

# Telephone and Texting Compliance News: Litigation Update — A Win for TCPA Compliance and the Lead Generation Industry

Article By:

Joshua Briones

Esteban Morales

Grecia A. Rivas

---

The Telephone Consumer Protection Act (TCPA) can be a difficult and complex area of law to litigate. In recent years, the plaintiffs' bar has upped that difficulty and complexity by targeting products designed to help with TCPA compliance — namely, products designed to confirm whether consumers provided TCPA-compliant consent. One such product is TCPA Guardian offered by Jornaya. In *Williams v. DDR Media, LLC, et al.*, No. 22-cv-03789-SI, 2024 US Dist. LEXIS 211342 (ND Cal. Nov. 20, 2024), Jornaya fell into the crosshairs of a California Invasion of Privacy Act (CIPA) suit alleging that the use of TCPA Guardian violated the statute because it constituted “unauthorized . . . read[ing]” of a communication under the California Penal Code § 631(a). In a noteworthy decision for the lead generation space, the US District Court for the Northern District of California disagreed, granting summary judgment for Jornaya.

According to Plaintiff Loretta Williams, TCPA Guardian wiretapped her communications in violation of California Penal Code § 631(a) by allegedly recording her keystrokes when she visited a website. Her argument rested on the notion that the hashing process used by TCPA Guardian involved “processing and evaluating” — therefore “reading” — data, which she claimed constituted unauthorized wiretapping under CIPA. However, the court disagreed:

[T]he phrase “reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication” in CIPA requires some effort at understanding the substantive meaning of the message, report or communication, and . . . the evidence shows that TCPA Guardian does not “read, attempt to read, or to learn the contents or meaning” of the information that is input on websites hosting that software.

*Id.* at \*16. The court emphasized that hashing is an automated, technical process that anonymizes data and does not involve interpretation. TCPA Guardian, by design, transforms data into an incomprehensible “hash,” and no original data was stored or retained. *Id.*

Without more, simply formatting data at the outset did not trigger CIPA:

The evidence shows that the data Jornaya receives is automatically subjected to an algorithm that transforms the data into an incomprehensible “hash” that has no inherent substantive meaning, and that Jornaya does not retain the original unhashed data in its servers. The Court is not persuaded by Williams’ argument that the initial step of the hashing process, during which the original data is formatted in a particular way, constitutes “reading” under CIPA. The alteration of the data is an automatic, almost instantaneous step in the hashing process, and does not involve any attempt by Jornaya to understand the substantive meaning of the data.

*Id.*

The court’s decision in *Williams* delivers a clear message: compliance tools that prioritize privacy and operate without substantive interpretation are not wiretapping consumers under CIPA. This ruling provides reassurance for businesses leveraging technologies like TCPA Guardian, helping them confidently navigate TCPA compliance without fear of undue litigation.

©1994-2025 Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. All Rights Reserved.

---

National Law Review, Volume XIV, Number 332

Source URL: <https://natlawreview.com/article/telephone-and-texting-compliance-news-litigation-update-win-tcpa-compliance-and>