FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ENIGMA SOFTWARE GROUP USA, LLC, *Plaintiff-Appellant,* v. MALWAREBYTES, INC., *Defendant-Appellee.*	No. 21-16466 D.C. No. 5:17-cv-02915-EJD OPINION

Appeal from the United States District Court
for the Northern District of California
Edward J. Davila, District Judge, Presiding

Argued and Submitted November 8, 2022
Portland, Oregon

Filed June 2, 2023

Before: Richard R. Clifton and Patrick J. Bumatay, Circuit Judges, and M. Miller Baker,[*] International Trade Judge.

Opinion by Judge Clifton;
Concurrence by Judge Baker;
Dissent by Judge Bumatay

[*] The Honorable M. Miller Baker, Judge for the United States Court of International Trade, sitting by designation.

SUMMARY[**]

Lanham Act

The panel affirmed in part and reversed in part the district court's judgment dismissing a lawsuit brought by Enigma Software Group USA LLC, a computer security software provider, against its competitor Malwarebytes, Inc. for designating its products as "malicious," "threats," and "potentially unwanted programs"; and remanded for further proceedings.

Enigma's operative complaint alleged a false advertising claim under Section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a)(1)(B), and tort claims under New York law. Dismissing the motion under Fed. R. Civ. P. 12(b)(6), the district court concluded that all of Enigma's claims were insufficient as a matter of law.

The district court primarily based the dismissal on its conclusion that Malwarebytes's designations of Enigma's products were "non-actionable statements of opinion." The panel disagreed with that assessment. In the context of this case, the panel concluded that when a company in the computer security business describes a competitor's software as "malicious" and a "threat" to a customer's computer, that is more a statement of objective fact than a non-actionable opinion. It is potentially actionable under the Lanham Act provided Enigma plausibly alleges the other elements of a false advertising claim.

[**] This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

The district court held that the tort claims under New York law failed because Malwarebytes was not properly subject to personal jurisdiction in New York. That meant Enigma's claim for relief under New York General Business Law (NYGBL) § 349 failed because that statute did not apply to the alleged misconduct. The panel disagreed and concluded that Malwarebytes is subject to personal jurisdiction in New York. As this action was initially filed in New York, the law of that state properly applies.

The common law claims for tortious interference with contractual relations and tortious interference with business relations were also dismissed by the district court. Those torts are recognized as actionable under California law, as they are under New York law, but the district court concluded that Enigma failed to allege essential elements for those claims under California law. The contractual relations claim failed because Enigma did not identify a specific contractual obligation with which Malwarebytes interfered. The business relations claim was dismissed because that claim required an allegation of independently wrongful conduct, and that requirement was not satisfied following the dismissal of the Lanham Act and NYGBL § 349 claims. Because the panel held that the Lanham Act and NYGBL § 349 claims should not have been dismissed, the panel concluded that the tortious interference with business relations claim should similarly not have been dismissed. The panel agreed with the district court regarding dismissal of the claim for tortious interference with contractual relations, however, and affirmed the dismissal of that claim.

Concurring, Court of International Trade Judge Baker wrote separately to touch on choice of law. He wrote that ordinarily the application of a transferor jurisdiction's law

carries with it the choice-of-law rules of that jurisdiction, but here the parties did not address the choice of law beyond the dispute over whether personal jurisdiction existed in the Southern District of New York. The opinion assumes—as the parties did in their briefing by not addressing choice of law—that under New York choice-of-law rules, New York substantive law applies to Enigma's state-law claims, save for the claims based on Malwarebytes' transactions with customers outside of New York.

Judge Bumatay dissented. He wrote that the Lanham Act protects against false or misleading representations of fact, but flagging a competitor's products as "potentially unwanted," a "threat," or "malicious" is no expression of fact—these are subjective statements, not readily verifiable, which means they are opinions. He wrote that by treating these terms as actionable statements of fact under the Lanham Act, the court sends a chilling message to cybersecurity companies—civil liability may now attach if a court later disagrees with your classification of a program as "malware." He wrote that Enigma's failure to allege a misstatement of fact is also dispositive on its state-law claims.

COUNSEL

Terry Budd (argued), Budd Law PLLC, Wexford, Pennsylvania; Christopher M. Verdini and Anna Shabalov, K&L Gates LLP, Pittsburgh, Pennsylvania; Edward P. Sangster, K&L Gates LLP, San Francisco, California; for Plaintiff-Appellant.

Moez M. Kaba (argued), Michael H. Todisco, and Warren S. Crandall, Hueston Hennigan LLP, Los Angeles, California; John C. Hueston, Hueston Hennigan LLP, Newport Beach, California; for Defendant-Appellee.

OPINION

CLIFTON, Circuit Judge:

Plaintiff-Appellant Enigma Software Group USA LLC ("Enigma"), a computer security software provider, sued a competitor, Defendant-Appellee Malwarebytes, Inc. ("Malwarebytes"), for designating its products as "malicious," "threats," and "potentially unwanted programs" ("PUPs"). Enigma's operative complaint alleged a false advertising claim under Section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a)(1)(B), and tort claims under New York law.

Malwarebytes moved to dismiss under Federal Rule of Civil Procedure 12(b)(6). The district court granted the motion, concluding that all of Enigma's claims were insufficient as a matter of law. It primarily based the dismissal on its conclusion that Malwarebytes's designations of Enigma's products were "non-actionable statements of opinion." As we explain in more detail below, we disagree with that assessment. In the context of this case, we conclude that when a company in the computer security business describes a competitor's software as "malicious" and a "threat" to a customer's computer, that is more a statement of objective fact than a non-actionable opinion. It is potentially actionable under the Lanham Act provided

Enigma plausibly alleges the other elements of a false advertising claim.

The district court also held that the tort claims under New York law failed because Malwarebytes was not properly subject to personal jurisdiction in New York. That meant Enigma's claim for relief under New York General Business Law ("NYGBL") § 349 failed because that statute did not apply to the alleged misconduct. We disagree and conclude that Malwarebytes is subject to personal jurisdiction in New York. As this action was initially filed in New York, the law of that state properly applies.

The common law claims for tortious interference with contractual relations and tortious interference with business relations were also dismissed by the district court. Those torts are recognized as actionable under California law, as they are under New York law, but the district court concluded that Enigma failed to allege essential elements for those claims under California law.

The contractual relations claim failed because Enigma did not identify a specific contractual obligation with which Malwarebytes interfered. The business relations claim was dismissed because that claim required an allegation of independently wrongful conduct, and that requirement was not satisfied following the dismissal of the Lanham Act and NYGBL § 349 claims. Because we hold that the Lanham Act and NYGBL § 349 claims should not have been dismissed, we conclude that the tortious interference with business relations claim should similarly not have been dismissed. We agree with the district court regarding dismissal of the claim for tortious interference with contractual relations, however, and affirm the dismissal of that claim.

In sum, we affirm in part, reverse in part, and remand for further proceedings.

I. Background and Procedural History

Enigma is a Florida company that markets and sells computer security software nationwide. Its products, according to its Second Amended Complaint ("SAC"), "(i) detect and remove malicious software (i.e., malware)" such as "viruses, spyware, adware, ransomware, and Trojans; (ii) enhance users' Internet privacy; (iii) offer users the choice to block 'Potentially Unwanted Programs' ('PUPs'); and/or (iv) eliminate security threats and risks from problematic software programs." SAC ¶ 2.

Malwarebytes is a Delaware corporation, headquartered in California. It is a direct competitor of Enigma in the anti-malware and computer security market. Founded in 2008, its flagship anti-malware products are aimed, according to the complaint, at "detect[ing] and remov[ing] malware, PUPs, and other potentially threatening programs on users' computers." SAC ¶ 7.

Enigma commenced this lawsuit against Malwarebytes in the U.S. District Court for the Southern District of New York asserting Lanham Act false advertising and supplemental tort claims under New York law. *See Enigma Software Grp. USA, LLC v. Malwarebytes Inc*., 260 F. Supp. 3d 401 (S.D.N.Y. 2017). Malwarebytes moved to dismiss for lack of personal jurisdiction and failure to state a claim or, in the alternative, to transfer the case to the Northern District of California under 28 U.S.C. § 1404. *Id.* at 404. The district court granted the motion to transfer and declined to reach the motion to dismiss. *Id.*

In the California federal court, Malwarebytes renewed its motion to dismiss, arguing that Enigma failed to state a claim and, in the alternative, that Malwarebytes was immune from suit as all of Enigma's claims were barred by Section 230 of the Communications Decency Act of 1996, 47 U.S.C. § 230(c)(2). *See Enigma Software Grp. USA LLC v. Malwarebytes Inc.*, No. 5:17-CV-02915-EJD, 2017 WL 5153698, at *1 (N.D. Cal. Nov. 7, 2017). The district court granted the motion, holding that Malwarebytes was immune from suit under Section 230. It did not examine whether Enigma failed to state a claim. *Id.* at *4.

Enigma appealed the district court's ruling. This court reversed and remanded, holding that Section 230 did not apply to "blocking and filtering decisions that [we]re driven by anticompetitive animus." *Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1050 (9th Cir. 2019).

On remand, Enigma filed its SAC asserting four causes of action: (1) false advertising in violation of the Lanham Act, 15 U.S.C. § 1125(a)(1)(B); (2) a violation of NYGBL § 349, prohibiting deceptive and unlawful business practices; (3) tortious interference with contractual relations; and (4) tortious interference with business relations.

Enigma alleged that from 2008 to October 2016, Malwarebytes's products did not identify any of Enigma's products as "malicious," "threats," "PUPs," or any other type of malware, nor did it quarantine or block consumers from using any of them. SAC ¶ 11. But starting in October 2016, the complaint alleged, Malwarebytes started to do so. Enigma alleged it was in retaliation for Enigma suing an affiliate of Malwarebytes called Bleeping Computer, which held itself out to the public as an independent website

reviewing software products. SAC ¶ 11. According to Enigma, Bleeping Computer was not independent and conveyed "false, misleading, and deceptive information" on its website about Enigma and its products, as well as "instruct[ing] users not to install, or to uninstall," Enigma products and "instead purchase Malwarebytes' competing products." SAC ¶ 23. Enigma alleged that Bleeping Computer disseminated this false information in exchange for sales commissions from Malwarebytes. SAC ¶ 11.

Enigma further alleged that Malwarebytes retaliated against it because the former subpoenaed the latter in the Bleeping Computer lawsuit seeking evidence of a "profiteering scheme" between Malwarebytes and Bleeping Computer "employing anticompetitive, unfair trade practices" to Enigma's detriment.

Malwarebytes moved to dismiss for failure to state a claim, and the district court again dismissed the case, as described above. Regarding the Lanham Act claim, the district court reasoned that Enigma alleged that Malwarebytes's designations of the former's products were "just [nonactionable] subjective opinions" rather than "verifiably false." As to Enigma's state law claims, the district court concluded that California law applied because New York lacked personal jurisdiction over Malwarebytes. For that reason alone, the district court held, the NYGBL § 349 claim failed. But even if New York law applied, the claim failed for the same reasons that the Lanham Act claim failed. The district court concluded that Enigma's tortious interference claims failed under California law. The district court reasoned that the contractual interference claim failed to identify "a specific contractual obligation with which Malwarebytes interfered" and failed to "plead that Malwarebytes engaged in any independently wrongful act

which interfered with a specific contractual obligation under its at-will agreements with users." The interference with business relations claim failed because Enigma did not "allege any other independently wrongful conduct,"—meaning conduct "proscribed by some [statutory or common law] standard,"—beyond the failed Lanham Act and NYGBL § 349 claims.

In dismissing the case, the district court also denied leave to amend, reasoning that "there are no further facts Enigma can allege to cure the complaint." Enigma timely appealed.

II. Discussion

We review de novo a district court's dismissal for failure to state a claim, crediting all factual allegations as true and construing the pleadings in the light most favorable to the non-moving party. *Tingley v. Ferguson*, 47 F.4th 1055, 1066 (9th Cir. 2022).

A. Lanham Act

Enigma argues that the district court erred in dismissing its Lanham Act claim. Enigma alleged that Malwarebytes designated its products and domains as "malicious," "threats," and "PUPs" and that such statements were "factually false" and misrepresented the very purpose of its software. The district court held that these statements were non-actionable statements of opinion. As to the statements that Enigma's products are "malicious" and "threats," we disagree.[1]

[1] Enigma also argues that our previous opinion in *Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040 (9th Cir. 2019), compels reversing the district court's dismissal of the Lanham Act claim. There,

To state a claim for false advertising under Section 43(a) of the Lanham Act, Enigma had to allege that (1) Malwarebytes made a false statement of fact in a commercial advertisement; (2) the statement deceived or had the tendency to deceive a substantial segment of its audience; (3) the deception was material, in that it was likely to influence the purchasing decision; (4) the false statement entered interstate commerce; and (5) Enigma has been or is likely to be injured as a result of the false statement. *Southland Sod Farms v. Stover Seed Co.*, 108 F.3d 1134, 1139 (9th Cir. 1997). Because the district court concluded that Malwarebytes's challenged designations were non-actionable statements of opinion rather than fact, the court did not consider whether the company plausibly alleged the other applicable requirements.[2]

To show falsity under the Lanham Act, a plaintiff must allege that "the statement was literally false, either on its face or by necessary implication, or that the statement was literally true but likely to mislead or confuse consumers." *Id.*; *see also Ariix, LLC v. NutriSearch Corp.*, 985 F.3d 1107, 1121 (9th Cir. 2021) (quoting *Coastal Abstract Serv., Inc. v. First Am. Title Ins. Co.*, 173 F.3d 725, 731 (9th Cir. 1999))

---

we held that Enigma's Lanham Act claim did not fall under Section 230 of the Communications Decency Act's intellectual property exception. *Id.* at 1052–53. We did not decide, however, whether Enigma stated a claim under the Lanham Act.

[2] In addition to the defending the district court's determination that the challenged designations were nonactionable opinions rather than statements of fact, Malwarebytes defends dismissal of the Lanham Act claim on the alternative grounds that those designations were not commercial speech, and that they did not deceive a substantial segment of the relevant audience. We remand those issues to the district court to consider in the first instance.

("An actionable statement is a specific and measurable claim, capable of being proved false or of being reasonably interpreted as a statement of objective fact.").

Taken as true at the stage of a motion to dismiss, Enigma's allegations are sufficient to state a Lanham Act claim. Malwarebytes's designations employ terminology that is substantively meaningful and verifiable in the cybersecurity context. Unlike non-actionable statements of puffery, which are "extremely unlikely to induce consumer reliance," Malwarebytes's designations of Enigma's products "make[] a claim as to the specific or absolute characteristics of a product" and are accordingly actionable statements of fact under the Lanham Act. *Newcal Indus., Inc. v. Ikon Off. Sol.*, 513 F.3d 1038, 1053 (9th Cir. 2008) (internal quotation marks and citation omitted). As Enigma points out, its products either contain malicious files and threaten the security of users' computers, or they do not. These statements are not the type of general, subjective claims typically deemed non-actionable opinions.

We must look to "the totality of the circumstances" when assessing whether a statement implies a factual assertion. *Underwager v. Channel 9 Australia*, 69 F.3d 361, 366 (9th Cir. 1995). Although "malicious" and "threatening" are "adjectives [that] admit of numerous interpretations," *Partington v. Bugliosi*, 56 F.3d 1147, 1158 (9th Cir. 1995), "[t]he context . . . is paramount" because "the reasonable interpretation of a word can change depending on the context in which it appears." *Knievel v. ESPN*, 393 F.3d 1068, 1075 (9th Cir. 2005). Malwarebytes's anti-malware program specifically labeled Enigma's software as "malicious" and a "threat," which a reasonable person would plausibly

interpret as the identification of malware.[3] SAC ¶¶ 143–64. Because whether software qualifies as malware is largely a question of objective fact, at least when that designation is given by a cybersecurity company in the business of identifying malware for its customers, Enigma plausibly alleged that Malwarebytes's statements are factual assertions.

Our dissenting colleague disagrees. The dissent contends, at 36, that "[c]ontrary to Enigma's claims, a program isn't simply 'potentially unwanted' or not. A software program isn't verifiably a 'threat' or not. And a website isn't measurably 'malicious' or not. In the cybersecurity context, these terms refer to a spectrum of digital features with no verifiable line to cross to determine when they apply."

We agree that "potentially unwanted" is too unspecific to provide a basis for a Lanham Act claim, as we noted above at 13, n.3. But the premise of the dissent regarding the terms "threat" and "malicious" rests on an understanding of the meaning of those words in this context that we do not share.

Malware, in its ordinary meaning, refers to software "written with the intent of being disruptive or damaging to (the user of) a computer or other electronic device; viruses, worms, spyware, etc., collectively." *Oxford English Dictionary Online* (2022); *see also Malware*, *Black's Law Dictionary* (11th ed. 2019) (defining malware as "software, used to monitor or gain access to another's computer system

[3] Unlike the terms "malicious" and "threat," which a cybersecurity application would use to describe malware, "potentially unwanted program" is too vague to be considered a factual assertion.

without authorization for the purpose of impairing or disabling the system.").

We think such a definition lends itself to verification. Enigma's complaint indicates that malware can come in many forms, including "viruses, spyware, adware, ransomware, and Trojans." SAC ¶ 2. But at bottom, as demonstrated by the dictionary definitions quoted above, the term necessarily implies that someone created software with the intent to gain unauthorized access to a computer for some nefarious purpose. The dissent offers no compelling reason why that cannot be determined objectively. Just like the certification at issue in *Ariix*, whether a given software qualifies as malware can be reduced to "a binary determination" based on "falsifiable criteria." 985 F.3d at 1122. The dissent's characterization of malware as "a spectrum of digital features with no verifiable line" is therefore incorrect.[4]

[4] The dissent contends that we have manufactured a claim against Malwarebytes stating, "Enigma has never alleged that Malwarebytes violated the Lanham Act based on the use of the term 'malware.'" Dissent at 42–43. Not so. Enigma alleged that Malwarebytes's software tells users that conducting a recommended "Threat Scan" "scans all the places *malware* is known to hide." SAC ¶ 132 (emphasis added). If Malwarebytes's software detected something as a "threat" or "PUP," the default configuration was to "treat detections as malware." SAC ¶¶ 133–34. The result is that Enigma customers using Malwarebytes's software to conduct a "Threat Scan" were left with the impression that Enigma's products were malware. *See, e.g.*, SAC ¶ 147 (stating that one customer contacted Enigma to inquire why "Malware bites [*sic*] says [Enigma's software] is an infection" and "another customer reported the 'malware bytes' program keeps detecting malware every time I try to download your software.'"); SAC ¶ 149 ("Please advise why your SpyHunter and RegHunter applications *are being detected as malware*.") (emphasis in

More importantly, judges are not experts in the cybersecurity field. We should not presume that we are. Enigma has alleged that those terms have implied meaning in that field which was understood by a significant portion of its users, SAC ¶¶ 143–64, such that Malwarebytes's allegedly false use of those terms can be proved or disproved as a matter of objective fact. Those allegations are not implausible, and the dissent does not claim that they are. To prevail, Enigma must ultimately prove that Malwarebytes's designation of its software was false. But at the motion to dismiss stage, the allegations are sufficient.

At root, the dissent's disagreement with our conclusion rests on its purported effort to protect expressions of "opinion" based on its misperception of the First Amendment. It makes that clear from its first paragraph. Dissent at 27. The dissent acknowledges that the protection afforded to commercial speech is limited and that "there can be no constitutional objection to the suppression of commercial messages that do not accurately inform the public." Dissent at 32 (quoting *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557, 562–63 (1980)). But it does not heed that distinction. As we said in *Ariix*,

> Today, consumers face waves of advertisements amid a sea of product choices. To navigate the seemingly unending stream of advertisements, consumers often depend on independent reviews for candid and accurate assessments. But when someone

original). In short, the dissent's contention is premised on a misreading of the record.

> falsely claims to be independent, rigs the ratings in exchange for compensation, and then profits from that perceived objectivity, that speaker has drowned the public trust for economic gain. Society has little interest in protecting such conduct under the mantle of the First Amendment.

Ariix, 985 F.3d at 1118–19.

In that case, we held that a five-star rating system comparing nutritional supplement products from the view of the speaker was an opinion not actionable under the Lanham Act. *Id*. at 1121. If Malwarebytes had said that its product was better than Enigma's product, that statement would be covered by *Ariix* and not subject to a Lanham Act claim. That is not the statement challenged by Enigma in this action, though. Malwarebytes stated that Enigma's products were a "threat" and "malicious." We conclude that those statements could be found to be statements of objective fact, subject to being found false. Like the "Medal of Achievement" certification in *Ariix*, those statements may properly be the subjects of a claim, outside the protection of the First Amendment, as we held in that decision. *Id*. at 1121–22.

The facts of this case do not closely match *Ariix*, but the principle is the same. Enigma has alleged that Malwarebytes disparaged Enigma's products for commercial advantage by making misleading statements of fact. If those allegations are true, and at this stage we must presume that they are, trying to wrap them in a First Amendment flag does not make them any less offensive or any less actionable. "Society has little interest in protecting such conduct under the mantle of the First Amendment." *Id*. at 1119.

B. Personal Jurisdiction

Enigma also argues the district court erred in holding that Malwarebytes was not subject to personal jurisdiction in New York and that California law applied to the dispute. We review personal jurisdiction rulings de novo. *Ayla, LLC v. Alya Skin Pty. Ltd.*, 11 F.4th 972, 978 (9th Cir. 2021).

As noted above, the Southern District of New York transferred this case to the Northern District of California.[5] Generally, diversity cases transferred under 28 U.S.C. § 1404(a) require that the transferee district court apply the state law, including the choice-of-law rules, of the original transferor court. *See Van Dusen v. Barrack*, 376 U.S. 612, 639 (1964) (holding, in a diversity case transferred at the request of the defendant, that "[a] change of venue under § 1404(a) generally should be, with respect to state law, but a change of courtrooms"); *Ferens v. John Deere Co.*, 494 U.S. 516, 529 (1990) (in another diversity case, extending the rule of *Van Dusen* to cases transferred at the request of the plaintiff); *Muldoon v. Tropitone Furniture Co.*, 1 F.3d 964, 965–66 (9th Cir. 1993) (under *Van Dusen* and *Ferens*, "the transferee court must follow the choice-of-law rules of the transferor court").

To apply the state law of the transferor jurisdiction in a § 1404(a) transfer case, the transferor court must have had personal jurisdiction over the defendant. Because the court in New York declined to rule on Malwarebytes's challenge to personal jurisdiction before transferring this case, "the

[5] The district court exercised federal question jurisdiction over Enigma's Lanham Act claim, *see* 28 U.S.C. § 1331, and—because the parties are citizens of different states—diversity jurisdiction over its state-law claims, *id*. § 1332.

transferee court must determine whether . . . jurisdiction would have been proper in the transferor court in order to decide which forum state's law will apply under *Erie*" and *Van Dusen*. *Davis v. Costa–Gavras*, 580 F. Supp. 1082, 1086 (S.D.N.Y. 1984) (citing *Roofing & Sheet Metal Servs., Inc. v. La Quinta Motor Inns, Inc.*, 689 F.2d 982, 992–93 (11th Cir. 1982); *Ellis v. Great Southwestern Corp.*, 646 F.2d 1099, 1107 (5th Cir. Unit A June 1981); *Martin v. Stokes*, 623 F.2d 469, 474 (6th Cir. 1980)); *see also Nelson v. Int'l Paint Co.*, 716 F.2d 640, 643 (9th Cir. 1983) (where transferor court lacked personal jurisdiction, state law of transferee court applies).

Accordingly, we must determine whether the court in New York had personal jurisdiction over Malwarebytes. If New York had such jurisdiction, as discussed above we must apply the law of New York to the state law claims; if the New York court lacked personal jurisdiction, we would apply the law of California.

"An exercise of personal jurisdiction in federal court must comport with both the applicable state's long-arm statute and the federal Due Process Clause." *Burri L. PA v. Skurla*, 35 F.4th 1207, 1212 (9th Cir. 2022). New York's long-arm statute states that a court may exercise specific personal jurisdiction over a non-resident if it "transacts any business within the state," N.Y. C.P.L.R. § 302(a)(1), and if the "cause of action 'aris[es] from' such a business transaction." *Best Van Lines, Inc. v. Walker*, 490 F.3d 239, 246 (2d Cir. 2007) (alteration in original) (quoting *Deutsche Bank Sec., Inc. v. Montana Bd. of Invs*., 850 N.E.2d 1140, 1142 (N.Y. 2006)).

"A defendant transacts business within the meaning of § 302(a)(1) when it purposefully 'avails itself of the

privilege of conducting activities [in New York], thus invoking the benefits and protections of its laws.'" *Brown v. Web.com Grp., Inc.*, 57 F. Supp. 3d 345, 356 (S.D.N.Y. 2014) (alteration in original) (quoting *Fischbarg v. Doucet*, 880 N.E.2d 22, 26 (N.Y. 2007)). "[P]roof of one transaction in New York is sufficient to invoke jurisdiction, even though the defendant never enters New York, so long as the defendant's activities [there] were purposeful and there is a substantial relationship between the transaction and the claim asserted." *Eades v. Kennedy, PC L. Offices*, 799 F.3d 161, 168 (2d Cir. 2015) (quoting *Chloé v. Queen Bee of Beverly Hills, LLC*, 616 F.3d 158, 163 (2d Cir. 2010)).

Whether there is personal jurisdiction based on the operation of a website depends on where the website falls on the "spectrum of interactivity." *Weiss v. Barc, Inc*., No. 12 CV 7571(TPG), 2013 WL 2355509, at *4 (S.D.N.Y. May 29, 2013). "Passive websites . . . are limited to making information available to users" and do not establish personal jurisdiction. *Id*. "Interactive websites knowingly transmit goods or services to users and if made available to New York residents, the activities can be sufficient for establishing personal jurisdiction over a defendant." *Id*. The website operated by Malwarebytes easily qualifies as interactive under *Weiss*.

As for whether the claim "arises from" a business transaction, the New York Court of Appeals has held that the "arising from" prong of Section 302(a)(1) does not require but-for causation between a defendant's New York business activity and a plaintiff's injury. *Licci v. Lebanese Canadian Bank*, 984 N.E.2d 893, 900 (N.Y. 2012). Instead, it requires "a relatedness between the transaction and the legal claim such that the latter is not completely unmoored from the former . . . . In effect, the 'arise-from' prong limits the

broader 'transaction-of-business' prong to confer jurisdiction only over those claims in some way arguably connected to the transaction." *Id.* at 900–01.

Applying these standards, Malwarebytes is subject to personal jurisdiction in New York. First, Malwarebytes "transacts business" in New York through its website, which allows New York–based users to buy and download products.[6] Malwarebytes does not have to be physically present in New York to transact business there within the meaning of the first clause of Section 302(a)(1). *See Chloé*, 616 F.3d at 169 (collecting cases). Second, Enigma's claims in this lawsuit arise at least in part out of Malwarebytes's transaction of business in New York. Courts in New York have held that the sale of copyright- and trademark-infringing works into New York through the internet is sufficient to establish personal jurisdiction under the "arising under" prong.[7]

New York's exercise of personal jurisdiction is also consistent with the Due Process Clause. *See Knight v. Standard Chartered Bank*, 531 F. Supp. 3d 755, 763

---

[6] *Cf. Citigroup Inc. v. City Holding Co*., 97 F. Supp. 2d 549, 565–66 (S.D.N.Y. 2000) (finding that a website permitting New Yorkers to apply for loans and communicate with defendant's employees was "unqualifiedly commercial in nature," rising to the level of transacting business required by § 302(a)(1)); *NFL v. Miller*, No. 99 Civ. 11846 JSM, 2000 WL 335566, at *1 (S.D.N.Y. Mar. 30, 2000) ("[O]ne who uses a web site to make sales to customers in a distant state can thereby become subject to the jurisdiction of that state's courts.").

[7] *See, e.g.*, *Mattel, Inc. v. www.fisher-price.online*, No. 21-CV-9608 (LJL), 2022 WL 2801022, at *4 (S.D.N.Y. July 18, 2022) (defendant's sale of counterfeit products in New York had "a substantial relationship with Plaintiff's claim that Defendant counterfeited and infringed upon [its trademarks] in violation of the Lanham Act").

(S.D.N.Y. 2021) ("[B]ecause the Due Process Clause permits the exercise of jurisdiction in a broader range of circumstances [than] N.Y. C.P.L.R. § 302, . . . a foreign defendant meeting the standards of § 302 will satisfy the due process standard.") (internal quotation marks and citation omitted). Therefore, if an exercise of personal jurisdiction satisfies New York's long-arm statute, it also satisfies the Due Process Clause. *See D.H. Blair & Co. v. Gottdiener*, 462 F.3d 95, 105 (2d Cir. 2006) ("[T]he constitutional requirements of personal jurisdiction are satisfied because application of [§ 302(a)] meets due process requirements.").

We therefore reverse the district court's holding that New York lacked personal jurisdiction over Malwarebytes and that California law applies to Enigma's state law claims. New York has personal jurisdiction over Malwarebytes with respect to its sales to New York–based customers, and therefore New York law applies to Enigma's state-law claims based on those transactions. We do not decide whether New York law applies to Malwarebytes's transactions with other customers outside the state of New York. That choice of law question is not before us in the current appeal.

C. State-law Claims

1. NYGBL § 349

The district court dismissed Enigma's NYGBL § 349 claim for two reasons. The first was that New York law did not apply. The second was that "an opinion that is not actionable under the Lanham Act is also not actionable under the NYGBL § 349." Because we hold that New York law applies and that Enigma's Lanham Act claim is actionable, we reverse the dismissal of the NYGBL claim and remand to the district court to reinstate.

2. *Tortious interference claims*

Enigma also argues that the district court erred in dismissing its claims for tortious interference with contractual and business relations. The district court construed the tortious interference claims under California law, but as discussed above, New York law applies to these claims. Reading the complaint in the light most favorable to the plaintiff, as we must, Enigma has sufficiently pled its cause of action for tortious interference with business relations but has failed to do so for tortious interference with contractual relations.

a. Tortious interference with business relations

To state a claim for tortious interference with business relations, New York requires a plaintiff to establish that:

> (1) it had a business relationship with a third party; (2) the defendant knew of that relationship and intentionally interfered with it; (3) the defendant acted solely out of malice, or used dishonest, unfair, or improper means; and (4) the defendant's interference caused injury to the relationship.

Kirch v. Liberty Media Corp., 449 F.3d 388, 400 (2d Cir. 2006) (quoting *Carvel Corp. v. Noonan*, 350 F.3d 6, 17 (2d Cir. 2003)). Enigma's complaint plausibly demonstrated each of these factors.

Enigma stated in its complaint that it had contracts with customers who purchased subscription-based licenses to use its SpyHunter 4 and RegHunter 2 software. SAC ¶ 235. Enigma also stated that it and Malwarebytes had some customers in common who, seeking added levels of security,

simultaneously used both companies' products. SAC ¶ 236. Enigma further alleged Malwarebytes took a series of steps to interfere with its prospective relationships with customers. For instance, Enigma stated that Malwarebytes (1) falsely labelled Enigma's products as "threats" and "PUPs," (2) automatically blocked customers from installing Enigma's software, and (3) automatically quarantined and preselected Enigma software for deletion. SAC ¶¶ 237–39. The result of this conduct, Enigma alleges, is that Malwarebytes induced Enigma's customers to choose either not to install, or to delete, Enigma's programs from their computers without any legitimate justification. SAC ¶ 240.

Further, Enigma alleged the prospective relationships with the requisite specificity to establish a claim for tortious interference with business relations. New York requires that a "plaintiff . . . identify a specific customer that the plaintiff would have obtained 'but for' the defendant's wrongful conduct," *Zetes v. Stephens*, 969 N.Y.S.2d 298, 304 (4th Dep't 2013), as relief should not be afforded for merely speculative damage, *see, e.g.*, *Parekh v. Cain*, 948 N.Y.S.2d 72, 76 (2d Dep't 2012) (dismissing a claim for tortious interference with business relations because the plaintiff did not identify a third party with which the plaintiff had business relations). For this, Enigma asserted that certain customers downloaded its software before paying for a full subscription. SAC ¶¶ 244–46. Because Enigma points to identifiable customers whose business it lost, its complaint plausibly alleges that it had business relationships with third parties.

The district court's dismissal of this claim for Enigma's inability to identify an independent wrongful act was erroneous for two reasons. First, Enigma's reinstated claims under the Lanham Act and NYGBL § 349 could serve as

independent wrongful acts if such a showing were necessary. More importantly—and unlike under California law, *see Ixchel Pharma, LLC v. Biogen, Inc*., 470 P.3d 571, 576 (Cal. 2020) ("[I]ntentionally interfering with prospective economic advantage requires pleading that the defendant committed an independently wrongful act.")—a claim for tortious interference with business relations under New York law does not require the plaintiff to show an "independent wrongful act." Instead, Enigma only needs to allege that Malwarebytes acted "solely out of malice, or used dishonest, unfair, or improper means," *Kirch*, 449 F.3d at 400, which it did in its complaint. *See* SAC ¶ 249 (Malwarebytes acted "for the sole purpose of inflicting intentional harm upon [Enigma]"). Accordingly, we hold that Enigma sufficiently alleged the elements of a claim for tortious interference with business relations.

b. Tortious interference with contractual relations

To establish a claim of tortious interference with contract under New York law, a plaintiff must plead the following elements:

> (1) the existence of a valid contract between the plaintiff and a third party; (2) the defendant's knowledge of the contract; (3) the defendant's intentional procurement of the third-party's breach of the contract without justification; (4) actual breach of the contract; and (5) damages resulting therefrom.

Kirch, 449 F.3d at 401 (internal quotation marks and citation omitted).

The district court held that the contractual relations interference claim failed because Enigma did not identify any contractual breach that Malwarebytes induced. Although the district court improperly analyzed this claim under California law, the bottom-line result was still correct under New York law.

To state a claim for tortious interference with contractual relations under New York law, a plaintiff must allege that the defendant induced an actual breach of contract. *See NBT Bancorp Inc. v. Fleet/Norstar Fin. Grp., Inc.*, 664 N.E.2d 492, 495–96 (N.Y. 1996) (holding that, although tortious interference can take many forms, New York mandates that actual breach be shown). Here, Enigma alleged that its preexisting customers *cancelled* their subscriptions and requested refunds because of Malwarebytes's conduct. SAC ¶¶ 239–41. And although this amounts to disruption of the contractual relationship between Enigma and its customers, it falls short of alleging any contractual breach by those customers. Because New York law requires such a breach, Enigma has not adequately pled one of the required elements for a claim of tortious interference with contractual relations.

III. Conclusion

We affirm the district court's dismissal of Enigma's claim of tortious interference with contractual relations. We reverse the district court's dismissal of Enigma's remaining claims and remand for further proceedings consistent with this opinion. Each party is to bear its own costs.

AFFIRMED in PART, REVERSED in PART, and REMANDED for further proceedings.

BAKER, Judge, concurring:

I join the majority opinion in full and write separately to briefly touch on choice of law. As the opinion acknowledges, ordinarily the application of a transferor jurisdiction's law under *Van Dusen* and *Ferens* carries with it the choice-of-law rules of that jurisdiction. *See Muldoon v. Tropitone Furniture Co*., 1 F.3d 964, 965 (9th Cir. 1993) (under *Van Dusen* and *Ferens*, "the transferee court must follow the choice-of-law rules of the transferor court").

Here, however, the parties have not addressed choice of law beyond the dispute over whether personal jurisdiction existed in the Southern District of New York. They appear to agree that if such jurisdiction existed, then New York substantive law would govern Enigma's state-law claims and, conversely, if such jurisdiction were lacking, then California substantive law would apply. The opinion therefore assumes—as the parties did in their briefing by not addressing choice of law—that New York's choice-of-law rules require application of that state's substantive law to Enigma's state-law claims, save for the claims based on Malwarebytes's transactions with customers located elsewhere.

BUMATAY, Circuit Judge, dissenting:

When a cybersecurity company flags another company's products as "potentially unwanted programs," "threats," or "malicious," could it be liable for false advertising under the Lanham Act? The answer is plainly "no." The Lanham Act protects against false or misleading representations of fact. *See* 15 U.S.C. § 1125(a)(1)(B). But flagging a competitor's products as "potentially unwanted," a "threat," or "malicious" is no expression of fact—these are subjective statements, not readily verifiable. That means they are opinions. The freedom to express opinions is at the core of the First Amendment. And that guarantee doesn't change because the opinions are about cybersecurity, malware, or internet domains.

Thus, even in the commercial context, we must be careful not to expand Lanham Act liability to encompass protected opinions. Unfortunately, that is exactly what our court does here. We mistake subjective expressions of opinion for provable statements of fact—falling for the claim that some of these terms have an uncontested, objective meaning in the cybersecurity field. Yet even a cursory review shows that's not true. By treating these terms as actionable statements of fact under the Lanham Act, our court sends a chilling message to cybersecurity companies—civil liability may now attach if a court later disagrees with your classification of a program as "malware." But we have neither the authority nor the competence to arrogate to ourselves regulatory oversight over cybersecurity.

For these reasons, I respectfully dissent.

I.

Enigma Software Group USA, LLC and Malwarebytes, Inc. develop competing anti-malware software products. "Malware" is a portmanteau of "malicious" and "software." Oxford English Dictionary Online (2022). So, as the term implies, anti-malware programs are designed to detect and remove potentially unwanted, threatening, or malicious programs from users' computers. For eight years, from 2008 to 2016, the two companies' products coexisted on users' systems without issue. But in 2016, things changed. In October of that year, Malwarebytes announced that it was getting "tougher" on potentially unwanted programs. The move was purportedly a response to software developers' efforts to circumvent the company's detection criteria.

Malwarebytes provided a statement announcing its new criteria:

> **How do we identify potentially unwanted software?**
>
> Analyzing and categorizing potentially unwanted software is a complex problem. Developers of potentially unwanted software rapidly evolve their products. Some even contain a few characteristics that resemble legitimate software to mask the unwanted functionality. It's an on-going process, and we work hard to identify common behaviors that help provide you the highest level of protection. In some cases, where the behavior is questionable, we will list the application even if it does not neatly fit into

> the listed criteria. In other words, we use our judgment.
>
> While we highlight potentially unwanted programs, you then make a choice in the exclusions list and select what you want to keep or remove.
>
> Here are some of the criteria we use:
>
> • obtrusive, misleading, or deceptive advertising, branding, or search practices
>
> • excessive or deceptive distribution, affiliate or opt-out bundling practices
>
> • aggressive or deceptive behavior especially surrounding purchasing or licensing
>
> • unwarranted, unnecessary, excessive, illegitimate, or deceptive modifications of system settings or configuration (including browser settings and toolbars)
>
> • difficulty uninstalling or removing the software
>
> • predominantly negative feedback or ratings from the user community
>
> • diminishes user experience
>
> • other practices generally accepted as riskware, scareware, adware, greyware, or otherwise commonly unwanted software by the user community

Malwarebytes informed its users that it must "regularly update" its software to meet these criteria. The company

also warned that "sometimes [it] get[s] it wrong" and provided an email address to ask for "reconsideration" of its decisions. Noting the need to respond promptly to "new forms of potentially unwanted software" that "frequently emerge and proliferate," Malwarebytes "reserve[d] the right to adjust, expand and update [its] criteria without prior notice or announcements."

Under the new criteria, Malwarebytes' software designated two of Enigma's anti-malware products—"SpyHunter 4" and "RegHunter 2"—as "potentially unwanted programs" and "threats." As a result, Malwarebytes' program blocked, quarantined, or disabled SpyHunter 4 and RegHunter 2's operation on users' computers. Enigma contends that Malwarebytes blocked its programs because of "anticompetitive animus" and in retaliation for Enigma suing a Malwarebytes affiliate. According to Malwarebytes, its program flagged SpyHunter 4 and RegHunter 2 as "scareware"—which Malwarebytes defines as programs that detect harmless system files and browser cookies and present them with alarming graphics "to convince users their systems have problems."

Malwarebytes' users had at least two options available if they wished to continue using Enigma's products. They could exclude Enigma's programs from scans by "unchecking" and "ignor[ing]" the detection following Malwarebytes' instructions, or they could stop using Malwarebytes' program. But Enigma disputes whether both programs can operate together. It argues that Malwarebytes' default settings effectively prevent users from excluding Enigma's programs from scans, citing complaints from users who struggled to change them.

In December 2016, in response to Malwarebytes' change of criteria, Enigma issued a "Countermeasure," which allowed Enigma's customers to download an installer that disabled Malwarebytes' products. Shortly after, Malwarebytes responded by having its anti-malware program block access to Enigma's web domains—URLs ending in ".enigmasoftware.com." Malwarebytes' program flagged the domains with a pop-up—"Malicious Website Blocked." Enigma alleges that Malwarebytes' domain blocking was retaliation for the "Countermeasure." After some time, Malwarebytes stopped flagging Enigma's domains, which Enigma takes as a concession that quarantining its websites was improper.

Enigma sued, alleging false advertising under the Lanham Act and various torts under New York state law. Enigma first brought suit in the Southern District of New York, which transferred the case to the Northern District of California. In the Northern District of California, the district court granted Malwarebytes' first motion to dismiss based on immunity under § 230 of the Communications Decency Act, 47 U.S.C. § 230. A divided panel of this court reversed because we held that "immunity under [§ 230] does not extend to anticompetitive conduct." *Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1054 (9th Cir. 2019). Dissenting, Judge Rawlinson noted that the majority's policy justifications for the carveout contravened both text and precedent. *Id.* at 1054–55 (Rawlinson, J., dissenting).

On remand, the district court again granted Malwarebytes' motion to dismiss. This time, the district court held that Malwarebytes' flagging of Enigma's products conveyed "non-actionable statements of opinion." *Enigma Software Grp. USA, LLC v. Malwarebytes Inc*.,

2021 WL 3493764, at *11 (N.D. Cal. 2021). Enigma appealed.

On de novo review, this should have been an easy affirm.

II.

A.

When it comes to the regulation of any speech, we should always begin with the First Amendment. The First Amendment protects against laws that abridge the freedom of speech. U.S. Const. amend. I. And that's true even in the commercial context. Since *Virginia Pharmacy Board v. Virginia Citizens Consumer Council, Inc*., 425 U.S. 748 (1976), the Supreme Court has recognized that First Amendment protections apply to the regulation of purely commercial speech. *Id.* at 761, 770. Such freedom advances at least three purposes: it "serves the economic interest of the speaker," it "assists consumers," and it "furthers societal interest in the fullest possible dissemination of information." *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557, 561–62 (1980).

Of course, the Constitution "accords a lesser protection to commercial speech than to other constitutionally guaranteed expression," and so "there can be no constitutional objection to the suppression of commercial messages that do not accurately inform the public." *Id*. at 562–63. But unless the commercial communication is "misleading," the government's power to circumscribe commercial speech is limited. *Id*. at 564.

This is where the Lanham Act fits in. In 1946, Congress created a cause of action for "unfair competition through misleading advertising or labeling." *POM Wonderful LLC v. Coca-Cola Co.*, 573 U.S. 102, 107 (2014). To protect

companies from competitors' false attacks, § 43(a) of the Lanham Act creates civil liability for:

> Any person who, on or in connection with any goods or services, . . . uses in commerce any . . . false or misleading description of fact, or false or misleading representation of fact, which . . . in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities[.]

15 U.S.C. § 1125(a)(1)(B). So, on one hand, to state a claim under the Lanham Act, a plaintiff must show that the defendant made "false or misleading representations of fact." *Ariix, LLC v. NutriSearch Corp.*, 985 F.3d 1107, 1121 (9th Cir. 2021). On the other hand, given the freedom of speech, "statements of opinion" are beyond the purview of the Lanham Act. *Id*.

With the First Amendment overlay here, we must be careful in delineating what constitutes "fact" versus "opinion." While statements of fact are actionable under the Lanham Act, "[s]tatements of opinion and puffery . . . are not." *Id*. And it makes no difference if the statements of opinion are made for the purpose of anticompetitive gain. After all, the suppression of "opinions"—even in the commercial space—gets into murky constitutional waters. Even so, it's not always easy to distinguish between the two. *See, e.g., Cochran v. NYP Holdings, Inc.*, 210 F.3d 1036, 1038 (9th Cir. 2000) (per curiam) ("[A] statement of opinion is not automatically entitled to First Amendment protection simply by virtue of its status as opinion; rather, a statement

of opinion may be actionable to the extent that it implies a false assertion of fact." (simplified)).

But our court has developed some good guideposts. Commercial speech is actionable if it is "specific and measurable," "capable of being proved false or of being reasonably interpreted as a statement of objective fact." *Ariix*, 985 F.3d at 1121. In other words, "a statement that is quantifiable, that makes a claim as to the specific or absolute characteristics of a product" may be actionable under the Lanham Act. *Newcal Indus., Inc. v. Ikon Off. Sol.*, 513 F.3d 1038, 1053 (9th Cir. 2008) (simplified). Given the serious creep on First Amendment protections when we curtail speech, when "it is highly debatable" whether a statement is verifiable enough to be actionable, we must "err on the side of nonactionability." *Partington v. Bugliosi*, 56 F.3d 1147, 1158–59 (9th Cir. 1995) (simplified).

Ariix is a good example of how these principles work. In that case, a nutrition-and-health research company published a guide that compared and reviewed nutritional supplements using a five-star rating system based on 18 criteria. 985 F.3d at 1111. It also awarded a "Medal of Achievement" to nutritional supplements manufacturers that meet two measurable conditions: (1) compliance with FDA's "good manufacturing practices" and (2) certification of product labels by an approved laboratory. *Id*. The research company portrayed itself to the public as independent, presenting only objective data and scientific analyses. But privately the company allegedly had financial ties to one manufacturer of nutritional products. *Id.* at 1112. The company was then accused of improperly manipulating the rating system and withholding the certification from a competing manufacturer that met the two conditions. *Id.* at 1112–13.

We first considered whether the company's five-star ratings were actionable. 985 F.3d at 1121. We said no. Even though the ratings were purportedly based on "objective and scientific criteria," we still held that they were not factual. *Id*. That's because "there is an inherently subjective element in deciding which scientific and objective criteria to consider." *Id.* As an example, we compared the ratings to college or law school rankings. While objective criteria go into the rankings (like acceptance rates, test scores, and class size), "selecting those criteria involves subjective decision-making." *Id*. Thus, we concluded that the ratings were "simply statements of opinion about the relative quality of various nutritional supplement products." *Id*.; *cf. Underwager v. Channel 9 Australia*, 69 F.3d 361, 367 (9th Cir. 1995) (concluding statements must rest "on a core of objective evidence" to be provable as true or false under defamation law).

But the "Medal of Achievement" certification was different. The award (or more precisely, the lack of an award) makes "specific and measurable statements" about a nutritional supplements manufacturer. *Ariix*, 985 F.3d at 1121–22. The company's certification is "a binary determination" based on "falsifiable criteria" and the failure to award the certification (when a manufacturer complies with the two criteria) "falsely implies to consumers" that the manufacturer did not meet manufacturing or labeling standards. *Id.* at 1122. Because "[t]hese implications are specific, measurable, and capable of being falsified," we held that they were actionable statements under the Lanham Act. *Id*.

So boiled down, whether commercial speech is actionable depends on whether the statement implies something that can be proven false.

With this legal background, I turn to Enigma's claims against Malwarebytes.

B.

Here, we must determine whether Malwarebytes' statements calling Enigma's products "potentially unwanted," a "threat," or "malicious" can be proven false. Given that each warning has an "inherently subjective element," *id.* at 1121, the answer is no. Even if Malwarebytes employed these terms to protect its products from competition from Enigma, there are no dispositive, objective criteria that would allow us to police whether the three terms were falsely used against Enigma. In other words, unlike the certification in *Ariix*, the three statements aren't "binary determinations." *Id*. Contrary to Enigma's claims, a program isn't simply "potentially unwanted" or not. A software program isn't verifiably a "threat" or not. And a website isn't measurably "malicious" or not. In the cybersecurity context, these terms refer to a spectrum of digital features with no verifiable line to cross to determine when they apply. *Cf. Underwager*, 69 F.3d at 367 ("the term 'lying' applies to a spectrum of untruths including 'white lies,' 'partial truths,' 'misinterpretation,' and 'deception'" and so is nonactionable). They thus depend on "subjective decision-making," *Ariix*, 985 F.3d at 1121, requiring the exercise of judgment to determine when the warning is warranted.

Without a "core of objective evidence" to assess the accuracy of the use of the warnings, *Underwager*, 69 F.3d at 367, no reasonable factfinder can say that Malwarebytes made a false representation of fact in labeling Enigma's products or website as a "threat," "malicious," or "potentially unwanted." In fact, nowhere does Enigma offer

an objective, measurable definition of the warnings from which we may draw an implication of testable falsehoods. Instead, Enigma hints that they carry "specific factual meanings" in the cybersecurity field and discovery is required before we may fully understand this. As shown below, this is not enough to state a claim under the Lanham Act, and we should have affirmed the dismissal of Enigma's claims.

i. Potentially Unwanted Program

Take the phrase "potentially unwanted program." That designation inherently requires some guesswork—estimating whether a program would be wanted—as made clear by using the term "potentially." And "unwanted" fits within the type of nonactionable "personal assessments or criticisms" that enjoy First Amendment protections. *See Partington*, 56 F.3d at 1158 (observing that "fake," "phony," "hefty mark-up," and "unfair" are too subjective or unprovable to be actionable). So the ordinary meaning of the phrase conveys both uncertainty and subjectivity—not falsifiability.

If there were any question about the subjective nature of the phrase, Malwarebytes made it clear that it developed its own criteria to determine what's "potentially unwanted." Malwarebytes announced eight criteria for the designation, including obtrusive or misleading advertising, negative feedback, the difficulty in uninstalling or removing a program, and whether the program can be considered "riskware, scareware, adware, greyware, or otherwise commonly unwanted by the community." It also acknowledged that some malware didn't "neatly fit into the listed criteria," which only represented "some of the criteria." It explained that identifying malware was

ultimately a judgment call, and "sometimes we get it wrong." To address the changes in programming, Malwarebytes expressly "reserve[d] the right to adjust, expand and update [its] criteria without prior notice or announcements."

Malwarebytes was thus explicit that subjectivity inhered in its "potentially unwanted program" determinations. As in *Ariix*, when a company develops a rating or designation containing "inherently subjective element[s]," like the eight criteria here, the designation cannot be actionable. Even if some of Malwarebytes' criteria could be treated as objective and technical, it would have no impact on the analysis. That's because "there is an inherently subjective element in deciding which scientific and objective criteria to consider." *Ariix*, 985 F.3d at 1121. And the weight assigned to each criterion would also reflect Malwarebytes' subjective assessment of what constitutes a "potentially unwanted product." *Id.*

In response, Enigma offers no objective, factual definition of its own. Nor does Enigma provide any evidence that the term has an agreed-upon and well-known meaning in the cybersecurity world. Indeed, Enigma's own allegations prove the phrase's subjective nature. For instance, Enigma's complaint alleges "Malwarebytes' new criteria rejected specific objective or scientific standards in favor of subjective characteristics." Similarly, Enigma repeatedly criticized Malwarebytes' criteria as "subjective," "vague," and "self-serving"—grounds on which we have previously held statements unactionable under the Lanham Act. *See Coastal Abstract*, 173 F.3d at 731 ("vague and subjective" statements are not liable under the Lanham Act). So crediting the complaint's allegations (as we must), Enigma "may [have] plead[ed] [it]self out of court."

Weisbuch v. County of Los Angeles, 119 F.3d 778, 783 n.1 (9th Cir. 1997).

ii. Threat

The analysis of the "threat" designation fares no better. Start with its ordinary meaning. Like "potentially" unwanted programs, "threat" generally refers to a "*possible* source of harm or danger." *American Heritage Dictionary of the English Language* (5th ed. 2011) (emphasis added). Given its tentative nature, it is not an absolute or specific measurement. And, as with "unwanted," a "source of harm or danger" involves a subjective determination. *See, e.g.*, *Hernandez v. Scottsdale Hotel Grp. LLC*, 2020 WL 6827745, at *3 (D. Ariz. Nov. 20, 2020) (holding the word "threatening" in a defamation suit "is not provable or falsifiable"). Indeed, Malwarebytes' user guide emphasizes that some programs or files categorized as "threats" are "not malicious" and "[i]t is up to individual users to research and make this determination." Malwarebytes User Guide, "Quarantine," § 8.1 (2016).

Enigma, for its part, doesn't contend that there is a single criterion for identifying software as a "threat." Instead, it suggests that the term is "widely used" and "commonly understood" in cybersecurity—pointing to several definitions from federal statutes and governmental and software industry authorities. But even accepting these definitions, they also confirm the subjective nature of the term "threats" and so undermine Enigma's assertions.

First, Enigma offers the National Institute of Standards and Technology ("NIST") glossary for a definition of "threat." But NIST's glossary has *no fewer than 20*

definitions for "threat."[1] Those definitions range from "[a]ny circumstance or event with the potential to adversely impact organizational operations . . . through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service" to "an activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity." *Id*. Thus, "threat" is defined in only the broadest terms—"potential" for "harm" and "adverse[] impacts"—with no attempt to narrow the field. And NIST prefaces its glossary with the warning that "[t]erminology changes over time" and its definitions may "contain potentially biased terminology." *Id*.

Next, Enigma asks us to adopt the International Organization for Standardization's ("ISO") definition of "threat." It provides that a "threat" is "a potential cause of an unwanted incident, which can result in harm to a system or organization." ISO/IEC 27000, Info. Sec. Mgmt. Standard, at 10 (2018). The problems with this definition are obvious. It requires a subjective assessment of what is "unwanted," and it requires some guessing because it applies to anything that "potential[ly]" causes harm. As with "potentially unwanted programs," such a definition offers no measurable or objective guidance.

Finally, Enigma looks to the definition of "cybersecurity threat" from the Cybersecurity Act of 2015, 6 U.S.C. §§ 650, 1501. The Act defines "threat" as:

---

[1] *Comput. Sec. Res. Ctr. Glossary*, U.S. Dep't. of Com. Nat'l Inst. of Standards and Tech. (NIST), available at: https://csrc.nist.gov/glossary/term/threat [https://archive.is/5yDWa].

> "[A]n action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system."

6 U.S.C. § 650(8)(A). Thus, this federal definition applies to a broad range of "impact[s]" and requires a subjective assessment of what is "adverse[]." Acknowledging the ambiguity of its definition, the Act excludes "any action that solely involves a violation of a consumer term of service or a consumer licensing agreement." § 650(8)(B).

Nothing in these definitions supplies an objective, measurable basis to assess the term's veracity. In fact, Enigma's identification of multiple meanings for "threats" *by itself* shows that the term represents an opinion rather than a fact. *See Steam Press Holdings, Inc. v. Hawaii Teamsters, Allied Workers Union, Loc. 996*, 302 F.3d 998, 1008–09 (9th Cir. 2002) (approving argument that a phrase "subject to multiple interpretations" is not "susceptible of verification"). As we've said, when a term or phrase lacks a "singular" and "concrete" meaning, it cannot be "readily verifiable." *Id*. at 1009. So Enigma's own attempt to provide meaning to the term only establishes its vague and unfalsifiable nature.

iii. Malicious

Nor does "malicious" have an objective and absolute measurement. In its complaint, Enigma pleads that calling a website "malicious" has a common meaning in the

"cybersecurity and privacy software markets"—"that the website is harmful and can be disruptive to [users'] computers." Even if we accept this allegation as pleaded fact, this definition of "malicious" reeks of subjectivity. Because of the vagueness and inherent non-objectiveness of "harmful" and "disruptive" in the definition of "malicious," the designation suffers from the same deficiencies as the other two—there is no implied objective fact that can be proven right or wrong. What can be "harmful" or "disruptive" is necessarily in the eye of the beholder. Imagine an energetic child in the classroom. Some might view the child as "playful," while others view him as "disruptive." Or spicy food. Some may find it enjoyable, while others might find it "harmful" to their digestion.

Likewise, whether Enigma's "Countermeasure" to disable Malwarebytes' software was "harmful" and "disruptive" is a matter of opinion. To Malwarebytes, a website that offered a program that deliberately targeted and removed its anti-malware products could fit the bill. To Enigma, its website was innocuous and only allowed its customers the choice to continue to use its products without interference from Malwarebytes. Rather than weighing in on this difference of opinion, we should have allowed the market to decide who is right.

C.

Ignoring the problems with the inherent subjectivity of these terms, the majority presses on with the expansion of Lanham Act liability here because, it claims, the term "malware" lends itself to verification. Maj. Op. 14. There are several problems with this.

First, Enigma has never alleged that Malwarebytes violated the Lanham Act based on the use of the term

"malware." To prove the Lanham Act claim, Enigma's complaint alleges that Malwarebytes used "false and misleading statements" in commerce based on "statements that SpyHunter 4 and RegHunter 2 are 'threats' and/or 'potentially unwanted programs' and that [Enigma's] website and domains are 'malicious' and disruptive." The term "malware" is not included among the statements allegedly violative of § 1125(a)(1)(B). Indeed, there's no basis to equate the terms "threats," "potential unwanted," and "malicious" with "malware." Malwarebytes' user guide defines "potentially unwanted programs" as a "class[] of *non-malware*," and explains that some programs "may [be] categorized as threats" even though they "are not malicious." Malwarebytes User Guide, "Quarantine," § 8.1 (2016). And Malwarebytes only referred to Enigma's *website domains* as "malicious," not its software. A malicious website may *host* malware, but calling a *website* malware is like calling a street address a criminal. So the majority is manufacturing its own claim against Malwarebytes—one that isn't even supported by the record.

To justify the *sua sponte* amendment of Enigma's complaint, the majority looks to Malwarebytes' user guide, which explains that a default setting for its scan configuration "[t]reat[s] detections" of potentially unwanted programs "as malware." Maj. Op. 14 n.4. But this allegation is irrelevant because the majority agrees that calling something "potentially unwanted" is "too unspecific" to be actionable under the Lanham Act. The majority also relies on the user guide's reference to a "Threat Scan," which "captures all programs treated as '*malware*' in all the places *malware* is known to hide." *Id*. But user guide statements that Malwarebytes' program *treats* something as "malware" or *scans* where malware is known to be isn't the same thing

as calling Enigma's products "malware" in commerce. The majority then somehow finds it actionable that *Enigma's own customers* called Enigma's programs "malware." *Id*. (citing allegations that Enigma's customers thought Enigma's products were "malware"). But what Enigma's customers say about Enigma is not a basis to find Lanham Act liability *against Malwarebytes*.

Second, while acknowledging that "judges are not experts in the cybersecurity field," the majority invents its own verifiable definition of "malware" for the field—"software [created] with the intent to gain unauthorized access to a computer for some nefarious purpose." *Id*. The majority then concludes that "malware can come in many in forms including 'viruses, spyware, adware, ransomware, and Trojans.'" *Id*. at 14. And finally, the majority says that these terms can be objectively determined. *Id*. at 14.

Even if Enigma's complaint *had* alleged that Malwarebytes designated Enigma's products as "malware" and if this definition were plausible, the majority's terminology admits subjectivity. One needn't be an expert in cybersecurity to see why. Take "adware." Adware monitors users' online activities and habits, typically without their knowledge, and uses the collected data to display targeted advertisements or sell to third parties. Adware usually comes bundled with free software (e.g., games, browser extensions, media players), allowing developers to generate revenue and continue developing useful and free software. Adware can expose sensitive data and slow or disrupt one's computer, though it also helps serve users with more relevant ads. And typically, the user has inadvertently authorized and consented to the adware's operation via a terms and conditions agreement. In such cases, has the adware been created and employed for "some

nefarious purpose?" This is plainly a subjective question that will elicit different responses from different people.

The majority also insists that "[j]ust like the certification at issue in *Ariix*," the "malware" designation "can be reduced to 'a binary determination' based on 'falsifiable criteria.'" Maj. Op. 14. It would seem the majority conflates the ability to *phrase* something as a binary determination, with the *objectivity* of that determination. One could also say, "whether green is the best color is objective and verifiable, because either it is the best, or it's not the best." But clearly that's a subjective question—appending "it is or it isn't" doesn't make the determination objective and verifiable. *See ZL Techs, Inc. v. Gartner, Inc.*, 709 F. Supp. 2d 789, 798 (N. D. Cal. May 3, 2010). And calling Enigma's products a "threat" or "malicious" is far from Ariix saying a manufacturer didn't comply with FDA standards or obtain the appropriate laboratory certification—both falsifiable criteria. *Ariix*, 985 F.3d at 1122.

* * *

In sum, Enigma cannot base its false advertising claim on nonactionable opinions, like the phrases here. We thus should have affirmed the dismissal of the Lanham Act claim.

III.

Not only is Enigma's failure to allege a misstatement of fact dispositive on the Lanham Act claim, but it's also dispositive on its state-law claims. We thus should have also affirmed the dismissal of Enigma's claims for (1) violation of New York General Business Law § 349, (2) tortious interference with business relations, and (3) tortious interference with contractual relations. In reviving the § 349

and business relations claims, the majority concludes that New York has personal jurisdiction over Malwarebytes. While I have serious reservations about the majority's jurisdictional analysis, we didn't need to reach that question because Enigma's claims would fail under either New York or California law.

First, General Business Law § 349, New York's law against deceptive business acts and practices, generally follows the Lanham Act. "[W]hat is non-actionable opinion under the Lanham Act is also non-actionable . . . under General Business Law § 349." *ONY, Inc. v. Cornerstone Therapeutics, Inc*., 720 F.3d 490, 498 (2d Cir. 2013). Since I would conclude that Malwarebytes' flagging of Enigma's products was non-actionable opinion, Enigma's § 349 claim must be dismissed as well.

Second, Enigma's claim for tortious interference with business relations is not viable under either California or New York law. In California, "interference with prospective economic advantage requires a plaintiff to allege an act that is wrongful independent of the interference itself." *CRST Van Expedited, Inc. v. Werner Enters., Inc*., 479 F.3d 1099, 1108 (9th Cir. 2007). "[A]n act is independently wrongful if it is unlawful, that is, if it is proscribed by some constitutional, statutory, regulatory, common law, or other determinable legal standard." *Korea Supply Co. v. Lockheed Martin Corp*., 63 P.3d 937, 954 (Cal. 2003). New York has adopted a similar general rule requiring an "independently unlawful act" for tortious interference with a business relationship. *Carvel Corp. v. Noonan*, 818 N.E.2d 1100, 1103 (N.Y. 2004). There is an "exception" in New York, however, when a defendant engages in "egregious wrongdoing" in the absence of an independent act, like

acting for the "sole purpose of inflicting intentional harm on plaintiffs." *Id*. at 1102–03 (simplified).

Here, because Enigma's Lanham Act claim fails, it hasn't shown that Malwarebytes engaged in independent wrongdoing for a business interference tort. And while Enigma alleges that Malwarebytes acted with anti-competitive animus, that is not enough to invoke New York's exception to the general rule because the exception does not apply to "normal economic self-interest." *Id*. at 1103. As Enigma alleged, Malwarebytes also sought to increase sales and "secur[e] a stronger, more dominant" market position for itself. Thus, Enigma concedes that Malwarebytes did not act "solely" to target Enigma, which the exception requires. *See id*. at 1103. So Enigma's business tort claim fails.

Third, I agree with the majority that Enigma failed to plead tortious interference with a contract—although I would hold it failed to do so under both New York and California law. Enigma's claim fails under California law because it doesn't allege an "independently wrongful act," as discussed above. *See Ixchel Pharma, LLC v. Biogen, Inc*., 470 P.3d 571, 580 (Cal. 2020) ("We therefore hold that to state a claim for interference with an at-will contract by a third party, the plaintiff must allege that the defendant engaged in an independently wrongful act."). And the claim must be dismissed under New York law because Enigma hasn't alleged a breach of a specific contract. *See NBT Bancorp Inc. v. Fleet/Norstar Fin. Grp., Inc*., 664 N.E.2d 492, 495–96 (N.Y. 1996) (Absent wrongful means, there is no tort "[w]here there has been no breach of an existing contract[.]").

So, in sum, the lack of an actionable Lanham Act claim deprives Enigma of its other claims.

IV.

For all these reasons, we should have affirmed the district court's order. I respectfully dissent.