

Northern District of California: Denies Dismissal Concerning Tech Company's Claim That It Offered End-to-End Encryption (Securities Law Alert)

03.31.22



(Article from *Securities Law Alert*, March 2022)

For more information, please visit the [Securities Law Alert Resource Center](#)

On February 16, 2022, the Northern District of California dismissed claims in a securities fraud class action against a tech company and its CEO based on 14 alleged false and misleading statements and omissions regarding the company's operations and its collection and use of users' personal data. *In re Zoom Sec. Litig.*, 2022 WL 484974 (N.D. Cal. 2022) (Donato, J.). However, the court denied dismissal regarding defendants' statement that the company offered end-to-end encryption. As to this statement, the court determined that plaintiff satisfied the falsity element by alleging that defendants represented that the company offered "end-to-end encryption" when it did not.

The statement at issue appeared in the company's April 2019 Registration Statement and Prospectus, which stated, "We offer robust security capabilities, including end-to-end encryption[.]" Plaintiff claimed this statement violated Section 10(b) by making false and misleading statements and omissions concerning the ability to use end-to-end encryption in the company's main product offering.

Determining that plaintiff satisfied the falsity element for this statement, the court pointed to plaintiff's allegation that "end-to-end encryption means that not even the company that runs the messaging service can access the cryptographic keys necessary to decrypt the end users' communication," while the company "secretly maintained access to the cryptographic keys that could allow [it] to decrypt and decipher the communications between the end users."

Defendants argued that plaintiff's falsity allegations were insufficient because the term "end-to-end encryption" can have different meanings. The court, however, rejected this argument, explaining that defendants' own statements, as alleged in the complaint, demonstrated otherwise. In a company blog post, the CEO stated that, "we recognize that we have fallen short of the community's -- and our own -- privacy and security expectations." The CEO's post also referred and linked to a post by the company's Chief Product Officer stating "we want to start by apologizing for the confusion we have caused by incorrectly suggesting that [our] meetings were capable of using end-to-end encryption. While we never intended to deceive any of our customers, we recognize that there is a discrepancy between the commonly accepted definition of end-to-end encryption and how we were using it."

The court observed that plaintiff's allegations distinguish this case from *Wochos v. Tesla*, 985 F.3d 1180 (9th Cir. 2021).^[1] In *Wochos*, the Ninth Circuit found that plaintiffs pleaded no facts to support their premise that the term "production car" had the distinctive and false

meaning that plaintiffs claimed it did. By contrast, the court stated that here plaintiff identified defendants’ “express acknowledgement” that they had “incorrectly suggested” their product was capable of using end-to-end encryption, and they had used the term end-to-end encryption “differently from the commonly accepted definition.”

[1] Please [click here](#) to read our discussion of the Ninth Circuit’s decision in *Wochos v. Tesla*.

Authors and
Contacts

Lynn Neuner
Partner
lneuner@stblaw.com
[+1-212-455-2696](tel:+12124552696)

Janet Gochman
Senior Counsel
jgochman@stblaw.com
[+1-212-455-2815](tel:+12124552815)

Jonathan Youngwood
Partner
jyoungwood@stblaw.com
[1-212-455-3539](tel:12124553539)

