



Portfolio Media. Inc. | 230 Park Avenue, 7<sup>th</sup> Floor | New York, NY 10011 | [www.law360.com](http://www.law360.com)  
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | [customerservice@law360.com](mailto:customerservice@law360.com)

## Cybersecurity & Privacy Group Of The Year: Latham & Watkins

By Allison Grande

*Law360 (February 2, 2024, 2:02 PM EST)* -- Latham & Watkins LLP steered a range of clients through cutting-edge data privacy disputes, including securing the dismissal of claims that Otonomo Inc. surreptitiously tracked drivers' locations and helping Apple Inc. escape a consumer class action over security vulnerabilities in its devices, earning the firm a place among Law360's 2023 Cybersecurity & Privacy Groups of the Year.

The past 12 months "represented another banner year" for the firm's privacy and cybersecurity practice, which embraces nearly 100 attorneys spread across offices in San Francisco, New York, Los Angeles, Houston, London, Beijing and a dozen other locations around the globe, according to Michael Rubin, global co-chair of the practice.

The interdisciplinary team has tackled high-stakes litigation and regulatory disputes at the cutting edge of data privacy, including several matters that have sought to advance novel applications of the California Invasion of Privacy Act in an attempt to hold clients liable for billions of dollars in potential statutory damages.

The group has also taken the lead in advising clients on emerging privacy issues related to generative artificial intelligence, a technology that Rubin noted "is transforming every industry it touches and continues to test the boundaries of existing legal rules and the public policies that underlie them."

"The fast-changing technology and legal landscape require us to stay one step ahead, crafting solutions to unforeseen risks well ahead of time," Rubin, who leads the firm's multidisciplinary AI task force, told Law360.

Rubin added that his group had been able to achieve such results in this rapidly evolving field due to their breadth of experience, willingness to work across borders and practice areas, and ability to "bring a 360-degree approach to all matters."

"Critically, Latham does not operate in practice silos," said Rubin, who's based in San Francisco. "Drawing on our deep technology industry knowledge, litigation experience and working relationships with regulatory enforcement authorities in the privacy and consumer protection space, the depth and breadth of Latham's unmatched global platform gives us the ability to put the right team together with extensive insight and relevant experience in order to come up with the most creative solutions for clients."



This approach was on full display in work the practice group did in the past year for clients swept up in a recent wave of litigation accusing a range of companies of violating the California Invasion of Privacy Act, a decades-old wiretapping law, through the technology they deploy on their website to keep track of visitors.

"It's no exaggeration to say that we've been writing the CIPA defense playbook," Rubin said.

In one such matter, the Latham team in January 2023 secured the dismissal of a putative class action accusing data-driven transportation platform Otonomo of tracking drivers' locations and movements without their consent through electronic devices installed in their cars.

The plaintiff had pressed the novel argument that Section 637.7 of the statute, which was enacted in 1999 and prohibits the use of an electronic tracking device attached to a vehicle to determine a person's location, applied to Otonomo's alleged practice of secretly collecting and selling data it gathers from devices placed in internet-connected vehicles made by more than a dozen car brands.

But in ruling on this matter of first impression, U.S. District Judge Trina L. Thompson of the Northern District of California concluded the telematics control unit at the heart of the dispute fell short of being an electronic tracking device covered by the statute because the system was a "component" of the vehicle rather than "attached" to it.

Rubin noted that only three cases had squarely addressed Section 637.7 in the statute's history. If the district court had adopted the plaintiff's novel contention, the result would have not only exposed Otonomo to a massive liability of \$1,000 for every time a car's location was cited, but also "would have had significant implications across the transportation sector, potentially exposing a wide variety of companies to similar claims of privacy violations," according to Rubin.

"With the court deciding on a question of law related to a statute ... written for a technology that didn't exist at the time, we had to construct our winning arguments from first principles of statutory interpretation, and successfully convinced the judge on the first try to dismiss the case with prejudice," Rubin said of the district court's decision, which the plaintiff moved in August to appeal to the Ninth Circuit.

The Latham team also obtained a favorable result for Pindrop Security in another case of first impression seeking to expand the California law to cover voice authentication and fraud-prevention software used by banks and other companies to protect customers.

The plaintiff in that matter sued under a never-before-used provision, Section 637.3, which was put on the books in 1978 and requires express consent before voiceprints or "voice stress patterns" can be examined to determine "the truth or falsity" of statements.

"In the face of potentially enormous exposure, we again developed creative, first-of-their-kind arguments about the 1978 statute, including by mining statutory history to show that it had been passed out of concerns about amateur use of lie detectors," Rubin said. "We ultimately persuaded plaintiff's counsel to voluntarily drop their claim with prejudice [in March] the night before oral argument on Pindrop's motion to dismiss, once again avoiding billions in potential statutory damages."

Outside the privacy law arena, the practice group secured another significant result for Apple in September, when a split Ninth Circuit panel affirmed a decision tossing consolidated proposed consumer class actions alleging the tech giant hid the fact that its software fix for a security bug slowed down the processing speeds of nearly all its iPhones, iPads and other popular products.

In its majority opinion, the appellate panel found the plaintiffs had failed to show that comments from Apple executives in 2017 about the speed of its devices were false, or that the consumers relied on the executives' statements and would not have bought Apple products if they had known the truth.

The plaintiffs lodged their claims after Apple quickly moved to patch two industrywide security vulnerabilities that had the potential to affect nearly every modern central processing unit before any bad actors could exploit the flaw.

"This is an incredibly important win to the technology industry, particularly in light of the endless ingenuity of criminals seeking new ways to breach devices and exploit data," said Melanie M. Blunski, a San Francisco-based partner on the Latham team. "This result helps ensure that companies can protect their customers and address newly discovered challenges without inadvertently putting users at an increased security risk by announcing that they are doing so."

The practice also defended Facebook's parent company, Meta Platforms Inc., in a putative class action accusing it of violating the Telephone Consumer Protection Act by sending unwanted automated text message reminders to users about friends' birthdays.

In a precedential December 2022 ruling, the Ninth Circuit held a lower federal court was correct to toss the dispute, finding the texts didn't violate the statute because users gave their phone numbers directly to Facebook. In doing so, the panel not only rejected the plaintiff's bid to press a broad "autodialer" definition that had previously helped spur a flood of litigation, but also freed Meta from potentially billions of dollars in statutory damages.

The Latham team also represented online game developer Zynga in a putative class action over a data breach that reportedly affected more than 200 million users.

In tossing the suit with prejudice in April 2022, a California federal judge sided with the argument put forth by Latham partner Serrin Turner that the U.S. Supreme Court's decision the previous June in *TransUnion LLC v. Ramirez* — in which the high court tightened standing rules to require a concrete injury — meant people whose data is stolen or mishandled cannot sue for damages under a general risk of identity theft.

The decision, which echoed the standing conclusion the judge reached in dismissing the suit with leave to amend in July 2021, marked "one of the first post-*TransUnion* dismissals of a data breach case, with significant implications for future privacy class actions," Turner told Law360.

Additionally, the practice group has guided clients through an array of regulatory matters, including its representation of SolarWinds in a suit brought by the U.S. Securities and Exchange Commission accusing it of underselling investors on its vulnerability to cyberattacks like the one that struck the company and its federal government clients in 2020.

While most of the group's significant achievements in the regulatory arena are confidential, this work is "noteworthy for the number of major active investigations on cutting-edge data issues we handle," said Rubin. "Of the [Federal Trade Commission's] self-proclaimed 10 most important enforcement matters of 2023, Latham handled 30% of them."

--Editing by Karin Roberts. All Content © 2003-2024, Portfolio Media, Inc.