FIRST AMENDMENT — COMMERCIAL SPEECH — NINTH CIRCUIT HOLDS THAT CYBERSECURITY SCREENING DECISIONS ARE VERIFIABLY FALSE UNDER THE LANHAM ACT. — *Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 69 F.4th 665 (9th Cir. 2023).

What happens when nonhuman technologies speak? The First Amendment, no longer only a fundamentally democratic protection for political discourse,[1] now routinely recognizes that nonhuman entities like corporations may express protectable speech.[2] One justification is consumer protection: citizens must receive information from companies to make informed decisions.[3] A second justification is more radical: nonhuman entities have inherently protectable speech rights under the First Amendment.[4] In an age of ever-expanding protections for commercial speech, often the second wins out. However, this approach to the commercial speech doctrine is an uneasy fit in the context of technology platforms. In a recent case, the Ninth Circuit reawakened a discussion of the degree to which existing doctrine allows cybersecurity companies to "speak" through their screening determinations and the extent to which those decisions may be protected as value-based opinions under the First Amendment. In the short term, the decision adds complexity to the liability assessments of cybersecurity companies; more broadly, it points to the ways that courts engage in unusual First Amendment line-drawing in the context of new technologies.

Enigma Software Group and Malwarebytes, Inc., each provide competing computer security software products that filter unwanted programs from customers' computers. In 2016, Enigma sued a purportedly independent software review website affiliated with Malwarebytes for providing allegedly false information about Enigma in its product reviews.[5] Later that year, Malwarebytes reconfigured its filtering software to exclude Enigma products. As a result, Malwarebytes's program designated Enigma Software's products as "malicious," "threats," and "potentially unwanted programs" (PUPS), which caused customers of both companies to delete Enigma from their computers.[6] Enigma Software saw this as retaliation for alleging unfair trade practices in the earlier

---

[1] *See* Burson v. Freeman, 504 U.S. 191, 196 (1992) ("Whatever differences may exist about interpretations of the First Amendment, there is practically universal agreement that a major purpose of that Amendment was to protect the free discussion of governmental affairs." (quoting Mills v. Alabama, 384 U.S. 214, 218 (1966))).

[2] *See generally* Citizens United v. FEC, 558 U.S. 310 (2010); Burwell v. Hobby Lobby Stores, Inc., 573 U.S. 682 (2014).

[3] *Cf.* Newcal Indus., Inc. v. IKON Off. Sol., 513 F.3d 1038, 1053 (9th Cir. 2008) (holding that "puffery" does not qualify as false advertising because it does not induce consumer reliance).

[4] *See* Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 765 (1976).

[5] Enigma Software Grp. USA, LLC v. Malwarebytes Inc., 260 F. Supp. 3d 401, 404–05 (S.D.N.Y. 2017).

[6] Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 69 F.4th 665, 670 (9th Cir. 2023).

lawsuit.[7] Enigma brought suit against Malwarebytes in the U.S. District Court for the Southern District of New York for false advertising under section 43(a) of the Lanham Act,[8] as well as deceptive and unlawful business practices, tortious interference with contractual relations, and tortious interference with business relations under New York state law.[9] Malwarebytes successfully moved to transfer the case to the Northern District of California for lack of personal jurisdiction, and Malwarebytes renewed its motion to dismiss there.[10]

Malwarebytes first moved to dismiss all claims based on the safe harbor provision, § 230, of the Communications Decency Act.[11] Under that provision: "No provider or user of an interactive computer service shall be held liable on account of . . . any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be . . . otherwise objectionable."[12] The district court held that the immunity provision applied and granted Malwarebytes's motion to dismiss,[13] which Enigma appealed.[14] The Ninth Circuit reversed, holding that no safe harbor applied for content deemed "objectionable" for anticompetitive reasons.[15] The Supreme Court denied certiorari,[16] with Justice Thomas issuing a statement reflecting his dislike for the current interpretation of § 230's safe harbor provisions generally.[17]

On remand, the district court then addressed Malwarebytes's motion to dismiss for failure to state a claim under the Lanham Act's false advertising provision and New York law.[18] Under the Lanham Act, a claim constitutes false advertising if it (1) is a false statement of fact in a commercial advertisement; (2) deceives or has the tendency to deceive a substantial segment of the audience; (3) is material deception in that it affects the purchasing decision; (4) enters interstate commerce; and (5) causes or is likely to cause injury.[19] The court granted Malwarebytes's motion to dismiss, reasoning that the determination of whether products were "malicious," "threats," or PUPS was a statement of opinion because

---

[7] *Id.*

[8] 15 U.S.C. § 1125(a).

[9] Enigma Software Grp. USA LLC v. Malwarebytes Inc., No. 17-cv-02915, 2017 WL 5153698, at *1 (N.D. Cal. Nov. 7, 2017).

[10] *Malwarebytes*, 260 F. Supp. 3d at 412.

[11] *Malwarebytes*, 2017 WL 5153698, at *1–2 (citing 47 U.S.C. § 230(c)(2)).

[12] 47 U.S.C. § 230(c)(2)(A).

[13] *Malwarebytes*, 2017 WL 5153698, at *4.

[14] Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1045 (9th Cir. 2019).

[15] *Id.* at 1052.

[16] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 14 (2020) (mem.).

[17] *Id.* at 14–18 (Thomas, J., respecting the denial of certiorari). Justice Thomas argued that actionable torts (like defamation) by platforms should be analogized to the preexisting liability scheme for those exercising editorial control over defamation in print media. That system held publishers (who exercise significant editorial control) to the highest standard of liability and distributors (who exercise some, but limited, control) to a lower standard of liability. *See id.*

[18] *Malwarebytes*, 69 F.4th at 671–74.

[19] *Id.* at 671 (citing Southland Sod Farms v. Stover Seed Co., 108 F.3d 1134, 1139 (9th Cir. 1997)).

it was not "verifiably false," and thus not actionable as false advertising under the Act.[20] The district court also held that the other claims based on New York law failed because Malwarebytes was not subject to personal jurisdiction in New York.[21] The district court noted, however, that even if New York law had applied, designations of Enigma's software as threatening malware were also statements of opinion for the purposes of state law.[22] Enigma again appealed this holding to the Ninth Circuit, arguing that designating its software as malware constituted a verifiably false statement of fact.[23]

In an opinion authored by Judge Clifton, the Ninth Circuit reversed in part, affirmed in part, and remanded,[24] holding that in a cybersecurity context, determining whether a program represents a threat constitutes a factual assertion at the motion to dismiss stage.[25] The court defined a factual assertion as one that is "literally false, either on its face or by necessary implication, or that the statement was literally true but likely to mislead or confuse consumers."[26] In holding that "malicious" and "threatening" could be used as verifiably false adjectives, the court explicitly considered the context of the statements.[27] Because Malwarebytes produced an antimalware program, its determinations of what constitutes maliciousness carried a context of verifiability. The court further considered "malware" to be an objective categorization in this context, writing: "[W]hether 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."[28] As such, "malware" is generally an objective categorization, but it is especially so in this context because of Malwarebytes's supposed expertise.

The majority then interrogated the meaning of "malware," arguing that this categorization was not, as the dissent argued, a "spectrum" but one of objective fact.[29] It did acknowledge, however, that "potentially unwanted programs" could only be a statement of opinion.[30] The majority cited the dictionary definition of malware as software "written with the intent of being disruptive or damaging to (the user of) a computer or other electronic device; viruses, worms, spyware, etc.,

---

[20] Enigma Software Grp. USA LLC v. Malwarebytes Inc., No. 17-cv-02915, 2021 WL 3493764, at *9 (N.D. Cal. Aug. 9, 2021).

[21] *Id.* at *8–9.

[22] *Malwarebytes*, 69 F.4th at 670.

[23] *Id.* at 671.

[24] *Id.* at 669.

[25] *See id.* at 672.

[26] *Id.* at 671 (citing Southland Sod Farms v. Stover Seed Co., 108 F.3d 1134, 1139 (9th Cir. 1997)).

[27] *See id.* at 672.

[28] *Id.*

[29] *Id.*

[30] *Id.*

collectively."[31] Thus, the majority argued, determining whether a program is a "virus[], spyware, adware, ransomware [or] Trojan[]" is a claim that "lends itself to verification," and can be "reduced to 'a binary determination' based on 'falsifiable criteria.'"[32] The majority dismissed the dissent's concern that the claim was not verifiable because "at bottom . . . the term necessarily implies that someone created software with the intent to gain unauthorized access to a computer for some nefarious purpose."[33] The majority also claimed limited expertise — writing that "judges are not experts in the cybersecurity field."[34] As such, the majority posited that Enigma's allegation that the term has a stable meaning in the field should not be held implausible at the motion to dismiss stage.

The majority eschewed any First Amendment concerns, including those raised by the dissent. It noted that commercial speech generally retains less protection under the First Amendment than other types of speech, but it does have limited protection.[35] That protection, however, does not extend to "commercial messages that do not accurately inform the public."[36] In holding that malware classification can constitute such an inaccurate message, the majority analogized to a case involving a supplement manufacturer's review system for nutritional supplements.[37] The system included a "five-star" rating system, which was based on objective criteria, and "Medals of Achievement," which were based on meeting two conditions.[38] The five-star rating system was a subjective statement of opinion, despite its roots in objective criteria, while the medal was held to be an assertion of fact.[39] Similarly, the court saw Malwarebytes as creating a system by which to evaluate software, including that of competitors.[40] However, its designation of "malware" was more like the Medal of Achievement, which was based on two falsifiable criteria, rather than the five-star rating system, which involved subjective assignment of values.[41]

Regarding the personal jurisdiction claims, the majority again reversed the district court's decision, holding that Malwarebytes was subject to personal jurisdiction in New York under the applicable long-arm

---

[31] *Id.* (quoting *Malware*, OXFORD ENG. DICTIONARY (2022), https://www.oed.com/dictionary/malware_n?tab=meaning_and_use [https://perma.cc/U57F-N6RV]).

[32] *Id.* at 672–73 (quoting Second Amended Complaint ¶ 2, Enigma Software Grp. USA LLC v. Malwarebytes Inc., No. 17-cv-02915 (N.D. Cal. Nov. 7, 2017); Ariix, LLC v. NutriSearch Corp., 985 F.3d 1107, 1122 (9th Cir. 2021)).

[33] *Id.*

[34] *Id.* at 673.

[35] *Id.*; *see also* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 566 (1980).

[36] *Malwarebytes*, 69 F.4th at 673 (quoting *id.* at 681 (Bumatay, J., dissenting)).

[37] *See Ariix*, 985 F.3d at 1107.

[38] *Id.* at 1111; *see also Malwarebytes,* 69 F.4th at 673.

[39] *Ariix*, 985 F.3d at 1121–22.

[40] *Malwarebytes*, 69 F.4th at 674.

[41] *Id.* at 673–74.

statute because it "transact[s] business" within the state.[42] The majority then reversed the dismissal of all but one of the state law unfair competition claims under the same logic it applied to the Lanham Act claims. For the claim of tortious interference with contractual relations, the majority held that Enigma failed to plead the required elements.[43] In a brief concurrence, Judge Baker clarified that the majority assumed that New York substantive law governed the claims, an issue that neither party raised.[44]

Judge Bumatay dissented, raising First Amendment objections. He argued that because decisions about what constitutes malware reflect subjective value judgments, they are opinions subject to constitutional protection.[45] Further, the cybersecurity context did nothing to change the categorization's fundamental status as an opinion.[46] Noting that the court should "err on the side of nonactionability"[47] in the case of speech, Judge Bumatay cautioned against empowering the Lanham Act to encompass protected opinions and against creating precedent that second-guesses cybersecurity companies' threat determinations.[48] Defining malware, according to Judge Bumatay, reflects individual judgment rather than application of a term of art. Judge Bumatay looked to the criteria Malwarebytes built to determine whether a program was "potentially unwanted," "malicious," or a "threat" to demonstrate that each of these determinations had no dispositive criteria. Instead, they "refer to a spectrum of digital features with no verifiable line to cross to determine when they apply."[49] Most importantly, Enigma never alleged that Malwarebytes actually labeled the software as "malware."[50]

Furthermore, Judge Bumatay pointed out that the majority's definition of malware betrayed its subjectivity by including "adware" as an example.[51] Adware, he pointed out, comes bundled with free software and often helps serve users with more relevant ads after they consent — a purpose which is not always "nefarious."[52] In sum, Judge Bumatay saw the malware label as a subjective determination involving judgment calls, likening the majority opinion to calling "green is the best color" a factual statement — because it can be verified that it is the "best."[53] He did not reach the personal jurisdiction questions because he agreed with the district court that, even if jurisdiction was appropriate, the

---

[42] *Id.* at 675–76.
[43] *Id.* at 678.
[44] *Id.* at 678–79 (Baker, J., concurring).
[45] *Id.* at 679 (Bumatay, J., dissenting).
[46] *Id.*
[47] *Id.* at 682. (quoting Partington v. Bugliosi, 56 F.3d 1147, 1159 (9th Cir. 1995)).
[48] *See id.* at 679.
[49] *Id.* at 683.
[50] *Id.* at 686.
[51] *Id.* at 687.
[52] *Id.*
[53] *Id.*

failure of the Lanham Act claims meant that the state law claims would also fail.[54]

The majority and the dissent ultimately split over whether a cybersecurity program's screening determinations constituted regulable facts or nonactionable opinions. Both Judges Clifton and Bumatay had to decide how to apply a doctrine covering actions of corporations and advertisers to digital services exercising quasi-editorial discretion.[55] In an era where corporate speech regulation appears to be enveloped in growing First Amendment absolutism,[56] the panel opinion of *Malwarebytes* shows that some judges may be more cautious about growing speech protections in the context of new technologies. The *Malwarebytes* majority was willing to engage in First Amendment line-drawing and limitation when the corporate speech was in the context of technology companies, while the dissent remained consistent with First Amendment expansionist logic. In the short term, the court's decision is important because it indicates that there could be increased liability in cybersecurity screening decisions; more broadly, the split indicates that new technologies are an area where doctrinal patterns like First Amendment expansionism are subject to reconsideration.

Commercial speech is sometimes defined as "speech that does 'no more than propose a commercial transaction,'"[57] and most paradigmatically applies in cases of commercial advertising.[58] Historically, commercial speech was understood to be beneath the First Amendment, the aim of which was political discourse.[59] That changed, however, in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*,[60] where the Court held that commercial speech had limited protection under the First Amendment and held it to a quasi–intermediate scrutiny standard of review.[61] Within commercial advertising, speech

---

[54] *Id.* at 688.

[55] *See id.* at 673 (majority opinion).

[56] *Compare* Genevieve Lakier, *Imagining an Antisubordinating First Amendment*, 118 COLUM. L. REV. 2117, 2118 (2018) (discussing the shift in First Amendment jurisprudence to protect powerful over marginalized actors), *and* Genevieve Lakier, *The First Amendment's Real* Lochner *Problem*, 87 U. CHI. L. REV. 1241, 1245 (2020) (discussing the implications of a free speech doctrine focused unilaterally on prohibiting government interference, rather than affirmative guarantees), *with* Zachary S. Price, *Our Imperiled Absolutist First Amendment*, 20 U. PA. J. CONST. L. 817, 819–20 (2018) (arguing that contemporary challenges may pressure the unusually expansive protections offered by the First Amendment).

[57] Friedman v. Rogers, 440 U.S. 1, 10 n.9 (1979) (quoting Pittsburgh Press Co. v. Pittsburgh Comm'n on Hum. Rels., 413 U.S. 376, 385 (1973)).

[58] *See* Lakier, *The First Amendment's Real* Lochner *Problem*, *supra* note 56, at 1260.

[59] *See* Valentine v. Chrestensen, 316 U.S. 52, 55 (1942).

[60] 447 U.S. 557 (1980).

[61] *Id.* at 566. The Court developed a four-part test that approximates a form of intermediate scrutiny:

> At the outset, we must determine whether the expression is protected by the First Amendment. For commercial speech to come within that provision, it at least must concern lawful

helping customers to make informed decisions could not be regulated, while false or misleading commercial speech firmly fell outside the purview of the First Amendment.[62] In the context of the Lanham Act, this means that regulation of false advertising is permissible because it prevents consumers from being misled by false statements of fact.[63] Opinion-based commercial speech amounts to "puffery," and should be protected by default because it does not interfere with consumer decisionmaking.[64]

Increasingly, however, the consumer protection rationale has competed with a second one, that corporations have inherent speech rights, separating the idea of speech from that of a human speaker.[65] Professors Nathan Cortez and William Sage describe this phenomenon as the "disembodied First Amendment,"[66] which removes First Amendment jurisprudence from its traditional realms of political and religious regulation to speech that is disconnected from the idea of a traditional "speaker."[67] This expansion of the commercial speech doctrine is not cost free. Because information is deeply tied with other activity in the contemporary world, protecting corporate speech can bleed into regulations of economic activity or antidiscrimination law.[68] Indeed, in the most recent Term, the Supreme Court held that the First Amendment right to speak allowed a website designer to discriminate against same-sex couples.[69] The legal troubles of overbroad commercial-speech protections apply in other areas, too. If health and safety regulations, which are often considered regulations on commercial speech, are held to a standard of strict scrutiny, regulatory regimes that consumers depend on for safety could fall.[70]

> activity and not be misleading. Next, we ask whether the asserted governmental interest is substantial. If both inquiries yield positive answers, we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest.

Id.

[62] *Id.* at 561, 593; *see also* Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 765 (1976).

[63] *See Malwarebytes*, 69 F.4th at 672 (citing Newcal Indus. v. IKON Off. Sol., 513 F.3d 1038, 1053 (9th Cir. 2008)).

[64] *See id.*

[65] *See* Nathan Cortez & William Sage, *The Disembodied First Amendment*, 100 WASH. U. L. REV. 707, 709 (2023).

[66] *Id.* at 750.

[67] *Id.* at 709.

[68] *See generally* Helen Norton, *Discrimination, The Speech that Enables It, and the First Amendment*, 2020 U. CHI. LEGAL F. 209 (discussing the ways that listener-centric commercial speech doctrine enables antidiscrimination law to coexist with the First Amendment).

[69] 303 Creative LLC v. Elenis, 143 S. Ct. 2298, 2316, 2322 (2023). Professor Frederick Schauer has asserted that even purely in the realm of commercial advertising, reaching parity for regulations of commercial and noncommercial speech could be "troublesome." *See* Frederick Schauer, *Commercial Speech and the Perils of Parity*, 25 WM. & MARY BILL RTS. J. 965, 978 (2017).

[70] Schauer, *supra* note 69, at 978.

New technologies, like that of Malwarebytes, may test the limits of doctrinal expansion in the case of disembodied commercial speech. At the extreme end of doctrinal expansion is the risk that a sophisticated artificial intelligence (AI) chatbot may be protected by the First Amendment.[71] The argument that such protection is imminent is that because corporate speech protections no longer require that there be a human speaker, technological innovations that substitute "speech" without humanity are not clearly unprotectable.[72] With "skis waxed for a quick descent down the slippery slope," proponents of robot speech draw a direct line from the fact that automated communications like robocalls implicate the First Amendment to protection of robot speech.[73] While the screening technology in *Malwarebytes* is nowhere near the sophistication of an AI chatbot, it inches slightly closer than an automated robocall.

The reasoning in the *Malwarebytes* dissent risks inviting this slippery slope logic. Judge Bumatay's opinion centered on the First Amendment implications of censoring value-based corporate statements.[74] This logic is consistent with the movement toward broader expansion of the commercial speech doctrine: that corporate statements must have inherent First Amendment protection. In other words, Judge Bumatay edges closer to disembodiment: when a service makes moderation decisions, its speech should be protected. In his model, the speech is still an opinion, but he finds the idea of protected quasi-factual speech unproblematic. Furthermore, once First Amendment analysis begins on commercial speech, the doctrinal thrust makes it difficult to censor.[75]

Whether a statement is verifiably false then becomes an important threshold question in the march toward disembodiment. The consumer protection rationale does not subject false commercial statements to First Amendment analysis, at least for now. As expressive rights inch further away from traditional speakers, so declines the truth/falsity distinction of a consumer protection rationale. Professor Frederick Schauer has asked why, if the goal is to bring commercial speech into parity with noncommercial speech, truth or falsity should make any difference —

---

[71] Toni M. Massaro, Helen Norton & Margot E. Kaminski, *SIRI-OUSLY 2.0: What Artificial Intelligence Reveals About the First Amendment*, 101 MINN. L. REV. 2481, 2482 (2017) (arguing that First Amendment expansion has unnecessarily prioritized "constraining the government" and whether speech "provid[es] value to listeners").

[72] Cortez & Sage, *supra* note 65, at 710.

[73] *Id.* at 723, 726 (citing Barr v. Am. Ass'n of Pol. Consultants, 140 S. Ct. 2335, 2346–47 (2020)).

[74] *Malwarebytes*, 69 F.4th at 681 (Bumatay, J., dissenting) ("When it comes to the regulation of any speech, we should always begin with the First Amendment.").

[75] *See id.* at 682 ("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.'" (quoting Partington v. Bugliosi, 56 F.3d 1147, 1159 (9th Cir. 1995))).

an everyday person's lies are clearly protectable speech.[76] Enforcing the truth/falsity distinction is therefore critical to maintaining the boundary between human versus nonhuman speech, and emphasizing it shores up the eroding line between the two. Such erosion has implications that courts have not fully considered as they expand commercial speech protections.

The Ninth Circuit's split in *Malwarebytes* reveals judges grappling with the not-yet-considered implications of commercial and noncommercial speech parity in the context of new technologies.[77] The emphasis on falsity places the analysis firmly *outside* the realm of First Amendment analysis, avoiding the dissent's logic and therefore its necessary conclusion. The dissent is willing to conduct the First Amendment analysis without questioning that such analyses under the current doctrinal structure generally fall in favor of protection. However, the majority opinion has worrisome implications of its own. In the short term, the majority's insistence that the First Amendment does not apply to malware classifications creates an ill-fitting standard — one in which cybersecurity screening determinations are subject to liability as factual statements.

Judge Clifton's opinion creates the potential for problematic interpretations rooted in labeling cyberthreat determinations as verifiably false. The opinion reaches this conclusion by insisting that the total context of Malwarebytes's professional expertise should be dispositive in rendering its decisions factual.[78] While expertise is certainly relevant to sorting factual from opinion-based claims, holding that borderline threat determinations risk liability could pose security risks if companies like Malwarebytes take a risk-averse approach when programming their software to protect users from legitimate threats. Notably, defamation also requires a showing of falsity,[79] which could lead to increased liability beyond false advertising for cybersecurity companies. Rather than embracing the inherent subjectivity of certain screening determinations, Malwarebytes must now make the determination of what constitutes appropriate screening internally.

Further, the majority's analysis betrays a desire to abdicate responsibility for making speech determinations within the technology sphere. Judge Clifton wrote that evaluating cybersecurity decisions pushes the limits of judicial expertise,[80] shifting the burden of expertise onto the commercial entity. In this way, the cybersecurity company must take on a quasi-professional responsibility, where it alone is responsible for

---

[76] Schauer, *supra* note 69, at 975–77 (citing Ocala Star-Banner Co. v. Damron, 401 U.S. 295, 300–01 (1971)).

[77] Schauer argues that one potential outcome is parity between human and corporate speech through the dilution of human speech rights. *Id.* at 978.

[78] *Malwarebytes*, 69 F.4th at 672.

[79] *See* Masson v. New Yorker Mag., Inc., 501 U.S. 496, 499 (1991).

[80] *Malwarebytes*, 69 F.4th at 673.

determining what could constitute an "objective threat" within its sphere. Yet, as Judge Bumatay pointed out in dissent, even including "adware" in the supposed list of malicious programs betrays an individualized value judgment.[81] Emphasizing the truth/falsity distinction allows this shifting of responsibility in the short term, though ongoing judicial abdication to answering these questions will not likely be possible as cases continue to arise.

One explanation for the majority opinion's attachment to the truth/falsity distinction despite this problematic result is that treating the value judgments of new technologies as speech inches the reasoning closer to protecting bot speech and other sophisticated artificial intelligence generations with no clear limiting principle. In cases involving new technology, even rudimentary ones like the software at issue here, the implications of pure parity for commercial and noncommercial speech may be more visible. Adjudicators may be unwilling, as Judge Bumatay desires, to continue the unfettered expansion of commercial speech doctrine in such a context. When technology was at issue, the *Malwarebytes* majority resisted doctrinal trends, and chose to limit the protectability of commercial speech while creating a difficult standard for cybersecurity companies exercising discretion going forward.

Malwarebytes thus reveals some judges' willingness to engage in First Amendment line-drawing in the context of new technologies. In doing so, the case continues its ongoing history as one that defies convention. Perhaps the decision reveals no more than an ill-fitting doctrine for a newly styled problem: one company cannot be allowed to filter the products of its competitors. Regardless, in holding that there is potential for false advertising liability in making cyberthreat assessments, the *Malwarebytes* majority bucked ongoing trends in the commercial speech doctrine and revealed how new technology presents challenges that may shape the doctrine's ongoing evolution.

---

[81] *Id.* at 687 (Bumatay, J., dissenting); *see also What Is Adware?*, MICROSOFT (Aug. 3, 2023), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-adware [https://perma.cc/JKE9-DNBX].