Shumaker

MAY 27, 2026 | PUBLICATION

Client Alert: Texas v. Meta and WhatsApp: A New Front in the Battle Over Encryption, Privacy Marketing, and Consumer Protection

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

C. Jade Davis

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

On May 21, 2026, the Texas Attorney General filed suit against Meta Platforms, Inc. (Meta) and WhatsApp, LLC (WhatsApp) in the 71st Judicial District Court of Harrison County. The complaint, brought under the Texas Deceptive Trade Practices, Consumer Protection Act (DTPA), Tex. Bus. & Com. Code Ann. § 17.41 et seq., alleges that Meta and WhatsApp engaged in false, misleading, and deceptive acts and practices by representing to consumers that WhatsApp communications were fully private and inaccessible, even to WhatsApp and Meta, when, in fact, the defendants allegedly could access plaintext communications in at least some circumstances.

The Core Allegation: A Gap Between Promise and Practice

WhatsApp's marketing has long been emphatic: "Your privacy is our priority. With end-to-end encryption on WhatsApp, your personal messages, photos, calls and more stay between you and the people you choose, meaning not even WhatsApp can see them." Meta CEO Mark Zuckerberg reinforced this claim in sworn testimony before the United States Senate, asserting that "we do not see any of the content in WhatsApp, it's fully encrypted . . . . Facebook systems do not see the content of messages being transferred over WhatsApp." Every WhatsApp chat features a banner at the top of the screen reinforcing the message that

conversations are end-to-end encrypted.

However, the petition alleges that these assurances are false. Citing a special agent for the Office of Export Enforcement within the Commerce Department's Bureau of Industry and Security, the complaint reports that the agent examined claims that Meta employees and contractors had the capability to view WhatsApp message content and concluded those claims were meritorious. According to reporting referenced in the petition, "Meta stores and can view WhatsApp messages" and "Meta can and does view and store all the text messages, photographs, audio, and video recordings" in an "unencrypted format." The complaint further alleges that Meta maintains a tiered permissions system allowing different employees and contractors—including a "significant number of foreign/overseas workers in India"—varying levels of access to WhatsApp content, including for content moderation work. The special agent's investigation was reportedly based in part on a November 2024 whistleblower complaint to the Securities and Exchange Commission (SEC).

The Deceptive Trade Practices Act Theory: A Different Angle

While there is a long history of enforcement actions involving Meta and WhatsApp, from the Federal Trade Commission's (FTC) $5 billion fine for privacy violations to multiple General Data Protection Regulation (GDPR) penalties totaling billions of euros imposed by the Irish Data Protection Commission, Texas' approach here takes a somewhat different angle. Historically, regulatory scrutiny around WhatsApp has focused more on transparency, consent, metadata sharing, and broader privacy governance issues rather than alleged inconsistencies between marketing representations and actual technical access practices.

The DTPA cause of action charges defendants with three categories of violations: (a) representing that they were unable to and would not access WhatsApp users' communications when, in fact, they could and did, in violation of § 17.46(b)(5); (b) representing that their services have characteristics, uses, or benefits they do not have by claiming that personal messages "stay between you and who you send them to—no one else, not even WhatsApp (or Meta), can read, listen to, or share them," also in violation of § 17.46(b)(5); and (c) failing to disclose information known at the time with the intent to induce users into utilizing defendants' services, in violation of § 17.46(b)(24).

The State seeks a permanent injunction enjoining Meta and WhatsApp from accessing the content of any Texan's WhatsApp communications absent consent, civil penalties of $10,000 per DTPA violation, attorneys' fees, costs, and other relief.

The Encryption Question: Signal Protocol, Source Code, and the Backdoor Problem

A critical technical dimension underlies the legal claims. WhatsApp integrated the Signal Protocol—the same end-to-end encryption protocol used by the Signal messaging application—across its platform by April 2016. In theory, end-to-end encryption means that data is encrypted on the sender's device and only decrypted on the recipient's device, rendering the contents unreadable to the service provider even as communications transit its servers.

However, the petition draws an important distinction: while Signal makes its source code publicly available for inspection and independent review—and those reviews have confirmed the absence of any backdoor—WhatsApp does not make its source code available to the public or even to third-party security auditors. Accordingly, the public "can only take the word of Meta and WhatsApp" that their implementation of the Signal Protocol does not include a kleptographic backdoor enabling Meta or third parties to circumvent encryption. The petition also highlights a distinction often lost on consumers: while the Signal Protocol encrypts the contents of communications, metadata (the who, when, and where of any exchange) is

not encrypted and remains fully accessible to Meta and WhatsApp.

Meta's Track Record: A Pattern of Privacy Violations and Misleading Conduct

A substantial portion of the petition details Meta's extensive history of privacy violations and misleading conduct, which the State offers to establish a pattern of behavior. The complaint recounts the 2012 FTC consent order settling allegations that Facebook "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing [that information] to be shared and made public." It recounts the 2019 historic $5 billion FTC penalty for violations of that consent order, a fine so large it was "almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide," and yet one that barely moved Meta's stock price—in fact, Zuckerberg's shares increased in value by more than $1 billion in just 30 minutes following the announcement.

The petition further catalogs GDPR fines totaling billions of euros, including the largest GDPR fine ever imposed, €1.2 billion for illegal transfers of European users' personal data to the United States, as well as a €91 million fine for storing user passwords in plain text without encryption. Meta was also fined by the European Commission for providing "incorrect or misleading information" about the technical feasibility of integrating Facebook and WhatsApp user accounts during the merger review process—when in fact that technical capability already existed. The complaint notes that Meta has recently laid off more than 100 employees in its risk review organization, the unit responsible for ensuring compliance with the FTC consent order and privacy requirements worldwide.

Implications Down the Road

If this case moves forward and particularly if Texas succeeds, the implications could be substantial across several dimensions.

Defining "End-to-End Encryption" as a Legal Concept

Perhaps the most consequential outcome of this litigation would be forcing courts to address what "end-to-end encryption" legally means. The petition highlights the gap between the theoretical promise of end-to-end encryption—that data is encrypted on the sender's device and only decrypted on the recipient's—and the alleged operational reality at Meta, where employees and contractors could access plaintext communications through a tiered permissions system. A ruling that "end-to-end encryption" carries a specific, enforceable meaning in consumer protection law would have ripple effects far beyond WhatsApp. Every company marketing encrypted communications would need to assess whether their implementation matches whatever legal standard emerges.

Whether Metadata Access Undermines Privacy Claims

The petition acknowledges that the Signal Protocol encrypts only message contents, not metadata, and that Meta and WhatsApp can identify the parties, timing, location, and frequency of communications. The question of whether access to rich metadata effectively undermines categorical claims of privacy—even if content encryption is technically intact—could push courts toward a more holistic definition of communication privacy, one that considers what can be inferred from metadata alone, not merely whether message text is readable.

How Much Technical Nuance Companies Must Disclose

The complaint identifies several limited exceptions that WhatsApp does disclose, such as receiving the last

five messages when a user reports abuse, or business messaging services that are not end-to-end encrypted, but argues that these limited disclosures do not come close to revealing the full extent of Meta's access. This raises a broader question about the level of technical detail companies must provide to avoid deceptive-practices liability. Courts may need to decide whether omitting discussion of tiered access systems, backup workflows, content moderation access, and cloud application programming interface (API) exceptions constitute actionable nondisclosure, particularly when a company's marketing uses categorical, absolute language like "not even WhatsApp."

Whether Consumer Expectations Override Engineering Definitions

WhatsApp's marketing arguably creates a consumer expectation that no one, including WhatsApp itself, can read private messages. If Meta defends on the basis that its engineering implementation complies with a narrow technical definition of end-to-end encryption, courts may be called upon to decide whether the reasonable consumer's understanding of these representations governs—not the engineer's. The DTPA framework, which focuses on the impact of representations on consumers rather than the technical accuracy of the underlying engineering, may favor the consumer-expectation approach.

Pressure on Corporate Marketing and Disclosure Practices

This case will likely create significant pressure for companies across the technology sector to narrow their marketing language, add more caveats to privacy representations, clarify backup and access workflows, and more carefully distinguish between encrypted transport, encrypted storage, metadata visibility, and operational access exceptions. The categorical nature of WhatsApp's claim that "not even WhatsApp can see them" left little room for nuance. Companies that market privacy features would be well-advised to evaluate whether their representations could withstand scrutiny under a DTPA-type analysis, particularly if their systems include any access pathway, however limited, that is inconsistent with the absolute assurances conveyed in their marketing.

The Open-Source Transparency Factor

The petition's contrast between Signal's open-source, publicly auditable code and WhatsApp's proprietary, closed-source implementation introduces a potentially important variable. If courts or regulators begin treating open-source transparency as a benchmark for validating encryption claims, companies that use proprietary implementations may face heightened scrutiny or a practical incentive to submit to independent third-party audits when marketing their products as "encrypted."

The Deterrence Problem

The petition's detailed recitation of Meta's prior fines underscores a persistent challenge: even unprecedented financial penalties have failed to deter Meta's conduct. The State's request for injunctive relief; specifically, an order enjoining Meta and WhatsApp from accessing the content of any Texan's WhatsApp communications absent consent, represents an attempt to move beyond monetary penalties and impose structural, behavioral remedies. Whether a state court can effectively impose and enforce such technical requirements on a global platform remains an open question, but the attempt signifies a shift in enforcement strategy from fines that function as a cost of doing business to operational constraints that could fundamentally alter how a platform works.

Why This Case Matters

For our Technology, Data Privacy, Cybersecurity & AI Service Line, this lawsuit is especially notable as it

represents the convergence of cybersecurity architecture, consumer protection law, and marketing representations. The questions at the heart of this case—how encryption is implemented, whether access exceptions are adequately disclosed, and whether marketing language matches technical reality—are precisely the issues that we regularly navigate with clients. This case should prompt every organization that markets privacy or encryption features to conduct a careful review of its public-facing statements, its technical architecture, its internal access controls, and the alignment (or misalignment) between them.

With questions or for more information, please contact Jade Davis or a member of our Technology, Data Privacy, Cybersecurity &AI team.

Shumaker