United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued September 14, 2018 Decided November 30, 2018

No. 18-5176

KASPERSKY LAB, INC. AND KASPERSKY LABS LIMITED,
APPELLANTS

v.

UNITED STATES DEPARTMENT OF HOMELAND SECURITY AND KIRSTJEN M. NIELSEN, IN HER OFFICIAL CAPACITY AS SECRETARY OF HOMELAND SECURITY,
APPELLEES

Consolidated with 18-5177

Appeals from the United States District Court
for the District of Columbia
(No. 1:17-cv-02697)
(No. 1:18-cv-00325)

Scott H. Christensen argued the cause for appellants. With him on the briefs were *Ryan P. Fayhee* and *Stephen R. Halpin III*.

Lewis S. Yelin, Attorney, U.S. Department of Justice, argued the cause for appellees. With him on the brief was *H. Thomas Byron, III*.

Before: TATEL, *Circuit Judge*, and EDWARDS and GINSBURG, *Senior Circuit Judges*.

Opinion for the Court filed by *Circuit Judge* TATEL.

TATEL, *Circuit Judge*: Kaspersky Lab is a Russian-based cybersecurity company that provides products and services to customers around the world. Recently, however, Kaspersky lost an important client: the United States government. In September 2017, based on concerns that the Russian government could exploit Kaspersky's access to federal computers for ill, the Acting Secretary of Homeland Security directed federal agencies to remove the company's products from government information systems. And a few months later, Congress broadened and codified that prohibition in the National Defense Authorization Act. Kaspersky sued, arguing that the prohibition constitutes an impermissible legislative punishment—what the Constitution calls a bill of attainder. The government responded that the prohibition is not a punishment but a prophylaxis necessary to protect federal computer systems from Russian cyber-threats. In consolidated cases, the district court concluded that Kaspersky failed to adequately allege that Congress enacted a bill of attainder and that the company lacked standing to bring a related suit against the Department of Homeland Security. The district court thus granted the government's motions to dismiss. We affirm.

I.

According to the allegations contained in Kaspersky's complaint, which we "must . . . accept . . . as true" at the motion-to-dismiss stage, *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007), Kaspersky Lab is one of the world's largest cybersecurity companies. *See* Complaint, *Kaspersky Lab, Inc. v. United States*, No. 1:18-cv-00325, ¶ 18

(D.D.C. Feb. 12, 2018) ("Compl."). Kaspersky operates in 200 countries and territories and maintains 35 offices in 31 of those countries. *Id.* The United States is one of Kaspersky's most important geographic markets, and Kaspersky has "a substantial interest in its ability to conduct federal government business." *Id.* ¶¶ 22–23.

Ranking among the world's top four cybersecurity vendors, Kaspersky "has successfully investigated and disrupted" cyberattacks by "Arabic-, Chinese-, English-, French-, Korean-, Russian-, and Spanish-speaking" hackers. *Id.* ¶¶ 20–21. Founded by a Russian national and headquartered in Moscow, Kaspersky boasts that its "presence in Russia and its deployment in areas of the world in which many sophisticated cyberthreats originate . . . makes it a unique and essential partner in the fight against such threats," including hacker groups with suspected connections to Russian intelligence services. *Id.* ¶ 20.

But the U.S. government has come to disagree. Around the beginning of 2017, executive and legislative branch officials began voicing concerns that Kaspersky's ties to Russia make it a proverbial fox in the government's cyber-henhouse: a threat to the very systems it is meant to protect.

The chorus of concern about Kaspersky began to swell in the spring of 2017. Between March and July of that year, Kaspersky garnered attention in at least five committee hearings before both houses of Congress. For example, at one hearing dedicated to the subject of Russian cyber-operations, Senator Marco Rubio highlighted "open source reports" detailing ties between Kaspersky's founder, Eugene Kaspersky, and the Russian Federal Security Service, successor to the KGB. *Disinformation: A Primer in Russian Active Measures and Influence Campaigns Panel II: Hearing*

Before the Senate Committee on Intelligence, 115th Cong., pt. 2, at 40 (2017). And at a later hearing, Senator Rubio asked six heads of various U.S. intelligence agencies, including the Central Intelligence Agency and the Federal Bureau of Investigation, whether they would install Kaspersky software on their own computers. All six replied no. *See Open Hearing on Worldwide Threats: Hearing Before the Senate Committee on Intelligence* ("*Worldwide Threats*"), 115th Cong. 48 (2017).

In September 2017, the Acting Secretary of Homeland Security issued Binding Operational Directive 17-01 (the "Directive"), which required most federal agencies to begin removing "Kaspersky-branded products" from their information systems within 90 days. National Protection and Programs Directorate; Notification of Issuance of Binding Operational Directive 17-01 and Establishment of Procedures for Responses ("BOD-17-01"), 82 Fed. Reg. 43,782, 43,783 (Sept. 19, 2017). Invoking her statutory authority to issue directives "for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk," 44 U.S.C. § 3552(b)(1), the Acting Secretary justified the Directive based on an interagency assessment of "the risks presented by Kaspersky-branded products," BOD-17-01, 82 Fed. Reg. at 43,783. The Directive gave Kaspersky roughly two months to submit a response and announced that the Acting Secretary would issue a final decision by mid-December. BOD-17-01, 82 Fed. Reg. at 43,784.

More congressional hearings followed. In October, the House Science Committee's Subcommittee on Oversight held a hearing on the potential threat posed by Kaspersky products to federal information systems. *See Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government: Hearing Before the*

House Subcommittee on Oversight, House Committee on Science, Space, and Technology, 115th Cong. 3 (2017). Several members expressed deep concerns about Eugene Kaspersky's personal and professional ties to Russia, citing reports that he was "educated at a KGB cryptography institute" and "worked for the Russian intelligence services before starting his software company." *Id.* at 12 (statement of Donald S. Beyer); *see also id.* at 4 (statement of Lamar S. Smith); *id.* at 8 (statement of Darin LaHood). The Committee also heard testimony about the susceptibility of the company's software to Russian exploitation, with one expert explaining that due to Russia's permissive "telecommunications surveillance and monitoring laws," Kaspersky could passively—in the absence of any "willful complicity or collaboration" in a Russian cyber-operation—provide the Russian government access to federal computers. *Id.* at 44 (testimony of Sean Kanuck).

The same subcommittee held a second hearing on November 14, this time to survey agencies' compliance with the Directive. *See Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive: Hearing Before the House Subcommittee on Oversight, House Committee on Science, Space, and Technology*, 115th Cong. 22 (2017). The subcommittee heard testimony from Jeanette Manfra, Assistant Secretary for Cybersecurity and Communications at the Department of Homeland Security, who described the Department's rationale for issuing the Directive. She emphasized three concerns. First, "certain Kaspersky officials" enjoy "ties" to "Russian intelligence and other government officials." *Id.* at 19. Second, Russian law "allow[s] Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks." *Id.* And third, all antivirus software, including Kaspersky's, receives "broad access" to the systems on which it operates. *Id.* So like a thief who has stolen

a security guard's master key, a cyberattacker can exploit antivirus software's "elevated privileges" to inflict serious damage on the systems the software ostensibly protects. *Id.* In the Department's view, Manfra concluded, the Directive "is a reasonable, measured approach to the information security risks posed by . . . [Kaspersky] products to the federal government." *Id.*

Congress apparently agreed with the Department of Homeland Security's assessment that Kaspersky software presented a serious threat. Earlier, in July 2017, when considering the Senate version of the National Defense Authorization Act for Fiscal Year 2018 ("NDAA"), the Senate Armed Services Committee, citing "reports that the Moscow-based company might be vulnerable to Russian government influence," recommended adding a provision that would prohibit the Department of Defense from using any Kaspersky software. Senate Armed Services Committee, *NDAA FY18 Executive Summary* 10 (2017), http://go.usa.gov/xU5JC; *see also* S. Rep. No. 115-125, at 302 (2017) (recommending "a provision that would prohibit any component of the Department of Defense from using, whether directly or through work with or on behalf of another element of the United States Government, . . . any software platform developed, in whole or in part, by Kaspersky Lab or any entity of which Kaspersky Lab has a majority ownership"). Later, after the Senate received the House version of the NDAA, Senator Jeanne Shaheen introduced an amendment that would prohibit all federal agencies from using Kaspersky products. *See* S. Amd. 663, 163 Cong. Rec. S4578 (daily ed. July 27, 2017). The final version of the NDAA, which included a version of Shaheen's amendment, *see* H.R. Rep. No. 115-404, at 460–62 (2017) (Conf. Rep.), passed the House on November 14 and the Senate on November 16.

The legislative prohibition on Kaspersky products appears in section 1634 of the NDAA. Subsections (a) and (b) require that, beginning October 1, 2018:

> 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.

NDAA, Pub. L. No. 115-91, § 1634, 131 Stat. 1283, 1740 (2017). In contrast to the narrow focus of subsections (a) and (b), subsection (c) of section 1634 mandates a broader review of federal cybersecurity, directing the Secretary of Defense, in consultation with other agency heads, to review and report on "the procedures for removing suspect products or services from the information technology networks of the Federal Government." *Id.* § 1634(c).

The President signed the NDAA in mid-December 2017, just a few days after the Secretary finalized the Directive.

Kaspersky filed suit shortly thereafter—or, more precisely, two Kasperskys filed two suits. Kaspersky Lab, Inc., a Massachusetts corporation, and Kaspersky Labs Limited, its U.K. parent (collectively, "Kaspersky"), first filed a complaint against the Department of Homeland Security. *See* Complaint, *Kaspersky Lab, Inc. v. U.S. Department of Homeland Security*, No. 1:17-cv-02697, ¶ 21 (D.D.C. Dec. 18, 2017). This case challenged the Directive under the Administrative Procedure Act; we shall call this the "Directive Case." The same two

companies then filed a second complaint, this time against the United States, alleging that the NDAA violates the Constitution's prohibition on bills of attainder. *See* Complaint, *Kaspersky Lab, Inc. v. United States*, No. 1:18-cv-00325, ¶ 4 (D.D.C. Feb. 12, 2018). We shall call this the "NDAA Case."

The district court consolidated the two cases for the purpose of resolving related dispositive motions, namely, cross-motions for summary judgment and a motion to dismiss in the Directive Case and a motion to dismiss in the NDAA Case. *Kaspersky Lab, Inc. v. U.S. Department of Homeland Security*, No. 1:17-cv-02697 (D.D.C. Feb. 16, 2018). The district court granted the government's motion to dismiss the NDAA Case for failure to state a claim, concluding that Kaspersky had failed to plausibly allege that section 1634 constitutes a bill of attainder. *See Kaspersky Lab, Inc. v. U.S. Department of Homeland Security*, 311 F. Supp. 3d 187, 205–18, 223 (D.D.C. 2018). Furthermore, because section 1634 covers more products and more agencies than the Directive, the court concluded that invalidating the Directive alone would redress none of Kaspersky's injuries, so it dismissed the Directive Case for lack of Article III standing. *See id.* at 218–23.

Kaspersky now appeals both orders. We review de novo a "district court's dismissal of a complaint for lack of standing or for failure to state a claim." *Washington Alliance of Technology Workers v. U.S. Department of Homeland Security*, 892 F.3d 332, 339 (D.C. Cir. 2018). We begin with the NDAA Case.

II.

Article I, Section 9, Clause 3 of the Constitution provides that "[n]o Bill of Attainder . . . shall be passed." Rarely litigated, the Bill of Attainder Clause nonetheless has real bite, and Kaspersky argues that section 1634's ban on the federal

government's use of Kaspersky products violates the Clause's prohibition on legislative punishment.

This court has previously assumed without deciding that the Bill of Attainder Clause's protection applies to corporations such as Kaspersky. *See BellSouth Corp. v. FCC* ("*BellSouth I*"), 144 F.3d 58, 63 (D.C. Cir. 1998) ("We assume, as do the parties, that the Bill of Attainder Clause protects corporations as well as individuals."); *see also Consolidated Edison Co. of New York v. Pataki*, 292 F.3d 338, 349 (2d Cir. 2002) (holding that corporations are "individuals" protected by the Bill of Attainder Clause). Acknowledging that the question remains open, the government does not argue here that the Clause protects individuals only. *See* Appellants' Br. 18 n.3 (stating that the court "need not resolve the question [of the Clause's applicability to corporations] in this case"). Therefore, absent an argument to the contrary and as in our previous cases, we shall continue to assume that the Bill of Attainder Clause extends to corporations.

To subjects of the British crown, bills of attainder meant a very particular thing: "parliamentary acts sentencing named persons to death without the benefit of a judicial trial." *BellSouth I*, 144 F.3d at 62. But our Constitution sweeps more broadly. Since early in our history, the Bill of Attainder Clause has been understood to prohibit all "bills of pains and penalties"—legislative acts imposing on specified individuals or classes punishments less severe than death, such as banishment, imprisonment, denial of the right to vote, or confiscation of property. *See Foretich v. United States*, 351 F.3d 1198, 1217 (D.C. Cir. 2003) (listing bills of pains and penalties); *BellSouth I*, 144 F.3d at 64 (same).

In the last two centuries, legislatures have innovated beyond death and banishment. But as punishments evolved

over time, so too did the courts' interpretation of the Clause. "Our treatment of the scope of the Clause has never precluded the possibility that new burdens and deprivations might be legislatively fashioned that are inconsistent with the bill of attainder guarantee." *Nixon v. Administrator of General Services*, 433 U.S. 425, 475 (1977). It is the job of the courts to "prevent[] Congress from circumventing the clause by cooking up newfangled ways to punish disfavored individuals or groups." *BellSouth I*, 144 F.3d at 65.

This job is not always straightforward. For example, in the post–Civil War years, the Supreme Court invalidated as bills of attainder laws prohibiting confederate sympathizers from serving as priests and lawyers, *see Cummings v. Missouri*, 71 U.S. 277, 319 (1866); *Ex Parte Garland*, 71 U.S. 333, 377–78 (1866), but not a law prohibiting convicted felons from practicing medicine, *see Hawker v. New York*, 170 U.S. 189, 191–92 (1898). Similarly, in the early Cold War period, the Court held that an alien was not punished by "the mere denial" of his Social Security benefits after the government deported him for being a communist. *See Flemming v. Nestor*, 363 U.S. 603, 605, 617 (1960). By contrast, the Court did invalidate as legislative punishments one statute in which Congress had mandated that "no salary or compensation should be paid" to three named federal employees suspected of engaging in "subversive" communist activities, *United States v. Lovett*, 328 U.S. 303, 305–13 (1946), and another statute in which Congress "ma[de] it a crime for a member of the Communist Party to serve as an officer or . . . an employee of a labor union," *United States v. Brown*, 381 U.S. 437, 438 (1965).

As this abridged history demonstrates, each bill of attainder case "has turned on its own highly particularized context." *Flemming*, 363 U.S. at 616. Regardless of their particulars, however, all bills of attainder share two basic

elements: "a law is prohibited under the bill of attainder clause 'if it (1) applies with specificity, and (2) imposes punishment.'" *Foretich*, 351 F.3d at 1217 (quoting *BellSouth Corp. v. FCC* ("*BellSouth II*"), 162 F.3d 678, 683 (D.C. Cir. 1998)). Because the government concedes, as it must, that section 1634 applies with specificity to Kaspersky, we focus on the second element, punishment.

A "punishment" is something more than a burden. *See Selective Service System v. Minnesota Public Interest Research Group*, 468 U.S. 841, 851 (1984) ("That burdens are placed on citizens by federal authority does not make those burdens punishment."). The task, then, is to distinguish permissible burdens from impermissible punishments. To do so, the Supreme Court instructs courts to conduct "three necessary inquiries":

> (1) whether the challenged statute falls within the historical meaning of legislative punishment; (2) whether the statute, "viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes"; and (3) whether the legislative record "evinces a congressional intent to punish."

Id. at 852 (quoting *Nixon*, 433 U.S. at 473, 475–76, 478). This court, while observing that "[t]he Court has applied each of these criteria as an independent—though not necessarily decisive—indicator of punitiveness," has explained that "the second factor—the so-called 'functional test'—'invariably appears to be the most important of the three.'" *Foretich*, 351 F.3d at 1218 (quoting *BellSouth II*, 162 F.3d at 684) (internal quotation marks omitted). We shall therefore begin with that test.

Functional Test

Courts need a sorting mechanism for distinguishing statutes with punitive purposes from statutes with merely burdensome effects. Put another way, the ultimate question is whether the burden is a means to an end or an end in and of itself. Seeking to answer this question, the functional test asks "whether the law under challenge, viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes." *Nixon*, 433 U.S. at 475–76. As we explained in our most recent bill of attainder case, *Foretich v. United States*, "where there exists a significant imbalance between the magnitude of the burden imposed and a purported nonpunitive purpose, the statute cannot reasonably be said to further nonpunitive purposes." 351 F.3d at 1221. In short: identify the purpose, ascertain the burden, and assess the balance between the two.

Importantly, the functional test provides an inferential tool; it does not impose an independent requirement. Although a serious imbalance may support an inference that the legislature's purported nonpunitive objective serves as a "smokescreen" for some undisclosed punitive purpose, *BellSouth I*, 144 F.3d at 66, an imperfect fit between purpose and burden does not necessarily prove punitive intent. The difference is nuanced but crucial: the question is not whether a burden is proportionate to the objective, but rather whether the burden is so disproportionate that it "belies any purported nonpunitive goals." *Foretich*, 351 F.3d at 1222.

Over the years and across cases, courts have considered a wide variety of factors in conducting this functional inquiry. Generally speaking, these factors fall into two categories.

First, a statute performs poorly on the functional test when its effect is significantly overbroad. *See Foretich*, 351 F.3d

at 1222 ("A grave imbalance or disproportion between the burden and the purported nonpunitive purpose suggests punitiveness, even where the statute bears some minimal relation to nonpunitive ends."). To determine whether the statute goes farther than necessary, courts compare the burden actually imposed with hypothetical "less burdensome alternatives" by which the legislature could have accomplished the same objective. *Nixon*, 433 U.S. at 482. A statute may be "less burdensome" when it includes procedural safeguards to "protect the constitutional and legal rights of [the] individual[s] adversely affected," *id.* at 477; lasts only temporarily or "sunsets" at a time certain, *BellSouth II*, 162 F.3d at 683; allows the affected individual to relieve himself of the burden by taking "belated[]" corrective action, *Selective Service System*, 468 U.S at 855; or imposes conditions instead of an absolute "bar," *BellSouth I*, 144 F.3d at 65. In considering less burdensome alternatives, however, courts must resist the temptation to label a statute a bill of attainder simply because "sometimes it works harshly." *Hawker*, 170 U.S. at 197.

Second, a statute flounders on the functional test when its reach is underinclusive. *Foretich*, 351 F.3d at 1224 ("[T]he functional test necessarily takes account of the scope or selectivity of a statute in assessing the plausibility of alleged nonpunitive purposes."). To be sure, selectivity alone does not a bill of attainder make. "[T]he Court has clearly stated that satisfaction of the specificity prong alone is *not* sufficient to find that a particular law implicates the bill of attainder clause, let alone violates it." *BellSouth II*, 162 F.3d at 684. Nevertheless, a concern for specificity reappears in the punishment inquiry, and courts take note when a statute seemingly burdens one among equals. For example, in *Foretich*, we invalidated a statute that prevented a particular father accused of sexually abusing his daughter from having visitation "without the child's consent." 351 F.3d at 1207

(quoting D.C. Code § 11-925). Explaining that "narrow application of a statute to a specific person or class of persons raises suspicion," we concluded in that case that "the narrow focus of the disputed Act [could not] be explained 'without resort to inferences of punitive purpose.'" *Id.* at 1224 (quoting *BellSouth I*, 144 F.3d at 67).

Just how overbroad or underinclusive is too overbroad or underinclusive? On this issue, the cases are less than pellucid. On the one hand, the Bill of Attainder Clause does not require narrow tailoring. Congress enjoys leeway to select among more or less burdensome options, and it "may read the evidence before it in a different way than might this court or any other, so long as it remains clear that Congress was pursuing a legitimate nonpunitive purpose." *BellSouth II*, 162 F.3d at 689. On the other hand, the functional test is "more exacting" than rational basis review. *BellSouth I*, 144 F.3d at 67. The functional inquiry demands not some conceivable nonpunitive purpose, but rather an actual nonpunitive purpose. *See Foretich*, 351 F.3d at 1223 ("[A] statute . . . does not escape unconstitutionality merely because the Government can assert purposes that superficially appear to be nonpunitive.").

So somewhere between the two poles of narrow tailoring and rational basis lies the functional test's tipping point. We have at times described the test as requiring a "coherent and reasonable nexus" or a "rational connection" between the burden imposed and nonpunitive purpose furthered. *Id.* at 1219, 1221. At other times, we have used somewhat more stringent language, demanding that courts "ensure that 'the nonpunitive aims of an apparently prophylactic measure [are] sufficiently clear and convincing.'" *BellSouth II*, 162 F.3d at 686 (alteration in original) (quoting *BellSouth I*, 144 F.3d at 65).

In this case, however, we have no need to choose between the rational-and-coherent or clear-and-convincing formulations, because section 1634 easily clears the latter, higher bar.

We begin with the nonpunitive interest at stake: the security of the federal government's information systems. Given the volume and variety of governmental functions conducted by and through computers, the district court hardly exaggerated when it described the government's networks as "extremely important strategic national assets." *Kaspersky Lab*, 311 F. Supp. 3d at 192–93. And those assets need protection: as Congress recognized in the Federal Information Security Modernization Act of 2014, "the highly networked . . . Federal computing environment" faces significant "information security risks," including the threat of "unauthorized access, use, disclosure, disruption, modification, or destruction of" government information. 44 U.S.C. §§ 3551, 3553. Indeed, although Kaspersky argues that Congress enacted section 1634 to further that body's undisclosed punitive intentions, the company does not dispute, as a general matter, that protecting federal computers from cyber-threats qualifies as a "legitimate nonpunitive purpose." *Patchak v. Jewell*, 828 F.3d 995, 1006 (D.C. Cir. 2016), *cert. granted sub nom. Patchak v. Zinke*, 137 S. Ct. 2091 (2017), *aff'd*, 138 S. Ct. 897 (2018).

While those cyber-threats emanate from all over the world, Russia might well top the list. As the Director of National Intelligence (DNI) testified to the Senate Select Committee on Intelligence in May 2017, "Russia is a full-scope cyber actor that will remain a major threat to [the] US Government . . . . Moscow has a highly advanced offensive cyber program, and in recent years, the Kremlin has assumed a more aggressive cyber posture." *Worldwide Threats*, at 16 (statement of Daniel

R. Coats). One need look no further, the DNI warned, than "Russia's efforts to influence the 2016 US election" to discern the "scope and sensitivity" of the targets Russia seems willing to attack. *Id.* In other words, Russia has demonstrated both the means and the willingness to launch cyber-operations against the U.S. government and its information systems.

Enter Kaspersky, a Russian company founded by a Russian citizen with its headquarters in Russia. In the months before enacting section 1634, Congress heard substantial expert testimony warning that Kaspersky's ties to Russia could jeopardize the integrity of the federal computers on which the company's products operate. With or without Kaspersky's willing cooperation, explained the experts, the Russian government could use Kaspersky products as a backdoor into federal information systems. Then, having gained privileged and undetected access, Russia could make all manner of mischief. The Acting Secretary of Homeland Security apparently agreed with these warnings. So Congress, after hearing all of this information, decided to disallow federal use of Kaspersky hardware, software, and services.

Viewed in context, section 1634 "has the earmarks of a rather conventional response" to a security risk: remove the risk. *BellSouth I*, 144 F.3d at 65. We think it worth emphasizing, moreover, that the government discontinued only its own use of Kaspersky products; all other individuals and companies in the universe of potential clients remain free to buy and use Kaspersky products as they please. To be sure, section 1634 may still impose serious financial and reputational costs on Kaspersky. And Congress, unable to predict the future, had no way of knowing for sure whether Kaspersky products would have caused harm if left in place. But "the severity of a sanction is not determinative of its character as punishment," *Selective Service System*, 468 U.S. at 851, and surely Congress

can do more than identify threats approaching at a distance and wait patiently for those threats to cause empirically provable consequences. Given the not insignificant probability that Kaspersky's products could have compromised federal systems and the magnitude of the harm such an intrusion could have wrought, Congress's decision to remove Kaspersky from federal networks represents a reasonable and balanced response. Section 1634 is prophylactic, not punitive.

Kaspersky, however, accuses Congress of imposing a disproportionate burden. According to the company, Congress could have made section 1634 less burdensome by, for example, including a sunset provision, permitting the government to use Kaspersky products on the condition that the company cease operating in Russia, or prohibiting the use of Kaspersky's hardware and software but not its services. Or, so says Kaspersky, Congress could have done nothing, leaving it to the executive branch to remove the company from the rolls of approved federal contractors pursuant to the process (and procedural safeguards) contained in federal procurement regulations.

But the fact that Kaspersky can imagine slightly less restrictive measures does not demonstrate that the law Congress actually chose amounts to punishment. Take Kaspersky's suggestion that instead of legislating, "Congress could have referred the matter to the executive branch to consider" debarring Kaspersky under the procedures set forth in the Federal Acquisition Regulation. Appellants' Br. 36. Debarment, however, prevents the government only from inking future contracts; it would neither require agencies to remove already-purchased Kaspersky products from their systems nor completely prevent third-party contractors from using Kaspersky products in fulfilling their own federal contracts. *See* 48 C.F.R. § 9.405-1 ("Notwithstanding the

debarment . . . of a contractor, agencies may continue contracts or subcontracts in existence at the time the contractor was debarred . . . ."); 48 C.F.R. § 9.405-2 ("[C]ontractors shall not enter into any subcontract in excess of $35,000, other than a subcontract for a commercially available off-the-shelf item, with a contractor that has been debarred . . . ."). Moreover, although Kaspersky insists that it would have preferred debarment because the Federal Acquisition Regulation contains "procedural safeguards," Appellants' Reply Br. 16 n.8, the company fails to identify how those procedural safeguards would have ultimately forestalled an end to future federal contracts. Indeed, debarment appears to be the worst of all worlds for all parties involved. Kaspersky would have still lost the opportunity to sell to the U.S. government—as it has under section 1634—but federal computer systems would have remained at risk from unremoved Kaspersky software.

Similar deficiencies plague Kaspersky's other proposals: either the suggested alternative does not adequately protect federal information systems, or it does not substantially lessen the burden on Kaspersky. With respect to the proposals that fail to protect federal computers as well as section 1634 does—for example, including a sunset provision—those we reject for failure to offer genuinely workable alternatives. And with respect to the remaining proposals that lessen the burden on Kaspersky only slightly, or that swap one burden for another—for example, requiring Kaspersky to discontinue all Russian operations—we cannot infer from the marginal difference between those hypothetical statutes and the statute actually passed that Congress chose section 1634 with punishment in mind. "In other words, it does not matter that Congress arguably could have enacted different legislation in an effort" to secure federal networks, because "it cannot be legitimately 'suggested that the risks . . . were so feeble that no one could reasonably assert them except as a smoke screen for some

invidious purpose.'" *BellSouth II*, 162 F.3d at 689 (quoting *BellSouth I*, 144 F.3d at 66).

Kaspersky also argues that it was unfairly "single[d] out" for mistreatment, Appellants' Br. 15, and that Congress should have instead "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 [Russian intelligence agencies], does business in Russia, has servers in Russia, or uses Russian networks," Appellants' Reply Br. 16. But Kaspersky identifies no cyber-product as vulnerable to malicious exploitation as Kaspersky's. And although the company accurately points out that many cyber-companies operate in Russia, we conclude that Congress, based on the evidence before it, could have reasonably determined that Kaspersky's Russian ties differ in degree and kind from these other companies'. It was Kaspersky—not these other companies—about whom the experts sounded the alarm. Kaspersky, in other words, is in a class of its own.

Indeed, in this respect, this case closely resembles *Nixon v. Administrator of General Services*, which concerned a statute that had directed the Administrator of General Services "to take custody," at least temporarily, of former-President Nixon's presidential papers and tape recordings. 433 U.S. at 429. The Court rejected Nixon's claim that the statute's specificity evinced punitive intent, concluding instead that Congress had permissibly created "a legitimate class of one" because "at the time of the Act's passage, only [Nixon's] materials demanded immediate attention." *Nixon*, 433 U.S. at 472; *see also BellSouth I*, 144 F.3d at 67 (concluding, given the unique characteristics of BellSouth Corporation's operating companies, that their "differential treatment" under the statute at issue was "quite understandable without resort to inferences

of punitive purpose"). The Court in *Nixon* also found it notable that in addition to offering a short-term Band-Aid solution to the problem presented by Nixon's records, the statute also established a commission to study the preservation of future administrations' presidential materials. *Id.* As the Court saw it, the statute permissibly dealt with a pressing issue at hand while simultaneously acting to prevent the same problem from arising again.

So too, here. No one argues that Kaspersky presents the only possible gap in the federal computer system's defenses. But Congress had ample evidence that Kaspersky posed the most urgent potential threat, and this court must give Congress "sufficient latitude to choose among competing policy alternatives," lest "our bill of attainder analysis . . . 'cripple the very process of legislating.'" *Foretich*, 351 F.3d at 1222–23 (quoting *Nixon*, 433 U.S. at 470); *cf. Clements v. Fashing*, 457 U.S. 957, 969 (1982) (holding, in the context of an equal-protection challenge, that "[a] [s]tate [may] regulate 'one step at a time, addressing itself to the phase of the problem which seems most acute'" (quoting *Williamson v. Lee Optical of Oklahoma Inc.*, 348 U.S. 483, 489 (1955))). The Bill of Attainder Clause does not make perfect the enemy of the good. Furthermore, like the statute at issue in *Nixon*, section 1634 contains not only specific provisions addressing a particular threat (subsections (a) and (b)), but also a broader provision directing further investigation of that threat. Specifically, subsection (c) directs the Secretary of Defense to conduct a review of "the procedures for removing suspect products or services from the information technology networks of the Federal Government." NDAA § 1634(c). Nothing in section 1634 prevents Congress from expanding its prohibition to include other companies or products later determined to pose a cybersecurity risk. Given this context, we are convinced that

section 1634 represents Congress's effort at triage, not punishment.

At the end of the day, the functional test does not require that Congress precisely calibrate the burdens it imposes to the goals it seeks to further or to the threats it seeks to mitigate. Instead, the test requires only that Congress refrain from "'pil[ing] on' . . . additional, entirely unnecessary burden[s]." *Foretich*, 351 F.3d at 1228 (Tatel, J., concurring in part and concurring in the judgment) (quoting *Consolidated Edison Co.*, 292 F.3d at 354). And given the reasonable balance between the burden imposed by section 1634 and the nonpunitive national security objective it furthers, we easily conclude that Congress has not done so here.

Historical Test

Having failed to make a persuasive showing on the functional test, Kaspersky faces an uphill battle. *Foretich*, 351 F.3d at 1218 ("[C]ompelling proof on [the functional test] may be determinative."). Although we cannot rule out the possibility that a persuasive showing on the historical or motivational tests could overcome a challenger's failure to raise a suspicion of punitiveness under the functional test, this, as we are about to explain, is not such a case—indeed, not even close.

Under the historical test, we ask "whether the challenged statute falls within the historical meaning of legislative punishment." *Selective Service System*, 468 U.S. at 852. This question overlaps significantly with the functional test because, historically, "legislative punishment" existed where the burden imposed so dramatically outweighed the benefit gained that courts could infer only a punitive purpose. "[T]he substantial experience of both England and the United States with [bills of attainder]," the Supreme Court explained in *Nixon*, "offers a

ready checklist of deprivations and disabilities 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; *see also Foretich*, 351 F.3d at 1219 (explaining that early Supreme Court bill-of-attainder cases "foreshadowed the development of the functional test").

Despite the apparent redundancy of the historical inquiry, we must double-check our functional-test work by comparing section 1634 to the "ready checklist" of historical punishments. "This checklist includes sentences of death, bills of pains and penalties, and legislative bars to participation in specified employments or professions." *Foretich*, 351 F.3d at 1218.

As Kaspersky admits, "'the particular burden imposed'" by section 1634 "'is not precisely identical to any of the burdens historically recognized as punishment.'" Appellants' Br. 24 (quoting *Foretich*, 351 F.3d at 1219). Kaspersky has not been sentenced to death, nor banished, nor had its property confiscated. *See BellSouth I*, 144 F.3d at 64 (listing historic "bills of pains and penalties"). Kaspersky nonetheless argues that section 1634, though not strictly analogous, is so "consistent with historical forms of punishment" that the historical test weighs in its favor. Appellants' Br. 24.

In support of this claim, Kaspersky highlights two characteristics shared by many historic bills of attainder: excluding or expelling individuals from a profession, and "mark[ing] specified persons with a brand of infamy or disloyalty." *Foretich*, 351 F.3d at 1219. In particular, Kaspersky cites four Supreme Court cases—two from the Civil War and two from the Cold War—in which, as previously noted, the Court invalidated statutes that excluded, respectively, former confederate sympathizers and communists

from particular vocations, including, in one case, from government service. *See Cummings*, 71 U.S. 277 (prohibiting ex-rebel sympathizers from serving as priests); *Ex Parte Garland*, 71 U.S. 333 (denying ex-confederate sympathizers admission to the bar); *Lovett*, 328 U.S. 303 (cutting off salary to certain "subversive" government employees); *Brown*, 381 U.S. 437 (criminalizing communists' service as officers in labor unions). Kaspersky also relies on our decision in *Foretich*, in which we concluded that "deprivation of parental rights and the opprobrium of being branded a criminal child abuser . . . may be of even greater magnitude than many of [the burdens] at issue in the historical cases." *Foretich*, 351 F.3d at 1220. Based on these decisions, Kaspersky argues that section 1634 imposes punishment because it "stamp[s] [Kaspersky] with Congress's legislative conclusion that the company is disloyal to the United States, or at least undeserving of the federal government's trust." Appellants' Br. 17.

The historical punishments Kaspersky cites are readily distinguishable from the burden section 1634 imposes on the company. To begin with, although we assume that the Bill of Attainder Clause protects corporations as well as natural persons, *see supra* at 9, we have no basis for likewise assuming that corporate entities feel burdens in the same way as living, breathing human beings. "[I]t is obvious," we have explained, "that there are differences between a corporation and an individual under the law," so "any analogy between prior cases that have involved individuals and this case, which involves a corporation, must necessarily take into account this difference." *BellSouth II*, 162 F.3d at 684. And as the Second Circuit has explained, "[t]here may well be actions that would be considered punitive if taken against an individual, but not if taken against a corporation." *Consolidated Edison Co.*, 292 F.3d at 349.

In particular, the stain of a "brand of infamy or disloyalty" matters most to flesh-and-blood humans. These are people who, most likely, have but one country of citizenship—a country in which they exercise civic privileges available exclusively to living individuals, such as voting, running for office, or serving in the armed forces. They are people who have neighbors and colleagues and communities in whose good graces they hope to remain. And they are people who have families and friends whose own reputations and happiness are tied, at least in part, to their own.

Corporations are very different. To be sure, corporations may derive substantial financial value from their brands' reputations. But that is precisely the point: reputation is an asset that companies cultivate, manage, and monetize. It is not a quality integral to a company's emotional well-being, and its diminution exacts no psychological cost. This is why, for example, "[t]he law of libel has long reflected the distinction between corporate and human plaintiffs by limiting corporate recovery to actual damages in the form of lost profits." *Martin Marietta Corp. v. Evening Star Newspaper Co.*, 417 F. Supp. 947, 955 (D.D.C. 1976); *see also Art Metal-U.S.A., Inc. v. United States*, 753 F.2d 1151, 1156 (D.C. Cir. 1985) (holding that a corporation suing for defamation "may only recover actual damages in the form of lost profits"). Unlike defamation actions brought by individuals, because a corporation "has no personal reputation," *Golden Palace, Inc. v. National Broadcasting Co.*, 386 F. Supp. 107, 109 (D.D.C. 1974), *aff'd*, 530 F.2d 1094 (D.C. Cir. 1976), "libel action[s] brought on behalf of corporation[s]" fall far short of implicating "'the essential dignity and worth of every human being,'" *Martin Marietta Corp.*, 417 F. Supp. at 955 (quoting *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 341 (1974)).

Because human beings and corporate entities are so dissimilar, any analogy between the statutes that courts have found to qualify as bills of attainder and section 1634 is strained at best. Section 1634 is unlike the statute at issue in *Cummings v. Missouri*, which following the Civil War closed "office[s] of honor, trust, or profit" to individuals who had "expressed sympathy with any who were drawn into the Rebellion," thereby permanently associating even passive sympathizers with "the most active and the most cruel of the rebels." 71 U.S. at 317–18; *see also Flemming*, 363 U.S. at 615 (explaining that "the finding of punitive intent" in *Cummings* "drew heavily on the Court's first-hand acquaintance with the events and the mood of the then recent Civil War"). Unlike the individuals expunged from federal payrolls in *United States v. Lovett*, Kaspersky has not been shunted into an underclass of citizens declared "unfit . . . to continue in Government employment" and "purg[ed] [from] the public service" for holding membership in communist organizations and espousing "views and philosophies" consonant with "subversive activity." 328 U.S. at 311–12; *see also Flemming*, 363 U.S. at 615 (explaining that "the determination that a punishment had been imposed" in *Lovett* "rested in large measure on the specific Congressional history" of the statute). Nor, finally, is Kaspersky at all like Dr. Foretich, who Congress had by legislative act "permanently associated . . . with criminal acts of child sexual abuse." *Foretich*, 351 F.3d at 1223.

Furthermore, all of the Supreme Court's employment ban cases have involved "a legislative enactment barring designated individuals or groups from participation in specified employments or vocations." *Nixon*, 433 U.S. at 474. Not so with section 1634. As the complaint itself alleges, Kaspersky is "one of the world's largest privately owned cybersecurity companies," and it does business all around the globe. Compl.

¶ 18. Because the federal government is far from Kaspersky's only client, section 1634 does not prevent Kaspersky from engaging in its chosen profession, namely, developing and selling cybersecurity products and services.

To the contrary, rather than an employment ban, section 1634 much more closely resembles the kinds of permissible "line-of-business restrictions" and "run-of-the-mill business regulations" that we approved in *BellSouth I*, 144 F.3d at 116, and *BellSouth II*, 162 F.3d at 686. In those cases, this court upheld two provisions of the Telecommunications Act of 1996, one that prohibited all Bell operating companies and their affiliates from engaging in certain types of electronic publishing for four years, *see BellSouth I*, 144 F.3d at 61, and another that prevented the operating companies from providing certain kinds of long-distance services without first meeting statutorily defined criteria, *see BellSouth II*, 162 F.3d at 680–81. Admittedly, the provisions at issue in the *BellSouth* cases presented easier calls: the two Telecommunications Act sections under review included statutory escape hatches—such as a sunset provision and a corporate restructuring workaround—that section 1634 lacks. Nonetheless, the *BellSouth* cases make clear that the Bill of Attainder Clause tolerates statutes that, in pursuit of legitimate goals such as public safety or economic regulation, prevent companies from engaging in particular kinds of business or particular combinations of business endeavors. *See BellSouth I*, 144 F.3d at 64–65 (contrasting punitive employment bars with nonpunitive conflict-of-interest and cross-ownership restrictions); *see also Navegar, Inc. v. United States*, 192 F.3d 1050, 1066 (D.C. Cir. 1999) (holding that a statute banning the manufacture of semiautomatic assault weapons did not constitute a bill of attainder against gun manufacturers). And section 1634 is just such a statute: for the protection of federal

computer systems, it prevents Kaspersky from selling products for use in federal computers.

At bottom, then, a wide valley separates section 1634 from the small handful of statutes that courts have found to be unconstitutional bills of attainder. All four of the relevant Supreme Court cases involved flesh-and-blood humans whom the legislature deemed untrustworthy or subversive based on those individuals' political beliefs. And this court's case, *Foretich*, concerned a legislative determination that a father had sexually abused his own daughter. Those cases differ markedly from the situation we face here, where Congress simply decided to stop using a company's products based on its determination that those products posed a national security risk. Section 1634 may well cost Kaspersky some revenue, but it stretches credulity to view what is ultimately a procurement decision as a "brand of infamy or disloyalty." *Foretich*, 351 F.3d at 1219. Of course, we do not foreclose the possibility that Congress could impose a brand of infamy or disloyalty upon a corporation that would rise to the level of legislative punishment. But, in this case, section 1634 represents no more than a customer's decision to take its business elsewhere. Though costly to Kaspersky, such a decision falls far short of "the historical meaning of legislative punishment." *Selective Service System*, 468 U.S. at 852.

Motivational Test

The motivational test asks "whether the legislative record 'evinces a congressional intent to punish.'" *Selective Service System*, 468 U.S. at 852 (quoting *Nixon*, 433 U.S. at 478). As we explained in *Foretich*, "[g]iven the obvious constraints on the usefulness of legislative history as an indicator of Congress's collective purpose," statutes rarely struggle to satisfy the motivational test. 351 F.3d at 1225. Indeed, "this

prong by itself is not determinative in the absence of 'unmistakable evidence of punitive intent.'" *Id.* (quoting *Selective Service System*, 468 U.S. at 855 n.15).

Kaspersky not only fails to offer such unmistakable evidence; it very nearly fails to offer any evidence whatsoever. Kaspersky relies solely on a handful of public comments made by Senator Shaheen, the sponsor of the amendment that became section 1634. In a September 2017 *New York Times* op-ed, the senator warned that the "threat . . . posed by antivirus and security software products created by Kaspersky Lab, a Moscow-based company with extensive ties to Russian intelligence" creates an "alarming national security vulnerability." Jeanne Shaheen, *The Russian Company that Is a Danger to Our Security*, N.Y. Times, Sept. 4, 2017. Similarly, in a press release several weeks later, Shaheen stated that the "case against Kaspersky Lab is overwhelming," warning that "[t]he strong ties between Kaspersky Lab and the Kremlin are alarming and well-documented." *Shaheen's Legislation to Ban Kaspersky Software Government-Wide Passes Senate as Part of Annual Defense Bill*, Jeanne Shaheen (Sept. 18, 2017), https://www.shaheen.senate.gov/news/press/shaheens-legislation-to-ban-kaspersky-software-government-wide-passes-senate-as-part-of-annual-defense-bill-.

The trouble with Kaspersky's reliance on Shaheen's comments is twofold. First, we detect no punitive intent in the senator's statements. To the contrary, she expressed a desire to take action to protect federal information systems—a nonpunitive objective. And second, even if Shaheen's statements did reveal a personal desire to punish Kaspersky, the company cites no corroborating evidence indicating that other members of Congress shared her supposedly punitive motivations. "'[S]everal isolated statements are not sufficient to evince punitive intent,' and cannot render a statute a bill of

attainder without any other indicia of punishment." *Foretich*, 351 F.3d at 1225 (quoting *BellSouth II*, 162 F.3d at 690) (internal quotation marks omitted). Therefore, like the functional and historical tests, the motivational test does nothing to support Kaspersky's argument that section 1634 constitutes a bill of attainder.

III.

Before concluding our consideration of the NDAA Case, we need to address a procedural concern raised by Kaspersky. As a general rule, "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 Partnership*, 863 F.3d 923, 936 (D.C. Cir. 2017). Kaspersky argues that as a consequence of consolidating the Directive and the NDAA Cases for purposes of resolving related motions, the district court impermissibly relied upon facts contained in the Directive Case's administrative record when considering the government's motion to dismiss the NDAA Case.

Although we cannot rule out the possibility that the district court improperly comingled facts from the two separate cases, we need not reach that issue. Because we are reviewing the district court's dismissal de novo, even if that court impermissibly ventured outside the pleadings, we can affirm based on the available permissible evidence. Among the information a court may consider on a motion to dismiss are "public records subject to judicial notice." *Kaempe v. Myers*, 367 F.3d 958, 965 (D.C. Cir. 2004). "A federal court may take judicial notice of 'a fact that is not subject to reasonable dispute' if it . . . 'can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned.'" *Hurd v. District of Columbia*, 864 F.3d 671, 686 (D.C. Cir.

2017) (quoting Fed. R. Evid. 201(b)). In this case, Kaspersky takes issue with the claims about the company memorialized in various congressional hearings and legislative materials, but the fact that those records exist is beyond dispute. Therefore, in the foregoing discussion, we have noticed section 1634's legislative record not for its truth, but for its existence. *See Hurd*, 864 F.3d at 686 (explaining that this court can rely on a public record "of what was said" without relying "on it for the truth of the matter asserted").

We therefore consult section 1634's legislative record to provide evidence of statutory purpose only—that is, what information Congress had before it when enacting the statute. And in this case, that is enough to resolve Kaspersky's claim. Relying just on the legislative record and, of course, the NDAA Case's complaint itself, we conclude for all the reasons already discussed that Kaspersky's complaint fails to plausibly allege that section 1634 is a bill of attainder. We shall therefore affirm the district court's dismissal of Kaspersky's NDAA Case for failure to state a claim upon which relief can be granted.

IV.

Having concluded that section 1634 is not a bill of attainder, and thus having affirmed dismissal of the NDAA Case, we turn to Kaspersky's other suit against the Department of Homeland Security. In its complaint, the company alleges that Binding Operational Directive 17-01 violates the Administrative Procedure Act, and it seeks the Directive's invalidation. *See* Complaint, *Kaspersky Lab, Inc. v. U.S. Department of Homeland Security*, No. 1:17-cv-02697, at 22 (D.D.C. Dec. 18, 2017).

As the district court recognized, however, Kaspersky has a serious standing problem. Section 1634 prohibits all the same conduct as the Directive—and then some. Indeed, section 1634

sweeps more broadly than the Directive in two respects: it covers more Kaspersky products and applies to more agencies. *See Kaspersky Lab*, 311 F. Supp. 3d at 219 ("[T]he prohibition in the NDAA is broader than the prohibition in [Binding Operational Directive] 17–01, because it includes all Kaspersky Lab products and services (not just 'Kaspersky-branded' products), and because it does not exempt any national security systems."). Consequently, as Kaspersky apparently concedes, invalidation of the Directive alone would do nothing to help Kaspersky's plight as long as section 1634 remains good law.

And indeed it does. Thus, as the district court explained, "even if . . . the Court were to order the rescission of the [Directive], [Kaspersky's] harms would not be redressed." *Kaspersky Lab*, 311 F. Supp. 3d at 219. It is well-settled that courts lack jurisdiction to hear cases in which the plaintiff fails to identify a redressable injury. *See Simon v. Eastern Kentucky Welfare Rights Organization*, 426 U.S. 26, 38 (1976) (holding that to demonstrate standing, a plaintiff must show "an injury to himself that is likely to be redressed by a favorable decision"). Therefore, because courts "ha[ve] no jurisdiction to proceed to the merits of a lawsuit where [their] ultimate decision will have no real effect," *Kaspersky Lab*, 311 F. Supp. 3d at 219, we shall affirm the district court's dismissal of the Directive Case for lack of subject matter jurisdiction.

V.

For the foregoing reasons, we affirm the district court's dismissal of the NDAA Case for failure to state a claim upon which relief can be granted, as well as its dismissal of the Directive Case for lack of jurisdiction.

So ordered.