UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

KASPERSKY LAB, INC. and KASPERSKY LABS LIMITED, Appellants, v. UNITED STATES DEPARTMENT OF HOMELAND SECURITY, KIRSTJEN M. NIELSEN, in her official capacity as Secretary of Homeland Security, and UNITED STATES OF AMERICA, Appellees.	Case Nos. 18-5176, 18-5177

APPELLANTS' EMERGENCY MOTION FOR EXPEDITED CONSIDERATION OF THIS APPEAL AND AN EXPEDITED BRIEFING SCHEDULE

Pursuant to 28 U.S.C. § 1657, and D.C. Circuit Rules 27(f) and 47.2, Appellants Kaspersky Lab, Inc. and Kaspersky Labs Limited (collectively, "Kaspersky Lab") respectfully move for expedited briefing and oral argument in the above-captioned appeal. Appellants propose the following schedule for expedited briefing:

July 11, 2018	Brief for Appellants
August 13, 2018	Brief for Appellees
August 27, 2018	Reply Brief for Appellants

Kaspersky Lab respectfully requests that oral argument be scheduled as soon as possible, so that a decision may be issued before October 1, 2018. Section 1634(a) of the National Defense Authorization Act for Fiscal Year 2018, Pub. Law No. 115-91 (the "NDAA")—the statute at issue in this appeal—prohibits the federal government from using "any hardware, software, or services developed or provided, in whole or in part" by Kaspersky Lab. That section takes effect on October 1, 2018.

Kaspersky Lab has notified the Clerk of Court and opposing counsel of this motion by telephone. Appellees' counsel does not oppose the motion. Kaspersky Lab has requested expedited transcripts of the only two telephonic hearings held before the district court.

BACKGROUND

Kaspersky Lab is a multinational cybersecurity company exclusively focused on protecting against cyberthreats, no matter their origin. It is one of the world's largest privately owned cybersecurity companies.

On December 12, 2017, Congress singled out Kaspersky Lab in the NDAA and prohibited the federal government from using its software, hardware, and services. Section 1634 of the NDAA states, in pertinent part:

> SEC. 1634. PROHIBITION ON USE OF PRODUCTS AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB.

> (a) Prohibition.—No department, agency, organization, or other element of the Federal Government may use, whether directly or through work with or on behalf of another department, agency, organization, or element of the Federal Government, any hardware, software, or services developed or provided, in whole or in part, by—
>
> (1) Kaspersky Lab (or any successor entity);
>
> (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
>
> (3) any entity of which Kaspersky Lab has majority ownership.
>
> (b) Effective Date.—The prohibition in subsection (a) shall take effect on October 1, 2018.

Kaspersky Lab argues that this provision of the NDAA constitutes an unlawful Bill of Attainder under Article I, Section 9 of the U.S. Constitution.

Kaspersky Lab also challenges the Department of Homeland Security's ("DHS") Binding Operational Directive 17-01 (the "BOD") that deprived Kaspersky Lab of a protected liberty interest without due process. On September 13, 2017, DHS issued the BOD requiring all federal departments and agencies to identify and begin removing all "Kaspersky-branded products" within 90 days. 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, 43,783 (Sept. 19, 2017). DHS finalized the BOD on December 6, 2017. *See* Kaspersky Lab's Motion for Summary Judgment, Admin R. Ex. J,

Kaspersky Lab, Inc. v. United States Dep't of Homeland Sec., No. 1:17-cv-02697 (CKK), 2018 WL 2433583 (D.D.C. May 30, 2018).

Kaspersky Lab filed two lawsuits: the first against the DHS and its Secretary challenging the BOD (case no. 1:17-cv-02697), and the second against the federal government seeking invalidation of Sections 1634(a) and (b) of the NDAA (case no. 1:18-cv-00325). On May 30, 2018, the district court issued a consolidated memorandum opinion in Kaspersky Lab's two cases. *Kaspersky Lab, Inc. v. United States Dep't of Homeland Sec.*, Nos. 1:17-cv-02697, 1:18-cv-00325 (CKK), 2018 WL 2433583 (D.D.C. May 30, 2018). The district court dismissed the NDAA lawsuit for failure to state a claim on which relief could be granted and dismissed the BOD lawsuit for lack of standing. *Id.* at *26.

The prohibitions in the NDAA and the BOD targeting Kaspersky Lab and all of its products, software, hardware, and services throughout the federal government are causing Kaspersky Lab irreparable harm, including substantial reputational harm. That harm will not end without relief from this Court.

ARGUMENT

This appeal should be expedited because the district court's opinion is "subject to substantial challenge," delay will continue "to cause irreparable injury" to Kaspersky Lab, and other "persons not before the Court[] have an unusual interest in prompt disposition." U.S. Court of Appeals for the District of Columbia

Circuit, *Handbook of Practice and Internal Procedures* 33 (2018). Each of these considerations is discussed below.

I. The District Court's Opinion Is Subject to Substantial Challenge

The district court's rulings on Kaspersky Lab's NDAA and BOD claims are subject to substantial challenge on appeal.

A. The District Court's Analysis of the NDAA Claim Is Subject to Substantial Challenge

This Court "reviews *de novo* the dismissal of a complaint for failure to state a claim, accepting a plaintiff's factual allegations as true and drawing all reasonable inferences in a plaintiff's favor." *Momenian v. Davidson*, 878 F.3d 381, 387 (D.C. Cir. 2017) (citing *Vila v. Inter-Am. Inv., Corp.*, 570 F.3d 274, 278 (D.C. Cir. 2009)). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "Federal Rule of Civil Procedure 12(d) forbids considering facts beyond the complaint in connection with a motion to dismiss the complaint for failure to state a claim." *United States ex rel. Shea v. Cellco P'ship*, 863 F.3d 923, 936 (D.C. Cir. 2017).

Here, the district court too narrowly interpreted the Bill of Attainder jurisprudence and too broadly applied the motion to dismiss standard. First, this Court has held that legislation may be an impermissible Bill of Attainder if it is

similar "to the types of burdens traditionally recognized as punitive," even if it is "not squarely within the historical meaning of legislative punishment." *Foretich v. United States*, 351 F.3d 1198, 1220 (D.C. Cir. 2003); *see also United States v. Lovett*, 328 U.S. 303, 316 (1946) (A particular "permanent proscription from any opportunity to serve the Government is punishment, and of a most severe type."). In addition, Congress's "nonpunitive aims must be 'sufficiently clear and convincing' before a court will uphold a disputed statute against a bill of attainder challenge." *Foretich*, 351 F.3d at 1221 (quoting *BellSouth Corp. v. F.C.C.*, 162 F.3d 678, 686 (D.C. Cir. 1998)).

Contrary to this Court's holding in *Foretich*, the district court concluded that because the NDAA "targets the products of a multinational corporation," rather than individuals and their employment opportunities, "[t]he NDAA . . . is nothing like the legislation" at issue in historical Bill of Attainder cases. *Kaspersky Lab, Inc.*, 2018 WL 2433583, at *13. The district court summarized the rationale for Section 1634 of the NDAA as:

- Russia has committed cyberattacks;
- Kaspersky Lab cybersecurity products are present on federal government systems;
- all cybersecurity products can be used to exploit systems on which they are installed;
- Kaspersky Lab is headquartered in Russia, is subject to Russian laws, and "has certificates and licenses from the Federal Security Service" in Russia; and

- Eugene Kaspersky "graduated from an institute that was sponsored by the KGB," worked for the Ministry of Defense in the past, and has "personal ties with Russian intelligence officers."

Id. at *3–8. The district court reasoned that this "information" was "sufficient . . . to say that it was rational for Congress to conclude . . . that barring the federal government's use of Kaspersky Lab products would help prevent further Russian cyber-attacks." *Id.* at *16. But this congressional "conclusion" is a non sequitur based on little more than innuendo and suspicion. Furthermore, the "information" above does not appear in the unclassified NDAA legislative record, but rather is drawn largely from the BOD administrative record, which Kaspersky Lab contests. On November 10, 2017, after the BOD took effect but before it became final, Kaspersky Lab filed a detailed written response that rebutted at length the legal arguments and factual allegations levied against Kaspersky Lab, corrected many misunderstandings, and highlighted the deficiencies in the administrative process. *See* Kaspersky Lab's Motion for Summary Judgment, Admin. R. Ex. I, *Kaspersky Lab, Inc. v. United States Dep't of Homeland Sec.*, No. 1:17-cv-02697 (CKK), 2018 WL 2433583 (D.D.C. May 30, 2018).

Second, Kaspersky Lab alleged sufficient facts to support its claim that the NDAA constitutes an unlawful Bill of Attainder. *See* NDAA Compl. ¶¶ 18–44.[1]

1. Complaint, *Kaspersky Lab, Inc. v. United States*, No. 1:18-cv-00325 (CKK), 2018 WL 2433583 (D.D.C. May 30, 2018) ("NDAA Compl.").

Rather than credit Kaspersky Lab's well-pleaded allegations and reasonable inferences from them, the district court weighed evidence from other sources and drew factual inferences *adverse* to Kaspersky Lab and in favor of the Appellees to bolster its conclusion that the NDAA is constitutional. For example, the district court reasoned that the NDAA is not punishment because it does not prevent Kaspersky Lab "from operating as a cybersecurity business." *Kaspersky Lab, Inc.*, 2018 WL 2433583, at *14. "The company may still operate and derive revenue throughout the world, including in the United States, by selling its products to individuals, private companies, and other governments." *Id.*; *see id.* (Kaspersky Lab has been deprived of "one tiny source of revenue"). These factual findings are contrary to the well-pleaded allegations of injury in the Complaint and cannot form the basis for resolving a motion to dismiss.

B. The District Court's Analysis of the BOD Claim Is Subject to Substantial Challenge

The district court's dismissal of Kaspersky Lab's BOD claim for lack of standing is flawed for similar reasons. "To demonstrate standing, a plaintiff must show that she has suffered an 'injury in fact' that is 'fairly traceable' to the defendant's actions and that is 'likely to be redressed' by the relief she seeks." *Attias v. Carefirst, Inc.*, 865 F.3d 620, 625 (D.C. Cir. 2017) (quoting *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016)), *cert. denied*, 138 S. Ct. 981 (2018). As this Court explained, "[e]ach element [of standing] must be supported in the same

way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation." *Arpaio v. Obama*, 797 F.3d 11, 19 (D.C. Cir. 2015) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992)). "[A]t the pleading stage, . . . plaintiffs are required only to 'state a *plausible* claim' that each of the standing elements is met." *Attias*, 865 F.3d at 625 (quoting *Food & Water Watch, Inc. v. Vilsack*, 808 F.3d 905, 913 (D.C. Cir. 2015)).

Here, the district court, having dismissed the NDAA claim, concluded that the NDAA would bar any relief Kaspersky Lab might receive if the court invalidated the BOD, so the BOD claim was not redressable. The fact that the court decided the NDAA claim first (in the same opinion), and against Kaspersky Lab, rendered its NDAA decision outcome determinative of the BOD claim.

The district court's analysis misses the mark. As in the disposition of the NDAA claim, the court weighed evidence and drew factual inferences adverse to Kaspersky Lab. Moreover, the court failed to apply the correct standing principles for procedural due process claims. In relevant part, Kaspersky Lab framed its BOD claim as alleging not only a deprivation of a constitutionally protected right, but also deprivation "with constitutionally insufficient procedures attendant upon

that deprivation." BOD Compl. ¶ 85.[2] Where a plaintiff "alleges a deprivation of a procedural protection to which he is entitled[,] [he] never has to prove that if he had received the procedure the substantive result would have been altered." *NB ex rel. Peacock v. District of Columbia*, 682 F.3d 77, 86 (D.C. Cir. 2012) (quoting *Sugar Cane Growers Coop. of Fla. v. Veneman*, 289 F.3d 89, 94 (D.C. Cir. 2002)). This Court applies "this relaxed standard for redressability in procedural rights cases." *Id.* (internal quotation marks and alterations omitted). The district court's failure to apply the correct standard, as well as its failure to accord Kaspersky Lab's factual allegations the consideration they are due at the pleadings stage, among other things, renders the court's analysis of the BOD claim erroneous.

For these and other reasons, the district court's opinion is subject to substantial challenge.

II. Delay Will Cause Irreparable Injury to Kaspersky Lab

The NDAA and BOD eliminate and prohibit any relationship between the U.S. Government and services and products provided by Kaspersky Lab by October 1, 2018. Although Kaspersky Lab's contracts with the U.S. Government do not account for a large portion of its annual revenue, "[t]he U.S. has been and remains one of the most significant geographic markets in Kaspersky Lab's global

2. Complaint, *Kaspersky Lab, Inc. v. United States Dep't of Homeland Sec.*, No. 1:17-cv-02697 (CKK), 2018 WL 2433583 (D.D.C. May 30, 2018) ("BOD Compl.").

business." BOD Compl. ¶ 32. "Sales to customers in the United States represent approximately one quarter of total global bookings in 2016," and Kaspersky Lab "has invested over a half a billion dollars in its operations over the last twelve years," including "over $65 million in 2016 alone." *Id.* Given its presence in the U.S. market, Kaspersky Lab "has a substantial interest in its status as a vendor to the U.S. Government." *Id.* ¶ 34.

Kaspersky Lab faces the prospect that the U.S. Government's unfounded mistrust of the company will remain enshrined in U.S. law. And the district court acknowledged that the BOD's "determination that Kaspersky Lab products present a risk to [the U.S.] federal government networks" bears "the imprimatur of government authority." *See Kaspersky Lab, Inc.*, 2018 WL 2433583, at *25 (internal quotation marks omitted). This reputational damage has had an immediate and severe financial impact on Kaspersky Lab. The impact is continuing and growing. Kaspersky Lab's position as a trusted software vendor has been compromised in all areas. It is difficult to envision a more irreparable harm to a company's reputation than the United States government declaring the company a threat to national security and refusing to do business with it.

III. Third Parties Not Before the Court Have an Unusual Interest in Prompt Disposition of This Appeal

The effects of the NDAA and BOD are sweeping. Beginning October 1, 2018, every agency and instrumentality of the U.S. Government is prohibited from using Kaspersky Lab services and products. Many, if not most, have already begun the process of removing Kaspersky Lab products from their systems as a result of the BOD and the upcoming NDAA effective date. All of these various entities have a strong interest in the prompt resolution of this appeal.

Other users of Kaspersky Lab products, as well as commercial partners that sell such products, also have a strong interest in prompt resolution. The federal prohibition on Kaspersky Lab products as a risk to government systems bears "the imprimatur of government authority." *See Kaspersky Lab, Inc.*, 2018 WL 2433583, at *25 (internal quotation marks omitted). As Kaspersky Lab alleged in its Complaint, "[o]ver 400 million users—from governments to private individuals, commercial enterprise to critical infrastructure owners and operators alike—utilize Kaspersky Lab technologies to secure their data and systems." BOD Compl. ¶ 29. Those users have a strong interest in this Court's prompt consideration of whether the U.S. Government singling out and targeting Kaspersky Lab violates the Constitution.

CONCLUSION

For the foregoing reasons, Kaspersky Lab's Emergency Motion for Expedited Consideration of This Appeal and an Expedited Briefing Schedule should be granted.

Dated: June 8, 2018

Respectfully submitted,

/s/ Scott H. Christensen

Scott H. Christensen, D.C. Bar No. 476439
Stephen R. Halpin III, D.C. Bar No. 1048974
HUGHES HUBBARD & REED LLP
1775 I Street, N.W., Suite 600
Washington, D.C. 20006-2401
Telephone: (202) 721-4600
Facsimile: (202) 721-4646
Email: scott.christensen@hugheshubbard.com
Email: stephen.halpin@hugheshubbard.com

Attorneys for Plaintiffs Kaspersky Lab, Inc. and Kaspersky Labs Limited

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, Appellants Kaspersky Lab, Inc. and Kaspersky Labs Limited state as follows:

1. Kaspersky Lab, Inc. is a Massachusetts corporation with its principal place of business in Woburn, Massachusetts. Kaspersky Lab, Inc. is a direct wholly owned subsidiary of Kaspersky Labs Limited, a U.K. holding company.

2. Kaspersky Labs Limited has no parent corporation, and no publicly held corporation owns 10% or more of its stock.

PROVISIONAL CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rule 28(a)(1)(A), Appellants Kaspersky Lab, Inc. and Kaspersky Labs Limited state as follows:

(A) Parties and Amici

Appellants in this case are Kaspersky Lab, Inc. and Kaspersky Labs Limited. Appellees are the United States Department of Homeland Security, Kirstjen M. Nielsen, in her official capacity as Secretary of Homeland Security, and the United States of America.

(B) Rulings Under Review

Appellants seek review of the consolidated memorandum opinion and orders of District Judge Colleen Kollar-Kotelly entered on May 30, 2018 granting the motions to dismiss filed by Appellees below (Docket Entries 25 & 26 in Case No. 1:17-cv-02697-CKK and Docket Entries 13 & 14 in Case No. 1:18-cv-00325-CKK).

(C) Related Cases

Appellants are not aware of any cases related to this appeal.

CERTIFICATE OF SERVICE

I hereby certify that on June 8, 2018, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the CM/ECF system. I also certify that I have caused four copies of the foregoing to be hand delivered to the Court. I also certify that I have electronically mailed the foregoing to:

H. Thomas Byron III
Assistant Director
Civil Division, Appellate Staff
U.S. Department of Justice
Main (RFK) Room 7529
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530
Ph: (202) 616-5367
Fx: (202) 307-2551
H.Thomas.Byron@usdoj.gov

Sam M. Singer
Trial Attorney, U.S. Department of Justice
Civil Division, Federal Programs Branch
Direct Dial: (202) 616-8014
Fax: (202) 616-8460
Samuel.M.Singer@usdoj.gov

Dated: June 8, 2018

/s/ Scott H. Christensen
Scott H. Christensen, D.C. Bar No. 476439