ORAL ARGUMENT SCHEDULED SEPTEMBER 14, 2018

Nos. 18-5176 & 18-5177

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

KASPERSKY LAB, INC. and KASPERSKY LABS LIMITED,

Plaintiffs–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,

Defendants–Appellees.

On Appeal From the United States District Court for the District of Columbia, Nos. 1:17-cv-02697 & 1:18-cv-00325, Honorable Colleen Kollar-Kotelly

REPLY BRIEF OF APPELLANTS

Ryan P. Fayhee
Scott H. Christensen
Stephen R. Halpin III
HUGHES HUBBARD & REED LLP
1775 I Street, N.W.
Washington, D.C. 20006-2401
Telephone: (202) 721-4600
Email: ryan.fayhee@hugheshubbard.com
Email: scott.christensen@hugheshubbard.com
Email: stephen.halpin@hugheshubbard.com

Attorneys for Plaintiffs–Appellants

Table of Contents

Page

Table of Authorities

Page(s)

Cases

---

* Authorities upon which Kaspersky Lab chiefly relies are marked with asterisks.

Table of Authorities
(Continued)

Page(s)

Statutes and Rules

Legislative and Administrative Proceedings

Table of Authorities
(Continued)

Page(s)

Periodical Materials

Glossary

APA	Administrative Procedure Act, 5 U.S.C. §§ 500–596
Bill of Attainder Case	*Kaspersky Lab, Inc. v. United States*, No. 1:18-cv-00325 (CKK) (D.D.C.)
BOD	Binding Operational Directive 17-01, dated September 13, 2017
BOD Case	*Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec.*, No. 1:17-cv-02697 (CKK) (D.D.C.)
NDAA	National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, 131 Stat. 1283 (2018)

Summary of Argument

The District Court's decision on the Bill of Attainder Case should be reversed because the court applied an erroneous substantive legal standard and confused the applicable procedural standards. In determining that the Bill of Attainder Complaint failed to state a claim, the District Court misinterpreted the substantive legal principles that guide the bill of attainder inquiry. The District Court then analyzed material outside the Bill of Attainder Complaint—which it judicially noticed without the required procedural safeguards—under its incorrect substantive standard to rule in favor of the government. The government's opposition offers nothing to excuse those errors and, at points, supports Kaspersky Lab's arguments.

The District Court further erred by relying on its flawed analysis of the Bill of Attainder Complaint to dismiss the BOD Case. This Court should reject the government's request to decide any aspect of the BOD Case on a ground that the District Court did not reach.

For the reasons below and in Kaspersky Lab's opening brief, this Court should reverse and remand the orders of the District Court in the Bill of Attainder and BOD Cases.

Argument

I. The District Court's decision on Section 1634(a) should be reversed.

A. Section 1634(a) is a bill of attainder.

1. The government ignores precedent and relies on discarded law.

The parties agree that a burden can be an unconstitutional bill of attainder even if it is "not precisely identical to any of the burdens historically recognized as punishment." *Foretich v. United States*, 351 F.3d 1198, 1219 (D.C. Cir. 2003); *see* Gov't Opp'n at 31 ("[T]his Court has not narrowly limited the historic test to the checklist of statutory deprivations and disabilities previously deemed to be bills of attainder."). The government's assertions that Section 1634(a) is not identical to prior punishments, *see* Gov't Opp'n at 21–22; *id.* at 31–32, are of no moment.

The Supreme Court has explained that "the Bill of Attainder Clause was not to be given a narrow historical reading." *United States v. Brown*, 381 U.S. 437, 447 (1965). More than 150 years ago the Court held that "[t]he deprivation of any rights, civil or political, previously enjoyed, may be punishment, the circumstances attending and the causes of the deprivation determining this fact." *Cummings v. Missouri*, 71 U.S. (4 Wall.) 277, 320 (1867). "Disqualification . . . from positions of trust" can be a punishment prohibited by the Bill of Attainder Clause. *Id.* The government's repeated claim that Kaspersky Lab has not alleged a "constitutional right" infringed by Section 1634(a), *see* Gov't Opp'n at 22; *id.* at 35, is baseless.

See, e.g., Kaspersky Lab's Opening Br. at 21–24; *id.* at 23 ("Among the rights protected under the Bill of Attainder Clause is the right to be free from defamation of one's reputation."); *id.* ("The economic injury resulting from the legislature casting aspersions on a group is prohibited by the Constitution[.]"). And the government's assertion that "Kaspersky makes no claim that Section 1634 violates any guarantee of political or religious freedom," Gov't Opp'n at 32; *see id*. at 22, disregards Supreme Court precedent that punishment is not limited to the deprivation of "life, liberty, and property," but instead encompasses "every right known to the law," *Cummings*, 71 U.S. (4 Wall.) at 320.

The government claims that Congress "imposed no other limitation on Kaspersky's ability to conduct business in the United States" beyond "an unambiguous statutory prohibition against the use of Kaspersky products and services." Gov't Opp'n at 25. Asserting that Section 1634(a) is not punishment because "Kaspersky Lab is not prevented from operating as a cybersecurity business," J.A. 197; *see* Gov't Opp'n at 21, evokes the argument that banning confederates or communists from working as lawyers, priests, trade unionists, or government employees does not prevent them from working altogether. That argument has not prevented the Supreme Court from repeatedly striking down such bans as bills of attainder. *See Brown*, 381 U.S. at 449–50; *United States v. Lovett*, 328 U.S. 303, 315–16 (1946); *Ex parte Garland*, 71 U.S. (4 Wall.) 333, 377

(1867); *Cummings*, 71 U.S. (4 Wall.) at 320. In all of those cases, the legislature "imposed no other limitation" on the affected parties beyond a prohibition on certain employment.

2. Section 1634(a) punishes Kaspersky Lab for past action.

As the Supreme Court explained in *Brown*, "[i]t would be archaic to limit the definition of 'punishment' to "retribution.' Punishment serves several purposes; retributive, rehabilitative, deterrent—and preventive. One of the reasons society imprisons those convicted of crimes is to keep them from inflicting future harm, but that does not make imprisonment any the less punishment." 381 U.S. at 457. The Court emphasized that its 1950 decision in *American Communications Association, C.I.O. v. Douds*, 339 U.S. 382 (1950), "misread" prior precedent to the extent *Douds* suggested a law must punish past action to be a bill of attainder. *See Brown*, 381 U.S. at 460.[1] The government agrees that bills of attainder are not

---

1. The Supreme Court in *Douds* ruled that section 9(h) of the Labor Management Relations Act of 1947, which required officers of labor organizations to sign affidavits disavowing the Communist Party, was not a bill of attainder. *See* 339 U.S. at 385–86, 413–15. The Court reasoned that there was a "decisive distinction" between prior bill of attainder precedents and the statute at issue in *Douds*: "in the previous decisions the individuals involved were in fact being punished for *past* actions; whereas in this case they are subject to possible loss of position only because there is substantial ground for the congressional judgment that their beliefs and loyalties will be

(Footnote continued on next page)

limited to punishment for past action. *See* Gov't Opp'n at 23 n.5 (citing *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 476 n.40 (1977)). Twice in its brief, however, the government calls "decisive" its contention that Section 1634(a) prevents only future conduct and does not punish past action. The government is wrong, both on the law and the facts.

On the law, the government asks this Court to rely on the *Douds* past action/future action distinction that the Supreme Court discarded in *Brown*. *See* Gov't Opp'n at 22–23 ("Where Congress legislates 'to prevent future action rather than to punish past action,' and there are 'substantial ground[s] for the congressional judgment,' the distinction is 'decisive'; the statute is not a bill of attainder." (quoting *Douds*, 339 U.S. at 413)); *id.* at 32 (the fact that, according to the government, "Congress enacted Section 1634 'to prevent future action rather than to punish past action'" is "decisive" (quoting *Douds*, 339 U.S. at 413–14)). The *Brown* Court made explicit that "[h]istorical considerations by no means

---

(Footnote continued from previous page)

transformed into future conduct." *Id.* at 413. The Court concluded that "the intention [of section 9(h)] is to forestall future dangerous acts" and that "there is no one who may not by a voluntary alteration of the loyalties which impel him to action, become eligible to sign the affidavit." *Id.* at 414.

compel restriction of the bill of attainder ban to instances of retribution." 381 U.S. at 458. The government's invitation to rely on bad law should be declined.

Moreover, contrary to the government's assertion, *see* Gov't Opp'n at 23; *id.* at 32, Congress did in fact pass Section 1634(a) to punish past action. Executive branch officials based their banishment in part on past action in issuing the BOD, *see, e.g.*, J.A. 68, and, according to the government, Congress relied on those executive branch officials in enacting Section 1634(a), *see* Gov't Opp'n at 34. The government itself explained that banning Kaspersky Lab from government service was based on past action in Russia, including the fact that Eugene Kaspersky graduated 30 years ago from an institute "sponsored" in part by Russian military and defense agencies, later worked for the Ministry of Defense, and, according to a *Bloomberg* article from March 20, 2015, "rarely misses a weekly *banya* (sauna) night with a group of 5 to 10 that usually includes Russian intelligence officials." J.A. 39, 68; *see* Gov't Opp'n at 5–6. The government describes these and other activities as "certain ties, past and present." J.A. 68.

The Supreme Court has made clear that legislation need not be retributive to be a bill of attainder. The government is incorrect to suggest otherwise. In any event, the government's asserted justification for Section 1634 includes retributive reasons.

3. Banishing a single company based on general concerns that affect others is punishment.

The government asks this Court to rely on what it calls "the legislative record" or "legislative background" to defend the granting of a motion to dismiss. *See, e.g.*, Gov't Opp'n at 14–15.[2] The legislative material to which the government points singles out Kaspersky Lab for banishment from a background of cyberthreats from Russia that encompass all antivirus or cybersecurity providers. 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.'" *Foretich*, 351 F.3d at 1224 (emphasis omitted) (quoting *Selective Serv. Sys. v. Minn. Pub. Interest Research Grp.*, 468 U.S. 841, 847 (1984)).

In *Foretich*, the government asserted that the legislation at issue 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

---

2. The government prefers the terms "legislative record" and "legislative background" over "legislative history," perhaps because so little of what the government relies on can be found in the legislative history of the NDAA in general or Section 1634 in particular.

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

Here, the government claims that "Congress had ample foundation for Section 1634 in the expert, predictive judgments of executive branch officials entrusted with protecting the national security." Gov't Opp'n at 34. But the executive branch's judgment was based on:

- "[A]ll antivirus software 'operates with broad file access and elevated privileges.'" Gov't Opp'n at 5 (quoting J.A. 30).
- "Russian law authorizes the Russian Federal Security Service (FSB) 'to compel Russian enterprises to assist the FSB in the execution of FSB duties, to second FSB agents to Russian enterprises (with the enterprise's consent), and to require Russian companies to include hardware or software needed by the FSB to engage in 'operational/technical measures.'" *Id.* (quoting J.A. 30).

- "Kaspersky 'relies on the FSB for needed business licenses and certificates.'" *Id.* (quoting J.A. 30) (Although, "[a]ll information technology companies involved in cryptography-related activities operating in Russia (including leading U.S. companies) are required to obtain the same licenses and certificates from the FSB." J.A. 18 (Kaspersky Lab Complaint in the BOD Case)).[3]

- "'Russian law allows the FSB to intercept all communications transiting Russian telecommunication and Internet Service Provider networks.'" Gov't Opp'n at 6.

- "Kaspersky officials have 'personal and professional ties to Russian government agencies,' such as Russian intelligence agencies." *Id.*[4]

With the exception of the last point, these purported threats to national security (if accurate) describe any producer of antivirus and cybersecurity software doing business in Russia and using Russian networks to communicate. But Section

---

3. *See also* J.A. 37 (The FSB "has a regulatory role in licensing companies to engage in encryption-related activities and handle state secrets, as well as issuing certificates for individual products that use encryption and/or process state secrets," and "Kaspersky obtains licenses and certificates from the FSB like other regulated companies.").

4. See page 6 above for purported personal and professional ties, including Mr. Kaspersky attending a weekly sauna night with a group that usually includes Russian officials. *See* J.A. 38–39, 68. In addition, Kaspersky Lab's "officials might have 'acquaintances, friends, and professional relationships within the [Russian] government,'" *id.* at 68, which also easily might be true of other antivirus and cybersecurity providers that do business in Russia.

1634(a) targets only Kaspersky Lab.[5] As in *Foretich*, Section 1634(a) has a broad justification and a narrow application to one entity. Congress does not have constitutional license to single out a particular company for banishment as a federal contractor based on a weak soup of statements that affect a whole segment of the cybersecurity economy.

The government contends that Congress relied on executive branch officials' repeated conclusions that "the presence of Kaspersky-branded products . . . on federal information systems, presents a known or reasonably suspected information security threat, vulnerability, and risk to federal information and information

---

5. 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 affected many other high-profile cybersecurity vendors. Many do business in Russia and have 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.").

systems." J.A. 48; *see id.* at 29, 30, 32, 33, 34, 46, 49, 51; Gov't Opp'n at 34. The government further asserts that Congress's conclusion that Kaspersky Lab's products pose a national-security risk "does not necessarily (and not even inferentially) suggest legislative opprobrium of the company." Gov't Opp'n at 29. That is not credible. If Congress passed a law banning the federal government from using any airplanes manufactured by Wright Bros., Inc., because Congress stated the planes posed a national security risk, common sense dictates that airlines would not purchase Wright Bros. planes in the same quantity and passengers would avoid airlines that flew Wright Bros. planes.

Here, the federal government branding Kaspersky Lab a cyberthreat impairs the cybersecurity company's ability to operate. Worse than *Foretich v. United States*, 351 F.3d 1198 (D.C. Cir. 2003), Congress directed a loss of business by excluding Kaspersky Lab from the rolls of federal contractors. 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 (discussing the injury that gave Dr. Foretich standing to sue); *see also id.* at 1220 (the punishment imposed on Dr. Foretich is "not dissimilar to the types of burdens traditionally

recognized as punitive" and "may be of even greater magnitude than many of those at issue in the historical cases").[6]

The government also contends that in the Supreme Court's earlier cases "there was no suggestion . . . that Congress had established a legislative record demonstrating its good-faith determination that the regulated conduct would pose a significant national security risk." Gov't Opp'n at 35. That contention is wrong. The legislative histories of the statutes struck down in *Lovett* and *Brown* are replete with appeals to national security. For example, the House Report on the law struck down in *Lovett* observed:

> - "[A]ny government employee who fosters or sponsors or supports any organization which would undermine this foundation for a free government ought not to be

---

6. Since the publication of the Federalist Papers and the decision in *United States v. Brown*, 381 U.S. 437 (1965), the Supreme Court has recognized that corporations are protected by many constitutional rights. *See* Kaspersky Lab's Opening Br. at 12–13, n.5. One sister circuit has held that corporations are protected from punishment under the Bill of Attainder Clause. *See Consol. Edison Co. of New York v. Pataki*, 292 F.3d 338, 348 (2d Cir. 2002) ("[B]ills of attainder historically have targeted corporations as well as natural persons. Con Ed cites several English statutes that imposed disabilities on English boroughs, hardly natural persons." (citations omitted)). And this Court has assumed that conclusion. *See* Kaspersky Lab's Opening Br. at 11–12. While there are differences between a corporation and an individual, none of those differences make a difference to the bill of attainder analysis here, and the government does not articulate any reason to the contrary. *See* Gov't Opp'n at 18 n.3.

> employed by any department of Government in any position of trust." H.R. Rep. No. 78-448, at 5 (1943).
>
> - "If our military leaders on the far-flung battle fronts have deemed it wise and necessary to safeguard and protect our boys against false and distorted doctrines and philosophies, it would seem equally necessary and important that we on the home front should give a similar protection and safeguard to our soldiers and citizens at home, against entrusting official responsibility to those whose acts, philosophies, and teachings would destroy us from within." *Id.*
>
> - "[I]f the principles of our national structure are subverted and entombed their resurrection will cost a far greater sacrifice than we are paying today . . . ." *Id.* at 12.

Similar examples abound in the legislative history of the statute struck down in *Brown*:

> - "The Congress finds that, in the public interest, it continues to be the responsibility of the Federal Government to protect employees' rights to organize, choose their own representatives, bargain collectively . . . that the relations between employers and labor organizations and the millions of workers they represent have a substantial impact on the commerce of the Nation." Labor-Management Reporting and Disclosure Act of 1959, § 2(a), Pub. L. No. 86-257, 73 Stat. 519, 519 (1959).
>
> - The purpose of this Senate report was to "conduct an investigation and study of the extent to which criminal and other improper practices or activities are, or have been engaged in in the field of labor-management relations or in groups or organizations of employees or employers, to the detriment of the interests of the public." S. Rep. No. 85-1417, at 1 (1958). "Gangsters and hoodlums have successfully infiltrated some labor unions, sometimes at high levels. (a) They have assumed

> positions of trust in some labor unions. (b) They have exercised sinister influence over other union officials. (c) Higher union authority has shown no desire to rid the labor movement of those with lengthy criminal records." *Id.* at 6.

- "The committee adopted section 504 of the committee bill as a more effective restriction against Communist infiltration of labor organizations." H.R. Rep. No. 86-741, at 791 (1959).

Lovett and *Brown* make clear what the government ignores: the "attainder inquiry is in fact more exacting than a rational basis test, because it demands purposes that are *not merely reasonable but nonpunitive*." *BellSouth Corp. v. FCC*, 144 F.3d 58, 67 (D.C. Cir. 1998) ("*BellSouth I*") (emphasis added).

Congress cannot invoke the specter of "national security" and expect the courts to relent without further inquiry. The Founders were mindful of the danger that "[t]he legislative department," absent an independent judiciary, would be "every where extending the sphere of its activity, and drawing all power into its impetuous vortex." *See Plaut v. Spendthrift Farm, Inc.*, 514 U.S. 211, 221–22 (1995) (quoting The Federalist No. 48, at 333, 337 (James Madison) (J. Cooke ed., 1961)). As the Supreme Court reiterated in *Nixon v. Administrator of General Services*, "the Bill of Attainder Clause . . . 'reflect[s] . . . the Framers' belief that the Legislative Branch is not so well suited as politically independent judges and juries to the task of ruling upon the blameworthiness of, and levying appropriate

punishment upon, specific persons.'" 433 U.S. 425, 469 (1977) (quoting *Brown*, 381 U.S. at 445).[7]

4. There are less burdensome alternatives.

In assessing whether a law imposes punishment, "it is often useful to inquire into the existence of less burdensome alternatives by which that legislature (here Congress) could have achieved its legitimate nonpunitive objectives." *Nixon*, 433 U.S. at 482; *see Foretich*, 351 F.3d at 1222; *see also Consol. Edison Co. of New York v. Pataki*, 292 F.3d 338, 354 (2d Cir. 2002) (law was punishment under the functional test because the legislature "made no attempt whatsoever to ensure that the costs imposed on Con Ed were proportional to the problems that the legislature could legitimately seek to ameliorate"). Here, as Kaspersky Lab has argued

7. The legislation at issue in *Nixon* nullified a portion of a depository agreement the former President had entered into that would have allowed for the destruction of certain presidential records, including tape recordings. *See* 433 U.S. at 430–36. None of the records of other past presidents were in jeopardy, because all "were already housed in functioning Presidential libraries," so Mr. Nixon "constituted a legitimate class of one." *Id*. at 472. Congress's motivation to "guarantee the availability of evidence for use at criminal trials," *id.* at 477, and "preserv[e] monuments and records of historical value to our national heritage," *id.* at 478, could hardly have been seen as punitive.

previously, Congress could have achieved the same national security objective by means that were less burdensome to Kaspersky Lab.[8]

For example, 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 provides information to the FSB, does business in Russia, has servers in Russia, or uses Russian networks. The 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 interactions with private enterprises doing business in Russia, and the FSB's ability to intercept communications on Russian networks. *See* Gov't Opp'n at 11–12. Such a law of general applicability would have allowed companies to decide whether to continue operating in Russia or to remain a federal contractor. As in *Foretich*, "[i]f the disputed Act had been enacted to apply to all" cybersecurity vendors, "this would be a different case." *See* 351 F.3d at 1223. The fact that Kaspersky Lab "was

8. Among the reasons why debarment would have been a less burdensome alternative is that there is a well-established mechanism in the Federal Acquisition Regulation to debar a contractor with procedural safeguards that the government considered and rejected here. *See* J.A. 32.

singled out for [the] severe burden" of a permanent prohibition "belies the claim that Congress's purposes were nonpunitive." *Id*. at 1224.

B. The government fails to explain why the District Court could take judicial notice beyond the Bill of Attainder Complaint to dismiss that case.

The government asserts Kaspersky Lab's procedural arguments on the Bill of Attainder Case lack merit because the District Court "consolidated Kaspersky's two suits and resolved them both in a single opinion." Gov't Opp'n at 42. That is an inexact way of describing why the District Court's bill of attainder decision should be reversed on procedural grounds. (The District Court consolidated the two cases "solely for the purpose of briefing an upcoming round of dispositive motions," including the cross-motions for summary judgment on the administrative record in the BOD Case and the government's motion to dismiss the Bill of Attainder Case. J.A. 168 (Order of the District Court dated Feb. 16, 2018).[9]) The District Court erred by disregarding the different procedural postures of the two cases and resolving them as if they were one case. In particular, the District Court judicially noticed the truth of selected material from the "legislative record" of the NDAA and the administrative record in the BOD Case—both beyond the four

9. Docket entry 17 in case no. 1:17-cv-02697 and docket entry 7 in case no. 1:18-cv-00325.

corners of the Bill of Attainder Complaint—to resolve a motion to dismiss that case under Rule 12(b)(6) of the Federal Rules of Civil Procedure.

The government contends that "[t]he district court fully complied with the applicable standard" when it took judicial notice of various legislative and administrative proceedings swirling around Russian cyberthreats. *See* Gov't Opp'n at 44.[10] But a court cannot take judicial notice of the truth of the contents of statements made in Congress or documents from a separate administrative proceeding. In applying Rule 201 of the Federal Rules of Evidence, courts distinguish public documents offered for their existence from those offered for the truth of their contents, holding that judicial notice of the latter is inappropriate because the underlying facts are open to dispute. *See* Kaspersky Lab's Opening Br. at 45–47 (discussing *Hurd v. District of Columbia*, 864 F.3d 671 (D.C. Cir. 2017)); *accord Global Network Commc'n, Inc. v. City of New York*, 458 F.3d 150, 157 (2d Cir. 2006) ("A court may take judicial notice of a document filed in another court not for the truth of the matters asserted in the other litigation, but rather to establish the fact of such litigation and related filings." (quoting *Int'l Star*

---

10. Nowhere does the government address Kaspersky Lab's argument that, at minimum, Kaspersky Lab was entitled to notice and an opportunity to be heard before the District Court took judicial notice. *See* Kaspersky Lab's Opening Br. at 45 (citing Fed. R. Evid. 201(e)); *id.* at 47. That alone is enough to reverse the dismissal of the Bill of Attainder Case.

Class Yacht Racing Ass'n v. Tommy Hilfiger U.S.A., Inc., 146 F.3d 66, 70 (2d Cir. 1998))); *Torrens v. Lockheed Martin Servs. Grp., Inc.*, 396 F.3d 468, 473 (1st Cir. 2005); *United States v. Bonds*, 12 F.3d 540, 553 (6th Cir. 1993).

The legislative history the Supreme Court judicially noticed in *Territory of Alaska v. American Can Co.*, 358 U.S. 224, 226–27 (1959)—one of two cases the government cites on judicial notice[11]—was the deletion of a statutory provision that "never became part of the law," not the truth of any assertion made in Congress. The "legislative history" at issue in *Territory of Alaska* centered on changes to the statutory text itself, not statements by lawmakers or testimony from hearing witnesses.

The mixed contents of the government's "legislative record" further demonstrate why judicial notice of such material for its truth is inappropriate. This Court has explained that "[t]he individual opinions of witnesses at [congressional]

---

11. The government also cites *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308 (2007), for the uncontroversial proposition that "courts may consider 'matters of which a court may take judicial notice' in deciding a motion to dismiss." Gov't Opp'n at 44 (quoting *Tellabs*, 551 U.S. at 322). For example, in a defamation case, this Court "drew on a filing in an unrelated case as a record of what was said. But [the Court] did not, and could not, rely on it for the truth of the matter asserted." *Hurd*, 864 F.3d at 686. The citation to *Tellabs* does not support the government's position that the District Court was entitled to assume the truth of certain statements by lawmakers and hearing witnesses in ascertaining the congressional intent behind Section 1634(a).

hearings are of dubious value in interpretation of legislation." *March v. United States*, 506 F.2d 1306, 1314 n.30 (D.C. Cir. 1974) (citation omitted). In particular, "[r]emarks . . . made in the course of legislative debate or hearings other than by persons responsible for the preparation or the drafting of a bill are entitled to little weight." *Ernst & Ernst v. Hochfelder*, 425 U.S. 185, 203–04 n.24 (1976); *see Regan v. Wald*, 468 U.S. 222, 237 (1984) ("Oral testimony of witnesses and individual Congressmen, unless very precisely directed to the intended meaning of particular words in a statute, can seldom be expected to be as precise as the enacted language itself."); *Austasia Intermodal Lines, Ltd. v. Fed. Mar. Comm'n*, 580 F.2d 642, 645 (D.C. Cir. 1978) (Testimony at congressional hearings "should not be accorded undue weight as an indication of legislative intent . . . since the views expressed by witnesses at congressional hearings are not necessarily the same as those of the legislators ultimately voting on the bill." (citations omitted)).

Here, the government relies on congressional hearings spread out over months on cyberthreats in general, including from Russia. Those hearings have little connection to the text of the NDAA or Section 1634(a) in particular. The hearings covered topics ranging from Russian interference with the 2016 U.S.

elections[12] and Russian active measures and influence campaigns[13] to worldwide threats to U.S. national security[14] and defense acquisition reform efforts.[15] As noted above, legislation that targets Kaspersky Lab against a backdrop of testimony about a much broader problem affecting other companies only further supports that Section 1634(a) is punishment of Kaspersky Lab.

The government points to the fact that Senator Marco Rubio asked multiple hearing witnesses whether they would use Kaspersky Lab products on their computers. *See* Gov't Opp'n at 9.[16] The government is fond of pointing to the

---

12. *Russian Interference in the 2016 U.S. Elections: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. (June 21, 2017).

13. *Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Panel II: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. (Mar. 30, 2017).

14. *Open Hearing on Worldwide Threats: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. (May 11, 2017).

15. *Department of Defense Acquisition Reform Efforts: Hearing Before the S. Comm. on Armed Servs.*, 115th Cong. (Dec. 7, 2017). Senator Jeanne Shaheen was the only senator to speak about Kaspersky Lab and noted that she had "been banging the drum" on cyber concerns, "particularly with respect to Kaspersky software." *Id*. at 42.

16. Senator Rubio described the "open source reports" on which he relied, *see* Gov't Opp'n at 9, as "a Bloomberg article . . . and others." The Bloomberg article presumably is the March 2015 *Bloomberg* report about Eugene Kaspersky going to the sauna with friends in the Russian government. In any event, Senator Rubio is not a member of the committee that reported the

(Footnote continued on next page)

single-word answers of six members of the executive branch. *See id.* at 6, 10, 34. But the government ignores the testimony of other expert witnesses. One expert answered Senator Rubio's question about using Kaspersky Lab products: "I would, yes. I would also use a competing product at the same time. Always a bit of redundancy never harms." *Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Panel II: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. 40 (Mar. 30, 2017) (statement of Dr. Thomas Rid, Professor of Security Studies at Kings College, London). He went on to testify that "Kaspersky is not an arm of the Russian government if we look at the publicly available evidence. Kaspersky has published information about Russian cyber attack[s], cyber intrusion campaigns, digital espionage, about several different Russian campaigns. Name any American company that publishes information about American digital espionage?" *Id.* Another expert testified that "[t]here's no doubt [about] the efficacy of Kaspersky's products," but other products would

---

(Footnote continued from previous page)

NDAA, nor did he vote on the bill's passage. *See* U.S. Senate, *Roll Call Vote 115th Congress – 1st Session* (Sept. 18, 2017). His remarks carry no weight in discerning congressional intent. *See United States v. United Mine Workers of Am.*, 330 U.S. 258, 276–77 (1947) ("Mr. Beck was not a member of the Judiciary Committee which reported the bill, and did not vote for its passage. We do not accept his views as expressive of the attitude of Congress relative to the status of the United States under the Act.").

provide better protection in the United States because different locations in the world face different cyberthreats. *Id*. (statement of Kevin Mandia, Chief Executive Officer of FireEye, Inc., a global cybersecurity company).

The government's selective use of opinion testimony from congressional hearings is "akin to 'looking over a crowd and picking out your friends.'" Patricia M. Wald, *Some Observations on the Use of Legislative History in the 1981 Supreme Court Term*, 68 Iowa L. Rev. 195, 214 (1983) (quoting Judge Harold Leventhal). Statements before congressional committees are not subject to judicial notice for their truth and are not a reliable basis on which to ground a judicial determination of congressional intent. As to the BOD administrative record, the government cites no support for the proposition that a court can judicially notice the truth of an administrative record from a separate proceeding to decide a motion to dismiss.

By contrast, courts can judicially notice that Senator Jeanne Shaheen, who sponsored Section 1634(a), published a variety of statements that singled out Kaspersky Lab for opprobrium. A court can notice that those statements were made without ascribing any truth to their contents. Indeed, Kaspersky Lab denies the truth of Senator Shaheen's statements, which are tied to her introduction of the proposed statutory language that became Section 1634(a). *See* J.A. 158 ("When

broad defense legislation comes before the Senate in the weeks ahead, I hope to amend it to ban Kaspersky software from all of the federal government.").

At bottom, the government advances a procedure that would allow for easy dismissal of any challenge to a law passed by Congress. First, the government asserts that testimony during congressional hearings that never discussed the proposed statutory text and was not included in the committee reports on the bill—as well as a separate administrative record developed by a federal agency—forms the "legislative background" or "legislative record" of a law passed by Congress. *See, e.g.*, Gov't Opp'n at 26. Further, according to the government, not only is it appropriate for courts to consider such tangential "legislative material" when interpreting the text of the statute, but they are also entitled to judicially notice the truth of that material (including testimony by nonlawmakers) to determine what Congress intended. *See id.* at 44. Finally, the government maintains that the courts review only whether Congress acted "rational[ly]" on the basis of the selected quotations from the "legislative material" the court has already accepted as true. *See id.* As the Supreme Court recently observed in another context, this is "a sort of interpretive triple bank shot, and just stating the theory is enough to raise a judicial eyebrow." *See Epic Sys. Corp. v. Lewis*, 138 S. Ct. 1612, 1626 (2018). The District Court committed reversible procedural error in dismissing the Bill of Attainder Complaint.

II. The District Court's decision on the BOD should be reversed.

In response to Kaspersky Lab's argument that the District Court erred by ignoring Kaspersky Lab's procedural due process claim in the BOD Case, *see* Kaspersky Lab's Opening Br. at 52–53, the government asks this Court to affirm the District Court's dismissal on the "alternative ground" that Kaspersky Lab failed to state a claim. *See* Gov't Opp'n at 50–53 (citing *Parsi v. Daioleslam*, 778 F.3d 116, 126 (D.C. Cir. 2015)).[17] This Court typically does not consider questions that the district court did not have occasion to reach. *See United States v. Peyton*, 745 F.3d 546, 557 (D.C. Cir. 2014) ("We are a court of review, not of first view, and the district court . . . had no occasion to address this issue."). The government's

17. It is not clear whether the government believes this Court could affirm the entire BOD dismissal on the alternative ground that Kaspersky Lab received sufficient due process. *See* Gov't Opp'n at 50. To the extent that is the government's position, the government conflates the substantive Administrative Procedure Act ("APA") and procedural due process claims that Kaspersky Lab alleged in its complaint. *See* J.A. 21–22 ¶¶ 82–88. Kaspersky Lab's substantive APA claim focuses on whether the BOD was "supported by substantial evidence," whether the Department of Homeland Security "identif[ied] a rational connection between the facts before it and the conclusions it reached," and whether the BOD was otherwise "arbitrary and capricious and an abuse of agency discretion." *See id.* at 21–22 ¶¶ 87–88. The government's erroneous argument that the Department of Homeland Security provided Kaspersky Lab sufficient notice and an opportunity to be heard, *see* Gov't Opp'n at 50–53, has no bearing on the substantive APA claim.

case, *Parsi*, 778 F.3d at 126, illustrates the principle: "Here, the District Court expressly anchored its sanctions in two sources of judicial power—Rule 37 and the inherent power of courts—and we will only affirm if it correctly exercised these powers, notwithstanding Daioleslam's invitation to consider other bases of authority."

Conclusion

For the foregoing reasons, the orders of the District Court should be reversed.

Dated: August 13, 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. 32 (a)(7)(B), the foregoing Reply Brief of Appellants is proportionately spaced, has a typeface of 14-point or more, and contains 6,262 words excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

Dated: August 13, 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 August 13, 2018, I electronically filed the foregoing Reply Brief of Appellants with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system. I also certify that I will cause paper copies of the Brief to be hand delivered to the Court on August 14, 2018. The following participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system:

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

Dated: August 13, 2018

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