of these claims"); *id*. ¶ 41 ("Congress singled out Kaspersky Lab by name . . . without having undertaken any legislative fact-finding or analysis"); *id*. ¶ 41 (deriding "[t]he absence from the legislative record of any fact-finding or floor debate").

That, however, is not how the bill of attainder inquiry works. The question is whether "viewed in context, the focus of the enactment can be fairly and rationally understood." *Nixon*, 433 U.S. at 470-72. This entails examining not only the "legislative history" and "specific aspects of the text or structure of the disputed legislation," but also the "*context or timing*" of the statute, *Foretich*, 351 F.3d at 1225 (emphasis added), as well as its "operative effect," *McGowan v. State of Md.*, 366 U.S. 420, 453 (1961); *see BellSouth I*, 144 F.3d at 73 ("More instructive on congressional motivation than the scattered remarks is the timing and apparent triggering of the enactment.").[21]

[21]*See also Nixon*, 433 U.S. at 483 ("For Congress doubtless was well aware that just three months earlier, appellant had resisted efforts to subject himself and his records to the scrutiny of the Judicial Branch"); *Foretich*, 351 F.3d at 1226 (relying on an attempt by the Act's sponsors to broker a deal with plaintiff for him to relinquish his parental rights as evidence of punitive intent);

Thus, in ascertaining the purpose of Section 1634, the Court need not, and indeed should not, confine its review to the narrow, statute-specific legislative history. The Court should instead consider the "context or timing" surrounding the enactment, and it certainly should consider the rationale articulated by its originating committee and statements from its lead proponent. *Nixon*, 433 U.S. at 484 (stating that the purpose of a statute should be considered by reference to "the Members of Congress who voted its passage").

In any event, the congressional record belies Kaspersky's suggestion that the concerns articulated by Senator Shaheen were never "test[ed]" or "substantiated" by legislative fact-finding. Section 1634's passage followed months of congressional investigation and oversight on the risks posed by Kaspersky products, with no fewer than five separate committees hearing testimony on the subject. *See*, *supra*, Section I. These hearings, of course, do not reflect the full extent of congressional consideration on this issue. Many business meetings, including the markup for the precursor to this very bill, are closed to the public, and at least two committees held classified briefings on the Kaspersky threat.

ii. Nexus Between Means and End

The means of Section 1634 are closely tailored to match its purpose. The government need only show that the ends and means "overlap[] in large part." *Selective Serv.*, 468 U.S. at 854. And, as the D.C. Circuit has recognized, Congress has wide latitude in selecting the means of pursuing its goals without triggering any attainder concerns. *See BellSouth II*, 162 F.3d at 689. Section 1634 easily satisfies this standard. As explained, Congress's concerns about Kaspersky stemmed not from any unique aspects of its products or services, but rather the comparatively high risk of

S. La. Grain Servs., Inc. v. Bergland, 463 F. Supp. 783, 786 (D.D.C.) (assessing congressional purpose in light of prior DOJ prosecutions, GAO findings), *aff'd*, 590 F.2d 1204 (D.C. Cir. 1978).

Kaspersky software or services being exploited by the Russian government. Given these concerns, and the wide latitude Congress is afforded in fashioning a legislative solution, the prohibition is a legitimate restriction of future conduct. C*f. Dehainaut v. Pena*, 32 F.3d 1066, 1071-72 (7th Cir. 1994) (finding that the President's directive, which bars from reemployment with the FAA those air traffic controllers who had been discharged for striking, is a nonpunitive, prophylactic measure because there is an adequate nexus between the restrictions imposed by the directive and the directive's legitimate governmental purpose, which was to protect the FAA's operational efficiency and ensure the safe performance of the nation's air traffic control system).

Kaspersky argues that Congress could have legislated in general terms rather than singling out the company by name. But a statute is not "punishment" merely because it could have been framed more generally. *Nixon*, 433 U.S. at 471 (the Bill of Attainder Clause does not "limit[] Congress to the choice of legislating for the universe, or legislating only benefits, or not legislating at all"). A statute can be directed at a single individual or entity if the legislature offers valid, nonpunitive reasons for legislating with specificity. *Id*. at 471-72 (at the time of passage, only President Nixon's papers "demanded immediate attention"); *BellSouth II*, 162 F.3d at 689-90 (statute singling out Bell Operating Companies (BOCs) was not an unlawful attainder because of the "unique infrastructure controlled by the BOCs" which allowed them to exercise monopoly power).

As explained, Congress had good reason to conclude that the vulnerability created by the use of Kaspersky products "demanded immediate attention," *Nixon*, 433 U.S. at 472, and nothing required Congress to legislate more broadly. Congress may have been unprepared to authorize similar restrictions on other contractors without knowing more about the specific security risks of those products, or it may have decided that a general law would be unlikely to timely eliminate the specific vulnerability it sought to address. The Bill of Attainder Clause does not require Congress

to legislate *en masse* or not at all. Indeed, restricting Congress to legislating at greater levels of generality would "cripple the very process of legislating" by striking down every Act that "burdens some persons or groups but not all other plausible individuals." *Nixon*, 433 U.S. at 470-71. In these circumstances, Congress's response is reasonable, and certainly not so out of proportion to the non-punitive goal of protecting federal information systems so as to render the prohibition punitive. *See BellSouth II*, 162 F.3d at 687 (noting that even if there were alternate ways of fulfilling legitimate government interests, "it [is] up to the legislature to make this decision").[22]

iii. Magnitude of the Burden

Finally, the burden imposed on Kaspersky—losing the U.S. government as one of its many sources of revenue—is not in "grave imbalance" with the nonpunitive purpose of the provision. In *Foretich*, the D.C. Circuit found such imbalance because the statute permanently identified the plaintiff as guilty of the "horrific crime[]" of sexually abusing his daughter, despite repeated acquittal by courts. 351 F.3d at 1223. Here, agencies are prohibited from using Kaspersky hardware, software, and services, based on a determination that using them on federal networks poses unjustifiable information security risks. *Cf. BellSouth I*, 144 F.3d at 65 (finding no attainder where the regulatory burden is standard and used elsewhere); *ACORN*, 618 F.3d at 137

[22] Kaspersky questions Congress's justification for extending Section 1634's prohibition to all Kaspersky products and services, in light of Senator Shaheen's focus on "software" in her New York Times Op-Ed. Like Kaspersky's broader legal theory, this argument rests on the misapprehension that Senator Shaheen's media statements comprise the universe of information relevant to Congress's concerns about Kaspersky's products. While Senator Shaheen's statement may have focused on software, much of her reasoning applies to Kaspersky products and services, as evidenced by statements from other members of Congress. *See, e.g.*, House Science Committee Report 115-376 at 5 (discussing "infiltration of Kaspersky Lab into U.S. Government computer systems"). Any inference drawn from the more expansive scope of the law cannot establish, to the requisite degree of certainty, that Congress was acting to punish Kaspersky rather than to protect the United States.

(disqualifying corporation from federal funds did not amount to an unlawful attainder in part because corporation derived only 10% of its funding from federal grants). Such time-tested regulatory requirements cannot be placed in the same league as the crippling disabilities that have been found to satisfy the functional test of punishment. *See BellSouth II*, 162 F.3d at 686-88 (collecting cases showing that "burdensome regulation" is not equivalent to punishment). And to whatever extent the statute might establish differential treatment, it is valid because it is in pursuit of a legitimate regulatory purpose. *See BellSouth I*, 144 F.3d at 67 (finding "differential treatment . . . neither suggestive of punitive purpose nor particularly suspicious"); *see also Nixon*, 433 U.S. at 472 (authorizing "legitimate class of one").

C. The Legislative Record Shows No Punitive Intent.

With respect to the final factor of the legislative-punishment test, the Supreme Court has observed that the search for punitive legislative motives is "at best a hazardous matter, and when that inquiry seeks to go beyond objective manifestations it becomes a dubious affair indeed." *Flemming*, 363 U.S. at 617. Further, the presumption of constitutionality to which challenged enactments are entitled "forbids us lightly to choose that reading of the statute's setting which will invalidate it over that which will save it." *Id*. Thus, "only the clearest proof could suffice to establish the unconstitutionality of a statute on such a ground." *Id.; see also Selective Serv.*, 468 U.S. at 855 n.15 (requiring "unmistakable evidence of punitive intent" before a statute may be invalidated).

The D.C. Circuit has similarly recognized that "[t]he legislative record by itself is insufficient evidence for classifying a statute as a bill of attainder unless the record reflects overwhelmingly a clear legislative intent to punish," and that "[s]tatements by a smattering of legislators do not constitute unmistakable evidence of punitive intent." *Consol. Ed*, 292 F.3d at 354 (citation

omitted); *see also United States v. O'Brien*, 391 U.S. 367, 384 (1968) ("What motivates one legislator to make a speech about a statute is not necessarily what motivates scores of others to enact it."); *Butler v. Apfel*, 144 F.3d 622, 626 (9th Cir. 1998) (requiring "unmistakable evidence of a punitive motive" and rejecting a bill of attainder challenge based on legislative remarks).

As discussed, the legislative record, together with the context and timing in which Section 1643 was enacted, reveals that Congress's purpose in passing Section 1643 was preventive, not punitive. The primary goal of the statute was to protect federal information systems from the threat of Russian cyber intrusion, and evidence of that purpose appears throughout the congressional record. Kaspersky's claim relies heavily—indeed, almost exclusively—on its assertion that Section 1634 was enacted for the sole purpose of punishing the company. On this point Kaspersky offers no concrete facts, but rather asks the Court to draw inferences from various aspects of the legislative text and history. Kaspersky observes, for example, that "Congress singled out Kaspersky Lab by name," rather than "enact[ing] a rule of general applicability concerning cybersecurity." Compl. ¶¶ 40-41. Neither of these observations is particularly suspicious, much less suggestive of punitive intent. And both collapse into Kaspersky's wholly unsupportable assertion that Congress could not have singled out Kaspersky in the statute for any reason other than to punish its owners and operators. That the statute names Kaspersky plainly cannot be enough to demonstrate punitive intent, because it conflates the two elements of the attainder analysis (specificity and punishment) and contradicts the Supreme Court's statement that specificity alone does not offend the Bill of Attainder Clause. *Nixon*, 433 U.S. at 471.

The complaint points to no other plausible evidence of punitive motivation. Although Kaspersky makes much of what it incorrectly characterizes as the absence of "legislative fact-finding[s]," Compl. ¶ 38, it is unclear what it believes this proves. As explained, in assessing

Congress's motivation, courts are not confined to formal legislative fact-finding, but rather can consider the legislative process as a whole, including the "context or timing" of the challenged enactment. *Foretich*, 351 F.3d at 1225.

But even if the Court were to assume, contrary to the legislative record, that there was "congressional silence surrounding" the passage of Section 1634, that assumption would not help Kaspersky but rather "impede[] [it] in successfully carrying its burden on this factor." *SeaRiver*, 309 F.3d at 677. Statutes are presumed constitutional, *Heller v. Doe by Doe*, 509 U.S. 312, 320 (1993), and Kaspersky carries the burden of demonstrating punitive intent. The company has offered no concrete facts in support of its allegation of punitive intent, much less the type of "'smoking gun' evidence of punitive intent necessary to establish a bill of attainder." *SBC Commc'ns, Inc. v. FCC*, 154 F.3d 226, 243 (5th Cir. 1998).

CONCLUSION

For these reasons, this lawsuit should be dismissed.

Dated: March 26, 2018

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General

ERIC R. WOMACK
DIANE KELLEHER
Assistant Branch Directors
Civil Division

/s/ Samuel M. Singer
SAMUEL M SINGER (D.C. Bar 1014022)
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave, NW

Washington, D.C. 20530
Telephone: (202) 616-8014
Fax: (202) 616-8470

Attorneys for Defendant

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KASPERSKY LAB, INC.; and KASPERSKY LABS LIMITED,	)	
Plaintiffs,	)	
v.	)	Civ. No. 18-325 (CKK)
UNITED STATES OF AMERICA	)	
Defendant.	)	

[PROPOSED] ORDER

Having considered Defendant's memorandum in support of its motion to dismiss, it is hereby ORDERED that Defendant's motion is GRANTED and the complaint in this action dismissed with prejudice.

SO ORDERED.

_____
U.S. DISTRICT COURT