AN A.S. PRATT PUBLICATION
OCTOBER 2022
VOL. 8 NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 8** **October 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@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*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (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

(2022–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, 631.291.5541. 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.

Top Six Privacy Impacts on Mobile Health Apps from Overturning *Roe v. Wade*

By Jane E. Blaney, Peter A. Blenkinsop and Jeremiah Posedel*

The authors discuss the top six privacy impacts on mobile health apps of the U.S. Supreme Court's Dobbs decision.

The privacy of individuals who use mobile health apps – in particular, menstrual health and similar apps – was thrust into the spotlight with the U.S. Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization* to overturn *Roe v. Wade*, with users concerned about how their sensitive health information might be shared and for what purposes. This concern is driven by the fear that states which ban and criminalize abortion may seek relevant health data from app providers to identify and prosecute individuals who obtained an abortion out of state or otherwise circumvented their home state's statute. As a result, mobile health apps are now responding to a flood of user concerns and forced to analyze the implications to user data and their respective services in order to protect and maintain users – and their business.

While the implications of overturning *Roe v. Wade* will undoubtedly evolve with time, what follows are the top six privacy impacts of the decision on mobile health apps.

1. PRIVACY NOTICES MAY NEED TO BE AMENDED

Recent changes in privacy laws both in the United States and globally have led to increasingly complex privacy notices. Companies often draft broad notices that give the business as much flexibility as possible in terms of the data they collect, how they may use it and who they may share it with. Not only does this approach give the business some flexibility regarding how they can leverage user data in the future, but it also provides some legal cover. Specifically, the general position of the Federal Trade Commission ("FTC") on privacy – based on Section 5 of the FTC Act – is "do what you say and say what you do." By including broad data collection, usage and sharing rights in their privacy notices, companies mitigate the risk of processing data in the future in a

* Jane E. Blaney, an associate in the Minneapolis office of Faegre Drinker Biddle & Reath LLP, counsels insurance clients on regulatory and transactional matters, offering concentrated knowledge in health insurance, data analytics and technology, privacy and cybersecurity. Peter A. Blenkinsop, a partner in the firm's office in Washington, D.C., advises clients on regulatory compliance, focusing on two distinct but overlapping areas: (i) information privacy and data protection, and (ii) medical research. Jeremiah Posedel, a partner in the firm's Chicago office, counsels multinational and other companies on a wide range of information technology and data processing transactions and compliance issues. The authors may be contacted at jane.blaney@faegredrinker.com, peter.blenkinsop@faegredrinker.com and jeremiah.posedel@faegredrinker.com, respectively.

manner not initially disclosed to consumers. With the decision to overturn *Roe v. Wade*, app providers may want to reconsider this approach and instead, limit their processing activities (actual or potential) to give users comfort that their data will be used only for specific and limited ways – and only the minimum information necessary will be collected and maintained (as discussed in point 2 below). A first, and critical, step in giving users this comfort is updating the privacy notice to reflect the new, limited scope of processing.

2. DATA COLLECTION MAY NEED TO BE LIMITED

Unless specifically limited by law, mobile app data collection practice generally includes collecting more data than necessary. While there can certainly be benefits to this approach to data collection, it may expose a user to further scrutiny and risk if their sensitive data is subpoenaed. Mobile health apps should consider scrutinizing data collection and analyzing the benefits of such collection versus the risk to a user if such data was obtained and shared. If a mobile health app does limit data collection to what is necessary, disclosure of such a practice may provide users with the comfort they need to continue use of the mobile health app.

3. LOCATION TRACKING MAY NEED TO BE DISABLED

Although location data can be utilized to support marketing or other consumer analysis, enabling location tracking may increase the risk of user data being linked to a specific location if their data is subpoenaed. Mobile health apps should consider disabling location tracking or only collect it with the user's informed opt-in consent. When location data is collected, it should be permanently deleted as soon as the data is no longer relevant or the purpose for collecting it has been achieved.

4. DATA DISCLOSURES SHOULD BE SCRUTINIZED

Where a mobile health app shares or sells collected user data with a third-party, these third parties should be closely scrutinized to ensure their data practices are in alignment with the mobile health app's practices and that users are fully aware of the contemplated sharing and consent to it. For example, if sold to or shared with certain third parties, a user's health app data may be combined with other data to obtain a more complete user profile than intended. Where mobile health apps do enter into any sort of data sharing agreement, these privacy concerns and agreements should be clearly outlined in their contract. Further, avoid selling or sharing sensitive health data whenever possible.

5. CONSUMER EDUCATION SHOULD BE PROVIDED

User education is an important piece of data privacy. Users should be educated about their own responsibility to protect their data through responsible sharing. One such

example may be to prompt users to use browsers with private networks when clicking any link in an app that may lead to an external link.

6. DATA SECURITY PRACTICES SHOULD BE REVIEWED AND MAY NEED TO BE INCREASED

Mobile health apps should scrutinize their data security practices, analyzing both their own security as well as the security of any third party through whom user data or the mobile health app platform can be obtained. Especially in states that ban and/or criminalize abortion, there is growing concern of cyber attackers seeking to obtain relevant health data from app providers in an effort to expose or identify and report individuals who have sought an abortion out of state or through other means. Where mobile health apps contract with third parties, they should ensure their contracts address data security to protect sensitive user data.