AN A.S. PRATT PUBLICATION
JANUARY 2021
VOL. 7 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 1** **JANUARY 2021**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [245] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2021–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

California AG Settlement Suggests Privacy and Security Practices of Digital Health Apps May Provide Fertile Ground for Enforcement Activity

By Elizabeth H. Canter, Anna D. Kraus, and Rebecca Yergin [*]

This article contains a discussion of the California Attorney General's complaint and settlement against Glow, Inc., which resolved allegations that its fertility app had "expose[d] millions of women's personal and medical information," as well as takeaways from the case.

California Attorney General Xavier Becerra ("AG") has announced[1] a settlement[2] against Glow, Inc., resolving allegations that the fertility app had "expose[d] millions of women's personal and medical information."

In the complaint,[3] the AG alleged violations of certain state consumer protection and privacy laws, stemming from privacy and security "failures" in Glow's mobile application (the "Glow App"). The settlement requires Glow to comply with relevant consumer protection and privacy laws (including California's medical privacy law), mandates "a first-ever injunctive term that requires Glow to consider how privacy or security lapses may uniquely impact women," and imposes a $250,000 civil penalty.

According to the AG's announcement, the "settlement is a wake up call not just for Glow, Inc., but for every app maker that handles sensitive private data." This article contains a discussion of the complaint and settlement, as well as takeaways from the case.

THE COMPLAINT

As described in the complaint, the Glow App is "marketed as an ovulation and fertility tracker" and "collects and stores deeply sensitive personal and medical information related to a user's menstruation, sexual activity, and fertility." The types of information collected include medications, fertility test results, medical appointments, medical records, and

[*] Elizabeth (Libbie) H. Canter is a partner at Covington & Burling LLP representing a wide variety of multinational companies on privacy, cyber security, and technology transaction issues. Anna D. Kraus is of counsel at the firm advising on issues relating to the laws governing the health care industry. Rebecca Yergin is an associate at the firm and a member of the firm's Communications and Media and Data Privacy and Cybersecurity Practice Groups. Resident in the firm's Washington, D.C., office, the authors may be contacted at ecanter@cov.com, akraus@cov.com, and ryergin@cov.com, respectively.

[1] https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-landmark-settlement-against-glow-inc-%E2%80%93.

[2] https://oag.ca.gov/sites/default/files/People v. Glow - Final Judgment and Permanent Injunction - 07374856.pdf.

[3] https://oag.ca.gov/sites/default/files/2020 09-17 - People v Upward Labs - Complaint.pdf.

ovulation-cycle calculations, as well as "intimate details of [] sexual experiences and efforts to become pregnant." One feature of the Glow App is its "Partner Connection" offering, which "allows a Glow App user to link to a partner to share information."

As alleged, Glow violated multiple laws, including California's Confidentiality of Medical Information Act ("CMIA"). The CMIA regulates, in relevant part, "providers of health care" that collect and use "medical information," defined as "individually identifiable information . . . in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment."

According to the complaint, Glow is a "provider of health care" under CMIA because it "offer[s] software to consumers that is designed to maintain medical information for the purposes of allowing users to manage their information or for the diagnosis, treatment, or management of a medical condition."[4] The complaint also alleges that Glow's privacy and security practices violated California's Unfair Competition Law ("UCL") and False Advertising Law ("FAL").

The specific activities alleged to have triggered these violations of law from 2013 to 2016 include the following:

- The Partner Connect feature "automatically granted" linking requests and "immediately shared" certain "sensitive information" without obtaining authorization from the Glow user.
- The Partner Connect feature failed to verify the legitimacy of the person with whom the information was being shared.
- The Glow App's password change functionality asked for "old passwords" without authenticating such passwords on the back-end.
- Glow's Privacy Policy and Terms of Use made representations about the company's privacy and security practices that were "contradicted" by Glow's actual practices (e.g., "We have designed the Service to protect information about you from unauthorized disclosures to others.").

THE SETTLEMENT

The AG's settlement with Glow (1) requires Glow to comply with relevant consumer protection and privacy laws, (2) obligates Glow to consider how "privacy or security lapses may uniquely impact women," and (3) imposes a $250,000 civil penalty. The requirements of the settlement are discussed in turn.

[4] Citing Cal. Civ. Code 56.06(b).

First, the settlement requires Glow to comply with consumer protection and privacy laws, including the CMIA. To do so, Glow must implement an information security program "to protect the security, integrity, availability, and confidentiality" of "personal information," "medical information," and "sensitive personal information" that Glow "collects, stores, processes, uses, transmits, and maintains." "Personal information" has the meaning it is given under California's Data Security Law,[5] and "medical information" has the meaning it is given under CMIA, with the clarification that such information may be "enter[ed] or upload[ed] . . . into a mobile application or online service" by a consumer. "Sensitive information" refers to information that is not "medical information" or "personal information" but is individually identifiable information that describes a consumer's "sexual activity, sexual health, and reproductive health."

Under the settlement, Glow's information security program is required to protect the specified categories of information by taking measures such as:

- Preventing unauthorized access;
- Preventing unauthorized disclosure;
- Imposing a two-step authentication process for password changes;
- Providing annual employee training on the information security practices;
- Implementing procedures for vulnerability patching;
- Incorporating privacy-by-design principles and security-by-design principles when creating new Glow App features; and
- Establishing a point of contact at Glow to address security issues.

Second, the settlement requires Glow, for two years after implementing its information security program, to complete annual privacy and security risk assessments addressing Glow's efforts to comply with applicable privacy and security laws. The reports must be submitted to the AG's office.

Notably, the settlement requires the privacy assessment to "(i) consider online risks that women face, or could face, including gender-based risks, as a result of privacy or security lapses while using GLOW mobile applications or online services; (ii) consider the impact of any such risks, and (iii) document GLOW's efforts to mitigate any such risks." As noted, the AG's announcement of the settlement refers to this requirement as a "first-ever injunctive term" that requires a company to consider the unique impact of privacy and security lapses on women.

Third, the settlement imposes a civil penalty of $250,000.

[5] Cal. Civ. Code. 1798.81.5.

KEY TAKEAWAYS

The settlement highlights the sensitivity of health data, even if that data is not protected under the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Notably, the AG's announcement asserts, "[w]hen you meet with your doctor or healthcare provider in person, you know that your sensitive information is protected. It should be no different when you use healthcare apps over the internet."

The Glow complaint alleges that Glow is a "provider of health care" for the purposes of CMIA because it "offer[s] software to consumers that is designed to maintain medical information for the purposes of allowing its users to manage their information or for the diagnosis, treatment, or management of a medical condition. Specifically, the Glow app is designed for the user to store, email, and print information relating to their reproductive health such as ovulation and menstrual cycles, and/or for the diagnosis, treatment, or management of users seeking to become pregnant or treat infertility."

The settlement also states that health information may be "medical information" for the purposes of the CMIA "irrespective of how the information is transmitted," and thus may include information that is "manually enter[ed] or upload[ed] . . . into a mobile application or online service."

This settlement follows other recent health and medical privacy developments in California.

In early September, the California legislatures passed AB 173, creating a new healthcare-related exemption under the California Consumer Privacy Act of 2018.

Although the legislature also passed SB 980, the Genetic Information Privacy Act ("GIPA"), Governor Gavin Newsom recently vetoed the bill. GIPA would have imposed certain privacy and security obligations on direct-to-consumer genetic testing companies, and the governor's veto of the bill cited potential implications on research related to COVID-19.

Another recent development is the AG's announcement of a $8.69 million settlement against Anthem Inc., resolving allegations that the health insurer violated state law and HIPAA.