AN A.S. PRATT PUBLICATION
APRIL 2020
VOL. 6 • NO. 3

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

EDITOR'S NOTE: INFORMATION SECURITY
Victoria Prussen Spears

THE SEVEN LAYER CAKE OF INFORMATION SECURITY: A TECHNICAL GUIDE FOR THE NON-TECHNICAL READER
David Kalat

CALIFORNIA BILL PROPOSES CCPA EXCEPTIONS FOR HIPAA DE-IDENTIFIED INFORMATION, OTHER HEALTH DATA
Deepali Doddi and Daniel F. Gottlieb

FTC DATA PRIVACY SETTLEMENT MAY SIGNAL MORE DIRECT APPROACH TO REGULATING DATA SECURITY
Jonathan S. Kolodner, Alexis Collins, and Richard R. Cipolla

CAN BORDER AGENTS SEARCH YOUR PHONE? AN UPDATE
J. Alexander Lawrence and Sara Stearns

MAJOR BOOST FOR STANDARD CONTRACTUAL CLAUSES CHALLENGED BY THE *SCHREMS* 2.0 CASE, BUT MORE UNCERTAINTY FOR THE PRIVACY SHIELD
Mark Dawkins, Jenny Arlington, and Rachel Claire Kurzweil

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 | NUMBER 3 | APRIL 2020

Editor's Note: Information Security
Victoria Prussen Spears 67

The Seven Layer Cake of Information Security: A Technical Guide for the Non-Technical Reader
David Kalat 69

California Bill Proposes CCPA Exceptions for HIPAA De-Identified Information, Other Health Data
Deepali Doddi and Daniel F. Gottlieb 84

FTC Data Privacy Settlement May Signal More Direct Approach to Regulating Data Security
Jonathan S. Kolodner, Alexis Collins, and Richard R. Cipolla 88

Can Border Agents Search Your Phone? An Update
J. Alexander Lawrence and Sara Stearns 91

Major Boost for Standard Contractual Clauses Challenged by the *Schrems* 2.0 Case, But More Uncertainty for the Privacy Shield
Mark Dawkins, Jenny Arlington, and Rachel Claire Kurzweil 94

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*, [6] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [67] (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

(2020–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 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 Data Privacy Settlement May Signal More Direct Approach to Regulating Data Security

By Jonathan S. Kolodner, Alexis Collins, and Richard R. Cipolla*

The U.S. Federal Trade Commission ("FTC") has proposed a settlement with InfoTrax Systems, L.C., a third-party service provider, regarding multiple data security failures after a hacker accessed about one million consumers' sensitive personal information. This article discusses the settlement, which marks one of the first instances in which the FTC has alleged a violation of the FTC Act predicated solely upon the failure to maintain reasonable security measures by a third-party service provider.

The U.S. Federal Trade Commission ("FTC" or "Commission") has reached a proposed settlement[1] with InfoTrax Systems, L.C. ("InfoTrax"), a third-party service provider, regarding multiple data security failures. As a result of these security shortcomings, a hacker accessed about one million consumers' sensitive personal information after more than 20 intrusions into InfoTrax's network.

The settlement marks one of the first instances in which the FTC has alleged a violation of the FTC Act predicated solely upon the failure to maintain reasonable security measures by a third-party service provider.

The settlement is also notable for a Commissioner's concurring statement criticizing the settlement's standard 20-year term.

THE SETTLEMENT ORDER

Unlike many respondents facing FTC scrutiny for its data security practices, InfoTrax is not a consumer-facing company. Rather, InfoTrax operates website portals for direct sales companies. The clients of the direct sales companies, in turn, use the website portals to register and place orders on behalf of themselves and the end consumers. The distributors, through registering and placing orders, submit significant amounts of personal information (such as Social Security numbers and credit card numbers) about themselves and end consumers to InfoTrax.

The FTC alleges that InfoTrax failed to follow numerous best practices to protect the personal information it held on behalf of the direct sales companies. For example:

* Jonathan S. Kolodner (jkolodner@cgsh.com) is a partner at Cleary Gottlieb Steen & Hamilton LLP focusing on white-collar criminal enforcement and regulatory matters as well as complex commercial litigation. Alexis Collins (alcollins@cgsh.com) is a partner at the firm focusing on complex civil and antitrust litigation, criminal and regulatory enforcement matters, and cybersecurity. Richard R. Cipolla was previously an associate at the firm.

[1] https://www.ftc.gov/system/files/documents/cases/162_3130_infotrax_order_clean.pdf.

- InfoTrax failed to perform adequate code review and penetration testing to assess cyber risks;
- InfoTrax failed to take precautions to detect malicious file uploads or limit their upload on its network;
- InfoTrax failed to adequately silo clients' data;
- InfoTrax failed to regularly monitor for unauthorized attempts to transfer sensitive data from its network;
- InfoTrax stored confidential information in clear, readable text; and
- InfoTrax did not systematically delete personal information it no longer needed.

Exploiting these weaknesses, hackers allegedly accessed InfoTrax's systems more than 20 times over nearly two years, culminating with the theft of about one million consumers' sensitive personal information. InfoTrax was unaware of the intrusion until the hackers' activities impacted its servers' performance.

The complaint[2] alleges that InfoTrax's "failure to employ reasonable data security practices to protect personal information" constitutes an unfair act or practice in violation of the FTC Act. As a result of the violation and according to the terms of the settlement, InfoTrax is not permitted to handle personal information until it implements several specific safeguards to its security information program. Specifically, the Commission provides over two pages of directions, requiring improvements ranging from encrypting sensitive data and documenting its security practices to segmenting its network, performing annual penetration testing, and obtaining third-party assessments of its information security program. As is common in these cases, the settlement order runs for 20 years.

TAKEAWAYS

FTC Now Targeting Shoddy Security Practices Directly

Historically, the FTC connected a failure to properly safeguard data to a FTC Act violation in two discrete steps: (1) the FTC argues that the respondent's deficient data privacy practices do not comply with its own stated practices then (2) the FTC argues that the respondent's failure to follow its own stated practices is an unfair or deceptive act.[3]

Here, the FTC contends that InfoTrax's security shortcomings themselves constitute an unfair or deceptive act. The FTC's contention is novel and untested, and

[2] https://www.ftc.gov/system/files/documents/cases/162_3130_infotrax_complaint_clean.pdf.

[3] *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F. 3d 236 (3d Cir. 2015); *In the Matter of BLU Products Inc. et al.*, Matter No. 1723025 (Sept. 6, 2018).

may indicate a shift towards a more direct approach to regulating data security. This approach may be necessary to regulate respondents, like InfoTrax, that do not directly serve consumers or maintain privacy policies directed towards consumers. Such third-party service providers have become a recent focal point for the Commission.

FTC Mandates Specific Data Security Practices

Between the laundry list of security failures and the two pages of remediation requirements, the InfoTrax settlement outlines the security practices that the FTC expects entities handling personal data to maintain. In the past, the FTC provided limited direction in its settlement orders on how to ensure data security programs would be "reasonable designed" to protect confidential information. But last year the U.S. Court of Appeals for the Eighth Circuit ruled that the FTC cannot enforce such vague settlement orders. Perhaps to address the concerns expressed in that decision, the order in this case and in connection with other recent settlements now direct the implementation of specific security practices. The FTC has also issued a statement[4] acknowledging that it was mandating "new requirements that go beyond requirements from previous data security orders" and will continue to reevaluate requirements order-to-order.

10 or 20 Year Obligations?

As Commissioner Wilson noted in her concurring statement[5] regarding the settlement, the FTC' practice is to require undertakings in settlement orders in data privacy matters to extend for 20 years. Following the suggestion of the American Bar Association, Commissioner Wilson argued that FTC orders in data privacy settlements should sunset after only 10 years. The tenor of Commissioner Wilson's comments suggest that the FTC is unlikely to change its practice anytime soon, but nonetheless her comments provide ammunition to respondents during settlement negotiations to argue for a shorter period of time. Of course, particularly in the fast-moving technology sector, even 10 years of dated security requirements and third-party assessments may still feel like an onerous burden for a company.

[4] https://www.ftc.gov/system/files/documents/cases/2019-03-19_idressupclixsense_statement_final.pdf.

[5] https://www.ftc.gov/system/files/documents/public_statements/1553676/162_3130_infotrax_concurring_statement_cw_11-12-2019.pdf.