
California Settles with Glow App Over Alleged Privacy and Security Violations

SEPTEMBER 29, 2020

In September, the California Attorney General (the “AG”) reached a [settlement](#) with Glow, Inc. (“Glow”), a technology company that is responsible for an ovulation and fertility-tracking mobile application called the Glow app. The [AG alleged](#) violations of California’s [Confidentiality of Medical Information Act](#) (“CMA”), the [Unfair Competition Law](#) (“UCL”), and the [False Advertising Law](#) (“FAL”), though Glow made no admission of liability in the settlement. Ultimately, the settlement imposes a monetary fine as well as highly prescriptive injunctive terms that last for a period of 2 to 3 years and go far beyond the requirements of California law. Glow must maintain certain information related to user consent, document product design methodology for potential review by the AG, and provide risk assessments to the AG, among other things. The AG also has incorporated certain gender-specific requirements that companies may want to evaluate as part of their overall approach to “privacy by design” in developing their products. Companies operating in California also should evaluate these provisions to determine whether they make sense to consider or could create potential risks based on current operations, even if not formally required by existing law.

Background

The Glow app was designed to track user information including medications, fertility test results, medical appointments and records, ovulation cycle calculations, and pregnancy history. Users may also track additional information via the app, including efforts to become pregnant, miscarriages, abortions, and stillbirths. The AG alleged that, between the years of 2013 and 2016, the Glow app had privacy and security flaws that put such data at risk.

One alleged flaw was found in a feature called “Partner Connect,” which allowed two app users to share information between their accounts. According to the AG’s complaint, when one user would send a linking request to another, the app would automatically grant such a request without any authorization or confirmation from the user who was about to have their information shared.

Another alleged flaw involved Glow not adequately verifying or authenticating requests from users to change their account passwords, creating an exploitable vulnerability. Further, the defendants made representations about how they protected user privacy and personal data, but those representations were allegedly contradicted by the security flaws.

The settlement did not come about as the result of a breach or cybersecurity incident; rather, it addressed security and privacy violations made “in offering and operating the Glow app” absent any known breach.

Settlement Terms

The settlement imposes a \$250,000 civil penalty and injunctive terms related to information security and privacy. The Information Security Program requires the implementation of procedural safeguards (such as an employee training program), internal data access restrictions, risk assessments, and a process to obtain affirmative authorization from consumers to share their data outside of Glow with a third party or to use their data in a new or different way. Further, the settlement requires that Glow designates individuals to manage its compliance with the settlement terms, and that it notifies the AG of the number and title of these individuals.

Glow must get affirmative consent from users before disclosing user data to any third parties (excluding service providers); the notice must include “easy to read and understandable to a consumer” and include a description of the information that will be used and the purpose for its use, as well as instructions for the revocation of consent. Glow must maintain a record of the date of each user’s consent; this recordkeeping requirement suggests that the AG may request to review these records, although such review is not a term of settlement. In addition, Glow is not permitted to condition the use of its app on the provision of consent unless reasonably required for a feature to function. Glow must also conduct a regular inventory of its mobile apps and online services.

The settlement also requires Glow to implement and maintain a process to incorporate privacy-by-design and security-by-design principles into its apps. For apps that are designed to be used primarily by women, such principles should be designed specifically to assess “how privacy or security lapses may impact online threats affecting women and online risks that women face, or could face, including gender-based risks, from privacy and security lapses.” These processes must be documented for review by the AG. Glow must also perform an annual privacy risk assessment and an annual security risk assessment, which are to be submitted to Glow’s CEO, Board of Directors, and the AG.

Conclusion

This settlement indicates that the AG is taking a forward-leaning approach to settlements with technology companies and that it seeks to maintain engagement with companies long after settlements are reached. In addition, the highly prescriptive terms may be indicative of a broader approach to apps and an effort to go well beyond the requirements of California law. Finally, technology companies should be aware of the emphasis on gender-based risk in this settlement. California may be seeking to protect historically disadvantaged populations with future investigations and settlements. As such, developers of apps geared toward these populations should pay close attention to these developments.

Authors



Kirk J. Nahra

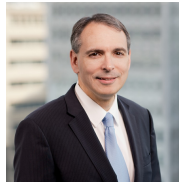
PARTNER

Co-Chair, Artificial
Intelligence Practice

Co-Chair, Cybersecurity
and Privacy Practice

✉ kirk.nahra@wilmerhale.com

☎ +1 202 663 6128



**Benjamin A.
Powell**

PARTNER

Co-Chair, Cybersecurity
and Privacy Practice

Co-Chair, Artificial

Intelligence Practice

✉ benjamin.powell@wilmerhale.com

☎ +1 202 663 6770



Ariel Dobkin

COUNSEL

✉ ariel.dobkin@wilmerhale.com

☎ ++1 202 663 6878