

Potential Lanham Act Reverberations: “Malicious” and “Threat” Are Statements of Fact, Not Opinion

JUNE 22, 2023

On June 2, 2023, the Ninth Circuit overturned a district court’s dismissal of a false advertising claim brought by Enigma Software Group USA LLC (Enigma) under Section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a)(1)(B) (the Lanham Act).¹ Enigma’s allegations against a competitor in the computer security space, Malwarebytes, Inc. (Malwarebytes), concern Malwarebytes’ designation of Enigma’s programs as “malicious” and a “threat.” After the district court found that such terms were “non-actionable statements of opinion” under the Lanham Act, the Ninth Circuit reversed and held that they were actionable statements of fact. As the dissent warned, this ruling sends a “chilling message to cybersecurity companies” that classify programs as malware.² And outside this context, this decision may have broader implications for the scope and definition of provable statements of fact under the Lanham Act.

In the Ninth Circuit, a plaintiff bringing a false advertising claim must, among other factors, allege that the defendant made a false statement of fact in a commercial advertisement.³ An actionable statement of fact must be “specific and measurable,” and “capable of being proved false or of being reasonably interpreted as a statement of objective fact.”⁴ In finding that the terms “malicious” and “threat” met the standard for an actionable statement of fact, the court explained that the terms were “substantively meaningful and verifiable in the cybersecurity context” and “make[] a claim as to the specific or absolute characteristics of a product.”⁵ In doing so, the court acknowledged that the terms “admit of numerous interpretations,” but argued that the context in which the words appear is “paramount.”⁶ For example, Malwarebytes’ anti-malware program labeling Enigma’s software as “malicious” and a “threat” would reasonably be interpreted by Malwarebytes’ customers as the identification of malware, and “whether software qualifies as malware is largely a question of objective fact.”⁷ The dissent argued that these terms, even in the commercial context, were protected as “subjective expressions of opinion.”⁸

This ruling is likely to have substantial implications for cybersecurity companies. As the dissent warns, “civil liability may now attach if a court later disagrees with your classification of a program as ‘malware.’”⁹ Eric Goldman, associate dean and professor at Santa Clara University School of Law, says the decision invites competitors to “use litigation as a weapon to try and force anti-threat vendors to change their classifications or scare them from making a negative classification in the first instance, just by virtue of the litigation costs.” Previously, a cybersecurity company’s flagging of computer software as “malicious” or a “threat” would likely have been considered a statement of opinion protected under the Lanham Act. However, following this decision, cybersecurity companies will need to

carefully weigh any decision to label software, even by implication, as malware.^[1] While a plaintiff must still ultimately prove that the malware label is false, that is a question for the jury, and the *Enigma Software* ruling that such a label is a statement of fact will enable more complaints to survive a motion to dismiss.

Outside the cybersecurity context, it remains to be seen whether this case will lead to an expanded definition of an actionable statement of fact under the Lanham Act. While the majority’s decision seems limited to the use of malware terminology against a competitor, its explanation as to why the terms “malicious” and “threat” are statements of fact hints at a wider application: malware “lends itself to verification” and “can come in many forms,” and whether something qualifies as malware “can be reduced to a binary determination based on falsifiable criteria.”^[2] Needless to say, labels commonly used in other commercial industries frequently fit that definition, and it will be interesting to see whether this case is cited against non-cybersecurity firms as well.

^[1] *Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.*, 2023 WL 3769331 (9th Cir. 2023).

^[2] *Enigma Software*, 2023 WL 3769331, at *27 (9th Cir. 2023).

^[3] *Southland Sod Farms v. Stover Seed Co.*, 108 F.3d 1134, 1139 (9th Cir. 1997). The other elements of a false advertising claim are that the statement deceived or had a tendency to deceive a substantial segment of its audience; the deception was material, in that it was likely to influence the purchasing decision; the false statement entered interstate commerce; and plaintiff has been or is likely to be injured as a result of the false statement. *Id.*

^[4] *Coastal Abstract Serv., Inc. v. First Am. Title Ins. Co.*, 173 F.3d 725, 731 (9th Cir. 1999).

^[5] *Enigma Software*, 2023 WL 3769331, at *12 (9th Cir. 2023).

^[6] *Id.* Judge Bumatay dissented, finding the terms cannot be proven false as they have an “inherently subjective element.” *Id.* at *36.

^[7] *Id.* at *12–13.

^[8] *Id.* at *27.

^[9] *Id.*

^[10] Of particular note, Malwarebytes never actually used the term “malware” to describe Enigma’s products. *Enigma Software*, 2023 WL 3769331, at *42–43 (9th Cir. 2023).

^[11] *Id.* at *14.

3 Min Read

Authors

[Susannah Torpey](#)

[Brandon Annette](#)

Related Locations

[Los Angeles](#)

[New York](#)

Related Topics

[False & Deceptive Advertising](#)

[Lanham Act](#)

[Technology Antitrust](#)

Related Capabilities

Antitrust/Competition

Advertising Litigation

Privacy & Data Security

Technology, Media & Telecommunications

Related Regions

North America

Related Professionals



[Susannah Torpey](#)



[Brandon Annette](#)

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.