AN A.S. PRATT PUBLICATION
JANUARY 2018
VOL. 4 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 | NUMBER 1 | JANUARY 2018

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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [4] (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

(2018–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, 718.224.2258. 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.

Cybersecurity: New Front for Attacks on Franchise Model

By Gary R. Duvall*

Recent cases holding franchisors liable for franchisees' data breaches are creating a dilemma for franchisors. This article provides tips on how to help franchisees protect customer data while not unduly creating liability risk for the franchisor.

Much has been written on the growing risks of data breaches and other cyberattacks, especially after the massive security breach at Equifax in September 2017. Recent cases holding franchisors liable for franchisees' data breaches are creating a dilemma for franchisors. This article provides tips on how to help franchisees protect customer data while not unduly creating liability risk for the franchisor.

THE *AARON'S* CASE

In *Michael Peterson, et al v. Aaron's, Inc., et al.*,[1] a franchisor was held liable for breach of consumer privacy by its franchisees. Aaron's and its franchisees rent equipment, including computer equipment. Aaron's franchisees installed computer-monitoring software in computers available for rent to consumers. According to the Federal Trade Commission ("FTC") press release, the software "surreptitiously tracked consumers' locations, captured images through the computers' webcams" and captured users' login credentials, all without the knowledge of the consumer. The software allowed the franchisees to disable a computer remotely. According to the complaint, "Aaron's franchisees used this illicitly gathered data to assist in collecting past-due payments and recovering computers after default."

The FTC found that Aaron's—by "enabling their franchisees to use this invasive software"—was itself in violation of the consumer's rights, and had violated the FTC rules against deceptive practices, even though this software was not used in any of the company-owned stores. While Aaron's did not use this technology in its company-owned stores, the FTC determined that Aaron's "knowingly assisted its franchisees" in implementing and using this software. Specifically, Aaron's: (1) allowed its franchisees to access the software designer's website to use the software; (2) used its server to transmit and store content from the monitoring: (3) provided franchisees with software technical support. The FTC Consent Order prohibited Aaron's, among other things, from collecting or using customer data without their consent.

---

* Gary R. Duvall is a partner at Dorsey & Whitney LLP preparing franchise, hotel management, license, and distribution documents and counseling clients in dispute resolution. He may be reached at duvall.gary@dorsey.com. His colleagues Chris Koa and Josh Piper can be reached at koa.chris@dorsey.com and piper.josh@dorsey.com, respectively.

[1] U.S. District Court, N.D. Georgia, ¶15,562, (Jun. 4, 2015).

This case illustrates that "bad facts make bad law." This monitoring software seemed to have clearly violated consumer privacy expectations. The franchisor did more than specify a third party supplier, it participated in support for the software. Therefore, the case also stands for the proposition that a franchisor is liable for the acts of a franchisee where the franchisor participates. Of course, a franchisor should just say no when it learns of franchisee practices that are clearly illegal or wrong. However, franchisors must be careful to not have too much involvement in a franchisee's privacy and security policies, to avoid being held liable for franchisee-caused problems. Best practices are summarized at the end of this article.

Accordingly, franchisors may wish to review their policies related to privacy and security, and their instructions and principles for franchisees, including any ongoing monitoring and auditing. Moreover, a franchisor should use a privacy officer or outside consultant with adequate expertise and training to assess information gathering activities of both the franchisor and the franchisees to reduce the risks of non-compliance with laws and of data breaches.

THE *WYNDHAM* CASE

FTC v. Wyndham Worldwide Corporation, et al.,[2] is another case in which a franchisor was alleged to be liable for technology practices of franchisees, in this case data security breaches. However, unlike *Aaron's* the underlying practices were not obviously wrongful.

Wyndham's franchisee was hacked in Phoenix in 2008, by sophisticated criminal hackers, who obtained hotel level consumer credit card numbers. Wyndham's systems were accessed, but information was lost only from the franchisee. Wyndham had an incident response plan that involved immediately hiring forensic experts, notifying affected employees, franchisees, customers, credit card companies, and government agencies. The credit card companies offered consumers credits for any fraudulent charges, so no consumer was harmed.

However, in April 2010 the FTC began to investigate, alleging that the franchisor had unreasonable practices, and alleging that the franchisor was taking responsibility for all 7000 franchisees' data practices. In July 2010, Wyndham refused to sign the FTC's proposed consent order, so the FTC filed a lawsuit. The FTC cited Wyndham for nine practices that did not meet the FTC's standards.

All of the consumer information was stolen at franchisee level. The FTC wanted to hold the franchisor liable for the alleged information security deficiencies of the franchisee. The franchisor's defense was that it had no duty for franchisee's security breach.

[2] U.S. Dist. Ct., D. N.J., ¶15,249, 10 F. Supp. 3D602 (Apr. 7, 2014).

The U.S. Court of Appeals for the Third Circuit decided against Wyndham on two ancillary matters, but agreed that there needed to be more than inconvenience to consumers. Thereafter, Wyndham and the FTC settled in 2015, and signed a Consent Order. The FTC dropped its theory of liability of the franchisor for franchisee data breach in this Consent Order. In the Consent Order Wyndham must maintain certain standards for payment card data security.

DOS AND DON'TS FOR FRANCHISORS

- Do say no when a franchisor learns of franchisee privacy and data security practices that are clearly illegal or wrong.
- Do provide third party training and support to franchisees related to privacy and data security from competent and reputable experts. For example, a franchisor can refer franchisees to third party trainers and cybersecurity experts to maintain payment card compliance.
- Don't have too much involvement in a franchisee's privacy and security policies, to avoid being held liable for franchisee-caused problems. Only if the franchisor has the expertise (or hires it) should it try to manage a franchisee's data collection and protection.
- Do provide franchisees with information on what they must do if there is a data breach, and have in place a franchisor data breach incident response plan as well. Such plans are governed by state and federal law, so consult a privacy lawyer to implement such a plan.