

AN A.S. PRATT PUBLICATION
NOVEMBER-DECEMBER 2019
VOL. 5 • NO. 9

PRATT'S
**PRIVACY &
CYBERSECURITY
LAW**
REPORT



LexisNexis

EDITOR'S NOTE: TAKE IT FROM THE TOP

Victoria Prussen Spears

**CYBERSECURITY STARTS AT THE TOP:
RISKS AND CONCERNS FOR DIRECTORS
AND OFFICERS**

Matthew D. Dunn and Melissa J. Erwin

**CAN A SECURITY BREACH IMPACT A COMPANY
YEARS LATER? LESSONS LEARNED FROM
THE EQUIFAX BREACH**

Stephen E. Reynolds and Rachel Spiker

BIOMETRICS DEVELOPMENTS: BIPA & BEYOND

Mary Buckley Tobin

**FTC AND NEW YORK ATTORNEY GENERAL
REACH \$170 MILLION SETTLEMENT AGAINST
GOOGLE AND YOUTUBE FOR ALLEGED
CHILDREN'S PRIVACY VIOLATIONS**

Lindsey L. Tonsager and Ani Gevorkian

KEEPING UP WITH THE CCPA

Pavel A. Sternberg

**NEWLY RELEASED DRAFT MEASURES ON
DATA SECURITY MANAGEMENT STRENGTHEN
CHINA'S DATA PROTECTION FRAMEWORK**

Tiana Zhang, Cori A. Lable, Jodi Wu,
Richard Sharpe, and Yue Qiu

FROM THE COURTS

Jay D. Kenigsberg

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5

NUMBER 9

NOVEMBER-DECEMBER 2019

Editor's Note: Take It from the Top

Victoria Prussen Spears

275

**Cybersecurity Starts at the Top: Risks and Concerns for Directors
and Officers**

Matthew D. Dunn and Melissa J. Erwin

277

**Can a Security Breach Impact a Company Years Later? Lessons Learned
from the Equifax Breach**

Stephen E. Reynolds and Rachel Spiker

284

Biometrics Developments: BIPA & Beyond

Mary Buckley Tobin

288

**FTC and New York Attorney General Reach \$170 Million Settlement Against
Google and YouTube for Alleged Children's Privacy Violations**

Lindsey L. Tonsager and Ani Gevorkian

291

Keeping Up with the CCPA

Pavel A. Sternberg

295

**Newly Released Draft Measures on Data Security Management Strengthen
China's Data Protection Framework**

Tiana Zhang, Cori A. Lable, Jodi Wu, Richard Sharpe, and Yue Qiu

299

From the Courts

Jay D. Kenigsberg

303

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 [275] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2019 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

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

(2019–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF

STEVEN A. MEYEROWITZ

President, Meyerowitz Communications Inc.

EDITOR

VICTORIA PRUSSEN SPEARS

Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

EMILIO W. CIVIDANES

Partner, Venable LLP

CHRISTOPHER G. CWALINA

Partner, Holland & Knight LLP

RICHARD D. HARRIS

Partner, Day Pitney LLP

JAY D. KENIGSBURG

Senior Counsel, Rivkin Radler LLP

DAVID C. LASHWAY

Partner, Baker & McKenzie LLP

ALAN CHARLES RAUL

Partner, Sidley Austin LLP

RANDI SINGER

Partner, Weil, Gotshal & Manges LLP

JOHN P. TOMASZEWSKI

Senior Counsel, Seyfarth Shaw LLP

TODD G. VARE

Partner, Barnes & Thornburg LLP

THOMAS F. ZYCH

Partner, Thompson Hine

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. Copyright 2019 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries 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.

FTC and New York Attorney General Reach \$170 Million Settlement Against Google and YouTube for Alleged Children’s Privacy Violations

*By Lindsey L. Tonsager and Ani Gevorkian**

The authors of this article explore a settlement of allegations against Google LLC and its subsidiary YouTube, LLC, claiming violations of the Children’s Online Privacy Protection Act and its implementing rule. Under the settlement, Google and YouTube are required to pay a total of \$170 million to the Federal Trade Commission and the New York Attorney General’s office.

The Federal Trade Commission (“FTC”) and the New York Attorney General’s office (“NYAG”) have settled allegations against Google LLC and its subsidiary YouTube, LLC claiming violations of the Children’s Online Privacy Protection Act and its implementing rule (together, “COPPA”). The settlement requires Google and YouTube to pay \$136 million to the FTC and \$34 million to the NYAG for a total penalty almost 30 times higher than the largest COPPA penalty previously imposed.

OVERVIEW OF THE COMPLAINT AND ORDER

The joint FTC-NYAG complaint¹ alleged that Google and YouTube collected personal information from children under 13 online and used that information to deliver online behavioral advertising, without first providing notice or obtaining verifiable parental consent as required by COPPA. More specifically, the complaint alleged that Google and YouTube had actual knowledge that certain YouTube channels were child-directed but nevertheless collected persistent identifiers in the form of cookie and advertising identifiers to serve behavioral advertising to viewers of those channels.

In addition to requiring the \$170 million total civil penalty and enjoining future COPPA violations, the settlement order² requires “fencing-in” relief—which is relief in the form of injunctive provisions that go beyond what is required under existing law.

* Lindsey L. Tonsager is a partner at Covington & Burling LLP helping national and multinational clients in a broad range of industries anticipate and effectively evaluate legal and reputational risks under federal and state data privacy and communications laws. Ani Gevorkian is an associate in the firm’s Communications & Media and Data Privacy & Cybersecurity Practice groups. The authors may be reached at ltonsager@cov.com and agevorkian@cov.com, respectively.

¹ https://www.ftc.gov/system/files/documents/cases/youtube_complaint.pdf.

² https://www.ftc.gov/system/files/documents/cases/172_3083_youtube_coppa_consent_order.pdf.

The order requires that YouTube and Google establish a system on YouTube that requires channel owners to self-designate whether the content they upload is child-directed. For videos designated as child-directed, YouTube will not collect persistent identifiers for behavioral advertising. The order further requires that Google and YouTube implement a training program for employees about the system and about COPPA's requirements overall. Finally, it imposes compliance reporting and record-keeping requirements.

The settlement is notable both for what it does—and doesn't—establish:

WHAT THE SETTLEMENT DOES

Reaffirms the Actual Knowledge Standard

The allegations against Google and YouTube were premised on Google and YouTube having actual knowledge of specific child-directed content on the YouTube platform. Under the COPPA statute, sites and services directed to a general audience are not subject to COPPA's requirements unless and until they gain "actual knowledge" that personal information is collected online from children. In 2013, the FTC also interpreted the statutory language to expand COPPA's scope to cover operators of general audience sites and services that have actual knowledge that they collect personal information through other child-directed sites and services. Here, the FTC found that Google had actual knowledge through:

- Google and YouTube's direct communications with companies who uploaded content to YouTube and specifically indicated to Google or YouTube that this content was directed to children;
- Content ratings that Google assigned to specific content on YouTube and which designated certain content as "generally intended for children ages 0-7;" and
- Google and YouTube's curation of specific YouTube content for its separate YouTube Kids app.

The FTC also expressed concern that Google and YouTube marketed YouTube to advertisers as a top destination for kids. For example, in a presentation to certain toy brands Google and YouTube stated that: "YouTube is today's leader in reaching children age 6-11 against top TV channels"; "YouTube was unanimously voted as the favorite website for kids 2-12"; YouTube is "[t]he new 'Saturday Morning Cartoons'"; and "YouTube was the "#1 website regularly visited by kids." The complaint noted that these statements contradicted statements that Google and YouTube were separately making to content providers that no users under 13 were on YouTube.

Significantly, a separate statement by Chairman Simons and Commissioner Wilson³ and statements by Andrew Smith, Director of the Bureau of Consumer Protection, during the press briefing announcing the settlement, emphasized that the FTC would bear the burden of establishing in court that Google and YouTube had actual knowledge of the child-directed status of each channel. This reliance on the actual knowledge standard is consistent with the text of the COPPA statute, which explicitly requires actual knowledge, and long-standing FTC precedent rejecting lower standards (such as constructive knowledge—like the AI-based predictive tool suggested by Commissioner Slaughter—or a reason to know standard) as inappropriate and unworkable.

Puts Pressure on Children’s Content Companies to Put Platforms on Notice

The complaint alleges that individual channels on the YouTube platform are “websites or online services” under COPPA and that, accordingly, content companies that post child-directed content on YouTube are on notice that the FTC will consider them to be standalone “operators” under COPPA, subject to strict liability for COPPA violations involving data collected from children through those channels. The FTC warned that it will be conducting a “sweep” of child-directed content on platforms following implementation of the order’s provisions. This language is likely to motivate children’s content companies to notify their platform partners that their content is child directed and to inquire further about COPPA compliance.

WHAT THE SETTLEMENT DOESN’T DO

No Legal Obligation for General Audience Platforms to Investigate

The Simons/Wilson separate statement explicitly provides that while Google will be required under the Order’s fencing in provisions to create a system for content providers to self-designate whether the content they post online is child-directed, this step goes beyond COPPA’s legal requirements and no other platform or adtech company is bound by this Order. The case continues the FTC’s long-held view that platforms and general audience services have no legal obligation to investigate whether third-party content on their platforms is directed to children.

No Requirement to Algorithmically Predict Whether Content is Child-Directed

While the order requires Google and YouTube to implement a mechanism for channel owners to identify child-directed content, it stops short of requiring YouTube to implement an algorithmic tool to predict whether content may be child-directed and tag such content itself for child-directed treatment. Commissioner

³ https://www.ftc.gov/system/files/documents/public_statements/1542922/simons_wilson_google_youtube_statement.pdf.

Slaughter advocated for such a technological backstop as a way of attempting to police channels that may mis-designate their content. However, as explained by the Chairman Simons/Commissioner Wilson statement and by Director Smith during the press conference, the FTC refrained from imposing such a requirement out of concern that the efficacy of an algorithm could be difficult to enforce, that the use of an algorithm could serve as a shield against enforcement, and that prescribing an algorithm that would keep pace with evolving technology could prove difficult. In addition (and as noted above), such an approach would impose a constructive knowledge standard on platforms contrary to the text of the COPPA statute, because it would require these algorithms to ferret through circumstantial evidence to assess the channel's audience and could at best provide a prediction of child-directed status.