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' REPLY IN SUPPORT
OF EMERGENCY MOTION TO STAY

The U.S. government's opposition to Kaspersky Lab's emergency motion to stay obfuscates the premise behind both that motion and the previous motion to expedite: This Court should have the opportunity to rule on whether Section 1634(a) of the NDAA is an unconstitutional bill of attainder before the statute becomes effective. After this Court expedited this appeal, three federal agencies published an interim rule that "implements Section 1634" starting July 16, 2018. (*See* Gov't Opp'n at 4–5.) "To implement section 1634, the [Federal Acquisition Regulation ('FAR')] prohibits contractors from providing any hardware, software,

or services developed or provided by Kaspersky Lab or its related entities, or using any such hardware, software, or services in the development of data or deliverables first produced in the performance of the contract." 83 Fed. Reg. 28,141, 28,141 (June 15, 2018) (Emerg. Mot. App. 8).[1] Amending the FAR and federal contracts effective July 16 to prohibit contractors from using Kaspersky Lab products or services effective October 1 accelerates the reputational and financial damage to Kaspersky Lab. The plain meaning of "implement" undermines the notion that the interim rule "in no way accelerates the statutory effective date." (Gov't Opp'n at 7.)

The government relies on the District Court's errors and on legal formalisms that are at odds with a just and speedy determination of the relief sought in this motion and in the overall appeal. Some of the government's arguments also support the likelihood that Kaspersky Lab will prevail on its bill of attainder challenge. As a result, Sections 1634(a) and (b), and any rule that accelerates their implementation, should be stayed until this Court can resolve Kaspersky Lab's lawsuit.

---

1. The government claims that it "published a notice on May 9, 2018" regarding the interim rule. (Gov't Opp'n at 5.) In support, the government cites (1) an OMB website that states the government is "proposing to amend" the FAR, with no proposal, and (2) a *National Law Review* article by an attorney at a law firm that states "[a]gencies are not bound by these postings." Neither constitutes notice of a forthcoming rule.

ARGUMENT

I. The government's arguments support Kaspersky Lab's emergency motion to stay.

A. Kaspersky Lab is suffering irreparable harm.

Asserting that Section 1634(a) is not harm or punishment because "Kaspersky Lab is not prevented from operating as a cybersecurity business," J.A. 197 (Gov't Opp'n at 13), recalls the argument that banning confederates or communists from working as lawyers, priests, trade unionists, or government employees does not prevent them from working altogether. The Supreme Court has repeatedly rejected that reasoning in striking down bills of attainder. *See United States v. Brown*, 381 U.S. 437, 449–50 (1965); *United States v. Lovett*, 328 U.S. 303, 315–16 (1946); *Ex parte Garland*, 71 U.S. (4 Wall.) 333, 377 (1867); *Cummings v. Missouri*, 71 U.S. (4 Wall.) 277, 320 (1867).

Moreover, the federal government branding Kaspersky Lab a cyberthreat impairs the cybersecurity company's ability to operate. *See* Gentile Decl. ¶¶ 17–41 (Emerg. Mot. App. 16–26)[2]; Gentile Suppl. Decl. ¶ 5 (Emerg. Mot. App. 29–30); Matesen Decl. ¶¶ 5–8 (Emerg. Mot. App. 32–34). The government's focus on the loss of federal contract dollars elides the substantial, ongoing reputational and

---

2. The government complains that Kaspersky Lab lacks support specific to Section 1634(a) (*see, e.g.*, Gov't Opp'n at 16–17), while it relies almost entirely on the BOD administrative record to justify the purpose of Section 1634(a) (*see, e.g.*, *id.* at 8–9, 20–22).

financial harm it is causing Kaspersky Lab, (Gov't Opp'n at 13–14), estimated to be in the "millions of dollars," *see* Matesen Decl. ¶ 7 (Emerg. Mot. App. 33). Worse than *Foretich v. United States*, 351 F.3d 1198 (D.C. Cir. 2003), Congress here directed a loss of business. But like *Foretich*, the primary harm to Kaspersky Lab is the significant reputational injury that causes others to avoid its products and services. *See, e.g.*, *id*. at 1211.

As the government recognizes, "the prohibition in Section 1634 is broader than that in the BOD." (Gov't Opp'n at 17.) That some irreparable harm is already ongoing does not mean that additional, broader harm is of no moment. A single action need not be the sole cause of a plaintiff's injury for a tortfeasor to be liable; it is sufficient if the action is a "substantial factor" in causing the harm. *See, e.g.*, *Butts v. United States*, 822 A.2d 407, 417 (D.C. 2003); *see also* Restatement (Second) of Torts § 622A (1977) ("Defamation is a legal cause of special harm to the person defamed if . . . it is a substantial factor in bringing about the harm[.]"). Section 1634(a) and its accelerated implementation are a substantial factor in the severe reputational harm Kaspersky Lab is experiencing. The fact that the BOD contributes to that harm does not absolve Congress of its constitutional obligations. The political branches should not be able to insulate themselves from judicial review by taking separate actions that together inflict reputational harm on a company.

B. Kaspersky Lab is likely to prevail on its claim that Section 1634(a) is punishment, because of its broad justification and narrow application.

In *Foretich*, this Court observed that "narrow application of a statute to a specific person or class of persons raises suspicion, because the Bill of Attainder Clause is principally concerned with '[t]he singling out of an individual for legislatively prescribed punishment.'" 351 F.3d at 1224 (quoting *Selective Serv. Sys. v. Minn. Pub. Interest Research Grp.*, 468 U.S. 841, 847 (1984)). The government asserted that the legislation at issue in *Foretich* was "primarily concerned with promoting the best interests of the child" in custody disputes, but the legislation clearly applied to a single dispute – involving Dr. Foretich, his former wife, and their daughter – and the legal standard "was not made available in other child custody cases." *Id*. at 1223.

Because the legislation in *Foretich* had a broad justification and a narrow application, "the particular means Congress adopted in [the] Act belie[d] any nonpunitive aim." *Id.*

> If the Act applied in all custody disputes, its provisions for dealing with allegations of sexual abuse would not cast aspersions on any particular person. But as the Government concedes, the Act targets only Dr. Foretich. As a consequence, the Act officially associates Dr. Foretich with criminal sexual abuse because it implies that his daughter alone needs special protections.

Id. at 1224. This Court concluded that, "[i]n light of the Act's narrow applicability, the Government's asserted purposes are simply implausible." *Id.* As a result, this Court came to the "inescapable" conclusion that "[t]he purposes the Government alleges thus cannot be viewed as nonpunitive." *Id.* at 1223.

Here, too, Section 1634(a) has a broad justification and a narrow application to one entity. The government relies on the "expert judgment about threats to U.S. national security," J.A. 30 (Gov't Opp'n at 22), presented in the September 1, 2017 Memorandum from Acting Secretary Jeanette Manfra:

- "The danger stems in part from *the inherent properties of anti-virus software, which operates with broad file access and elevated privileges*. Such access and privileges can be exploited by a malicious cyber actor such as Russia, which has demonstrated the intent to target the U.S. government and the capability to exploit vulnerabilities in federal information systems." J.A. 30 (emphasis added).

- "These actions could take place because of a range of factors, including Russian laws that authorize the Russian Federal Security Service ('FSB') to compel Russian enterprises to assist the FSB in the execution of FSB duties, . . . and to require *Russian companies* to include hardware or software needed by the FSB to engage in 'operational/technical measures.'" J.A. 30 (emphasis added). (Gov't Opp'n at 21.)

- "Finally, Russian law allows the FSB to intercept *all communications transiting Russian telecommunication and Internet Service Provider networks*, which presumably includes data transmissions between Kaspersky and its U.S. government customers." J.A. 30 (emphasis added). (Gov't Opp'n at 21.)

These purported threats to national security apply to any producer of antivirus software and to any company doing business in Russia and using Russian networks for communications. But the U.S. government singles out only Kaspersky Lab. The government all but gives away its case when it observes that "Section 1634 reflects the joint assessment of the political branches that the use of [Kaspersky Lab products and services] by federal entities poses a risk to the national security." (Gov't Opp'n at 23.) The Founders included the Bill of Attainder Clause in the Constitution so that Congress could not "pronounce[] upon the guilt of [a] party, without any of the forms or safeguards of trial." *Cummings v. Missouri*, 71 U.S. (4 Wall.) 277, 323 (1867). Adjudging individual guilt and fixing punishment is the province of the judiciary. *See id.*

There are "alternative means for achieving the legislative aim" of the United States protecting its information systems (Gov't Opp'n at 15), as Kaspersky Lab has argued previously. Congress could have passed a law of general applicability that prohibits the federal government from using products or services of any cybersecurity software producer that has provided information to the FSB, does business in Russia, has servers in Russia, or uses Russian networks.[3] After all, the

---

3. Congress may have thought that singling out Kaspersky Lab instead of enacting a law of general applicability was more politically expedient, given that a law of general applicability would likely have ensnared many other high-profile cybersecurity vendors. Many do business in Russia and have

expert judgment on which the government relies, and Kaspersky Lab contests, identified the threats to U.S. national security as inherent properties of antivirus software, the Russian government's ability to use antivirus software, the FSB's control over private enterprises doing business in Russia, and the FSB's ability to intercept communications on Russian networks. (Gov't Opp'n at 21.) Such a law of general applicability would have allowed companies to decide whether to continue operating in Russia or to remain a U.S. contractor. As in *Foretich*, "[i]f the disputed Act had been enacted to apply to all" cybersecurity vendors, "this would be a different case." 351 F.3d at 1223. The fact that Kaspersky Lab "was singled out for [the] severe burden" of a permanent prohibition "belies the claim that Congress's purposes were nonpunitive." *Id*. at 1224.

---

provided sensitive information to the FSB or other agencies of the Russian government. *See* Dustin Volz et al., "Tech Firms Let Russia Probe Software Widely Used by U.S. Government," *Reuters* (Jan. 25, 2018) ("Major global technology providers SAP, Symantec and McAfee have allowed Russian authorities to hunt for vulnerabilities in software deeply embedded across the U.S. government."); Joel Schectman et al., "Special Report: HP Enterprise Let Russia Scrutinize Cyberdefense System Used by Pentagon," *Reuters* (Oct. 2, 2017) ("Hewlett Packard Enterprise allowed a Russian defense agency to review the inner workings of cyber defense software used by the Pentagon to guard its computer networks, according to Russian regulatory records and interviews with people with direct knowledge of the issue."); Joel Schectman et al., "Under Pressure, Western Tech Firms Bow to Russian Demands to Share Cyber Secrets," *Reuters* (June 23, 2017) ("Western technology companies, including Cisco, IBM and SAP, are acceding to demands by Moscow for access to closely guarded product security secrets.").

II. The government's remaining arguments elevate form over substance.

The government urges this Court to require Kaspersky Lab to return to the District Court (Gov't Opp'n at 1–4) for an evaluation of whether it is likely to prevail on the merits in its bill of attainder challenge. This Court's review of constitutional issues is, of course, de novo. The repeated citations to the District Court's legal conclusions thus add little weight to the government's argument, but they do prove one of Kaspersky Lab's points: Moving first in the District Court would have been futile. The District Court erroneously held that Kaspersky Lab failed to state a legally cognizable claim; it would have been a waste of judicial and party resources to pursue motions practice in that court while the government accelerates implementation of the law subject to challenge before this Court.

Kaspersky Lab pursued a preliminary injunction in the BOD Case (case no. 17-cv-02697) before filing the Bill of Attainder Case (case no. 18-cv-00325). At the District Court's urging, Kaspersky Lab agreed to withdraw that request in exchange for expedited resolution on the merits of both cases in consolidated briefing. *See* J.A. 190 n.4.[4] The government's claim that "Plaintiffs never sought" injunctive relief relating to Section 1634(a) "before the district court in this case or

4. The District Court never reached the merits of Kaspersky Lab's claims in the BOD Case. J.A. 223.

any other case" (Gov't Opp'n at 1; *see id.* at 2, 3) is thus too sweeping and too specific to be accurate. And, after this Court's decision to expedite this appeal, there was no need for Kaspersky Lab to seek emergency injunctive relief until the government's shoot-first-ask-for-comments-later approach accelerated implementation of Section 1634(a).

This appeal challenges the constitutionality of Section 1634(a) of the NDAA and the related decision to dismiss the BOD Case on standing grounds. "The legal basis for the [interim] rule is section 1634 of the NDAA for FY 2018." 83 Fed. Reg. at 28,142 (Emerg. Mot. App. 9). If Section 1634(a) is a bill of attainder, then the government cannot pursue an interim rule implementing an unconstitutional law. There should be no need to "bring a new action in the district court against the agencies" that proffered the interim rule (Gov't Opp'n at 6), because Kaspersky Lab already sued the United States over Section 1634(a).[5]

The question before the Court in Kaspersky Lab's emergency motion to stay is not the merits of the appeal. Contrary to the government's suggestion that

---

5. Kaspersky Lab should not be forced to play a shell game by suing those agencies separately or seeking to enjoin other possible actions that the agencies might take if the Court grants this emergency motion. (*See* Gov't Opp'n at 17 ("Even if this Court were to enjoin enforcement of Section 1634 and the interim rule, the agencies would retain the discretion to take appropriate action[.]").) The interim rule notes that the government is "consider[ing] additional actions to implement section 1634." 83 Fed. Reg. at 28,141 (Emerg. Mot. App. 8).

Kaspersky Lab wants "this Court to consider the merits of [its] constitutional claims without full briefing or argument," (Gov't Opp'n at 7; *see id.* at 12 n.3), Kaspersky Lab has sought to prove one of the elements required for the emergency relief it seeks, namely its likelihood of prevailing on the merits. Kaspersky Lab welcomes full briefing and argument on the merits prior to Section 1634(a) becoming effective, as shown by its effort to expedite the appeal.[6] The question before the Court in the emergency motion is whether to maintain the status quo until it can decide the merits of the appeal in light of the government's efforts to accelerate changes to the status quo.

CONCLUSION

For the foregoing reasons, and for reasons stated in Kaspersky Lab's Emergency Motion to Stay, the motion to stay should be granted.

---

6. If the government is concerned that resolution of this emergency motion requires the Court to reach the merits of Kaspersky Lab's constitutional challenge to Section 1634(a) before full briefing and argument, then the Court could stay the interim rule (and any other regulations the government might propose to implement Section 1634(a)) and postpone a decision on whether to stay Section 1634(a) itself until argument.

Dated: July 9, 2018

Respectfully submitted,

/s/ Ryan P. Fayhee

Ryan P. Fayhee, D.C. Bar No. 1033852
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: ryan.fayhee@hugheshubbard.com
Email: scott.christensen@hugheshubbard.com
Email: stephen.halpin@hugheshubbard.com

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

CERTIFICATE OF COMPLIANCE

I certify that, pursuant to Fed. R. App. P. 27(d), the foregoing reply is proportionately spaced, has a typeface of 14-point or more, and contains 2,591 words.

Dated: July 9, 2018

/s/ Ryan P. Fayhee
Ryan P. Fayhee
HUGHES HUBBARD & REED LLP
1775 I Street, N.W.
Washington, D.C. 20006-2401
Telephone: (202) 721-4600
Email: ryan.fayhee@hugheshubbard.com

Attorney for Plaintiffs–Appellants

CERTIFICATE OF SERVICE

I hereby certify that on July 9, 2018, I electronically filed the foregoing Reply 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 on July 10, 2018. I also certify that I have caused the foregoing to be electronically mailed to:

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

Sam M. Singer
Trial Attorney
Civil Division, Federal Programs Branch
U.S. Department of Justice
20 Massachusetts Ave, N.W.
Washington, D.C. 20001
Office: (202) 616-8014
Fax: (202) 616-8460
Samuel.M.Singer@usdoj.gov

Dated: July 9, 2018

/s/ Ryan P. Fayhee
Ryan P. Fayhee D.C. Bar No. 1033852