AN A.S. PRATT PUBLICATION
JULY-AUGUST 2019
VOL. 5 • NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 NUMBER 6 JULY-AUGUST 2019

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 [171] (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. Kenigsberg
Senior Counsel, Rivkin Radler LLP

David C. Lashway
Partner, Baker & McKenzie LLP

Craig A. Newman
Partner, Patterson Belknap Webb & Tyler 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 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.

Data Breach Standing: U.S. Supreme Court Declines to Revisit Data Breach Injury Debate

Jenny R. Buchheit, Derek R. Molter, Stephen E. Reynolds, and Christian Robertson*

In data security litigation, standing remains a significant threshold issue. Litigants continue to debate whether a data breach or unauthorized disclosure alone constitutes sufficient injury to confer standing. Although the circuits are split, the Supreme Court has yet to provide additional clarification. However, recent appeals indicate the growing pressure on the Supreme Court to revisit the data breach standing issue. The authors of this article discuss the issue.

The U.S. Supreme Court has twice declined to revisit a highly contested issue common in data security litigation: Whether a data breach or unauthorized disclosure, without more, constitutes an injury sufficient for standing to sue? The Supreme Court's recent decision to remand in *Frank v. Gaos*,[1] and subsequent refusal to decide the issue in *Zappos.com, Inc. v. Stevens, Theresa, et al.*,[2] indicates not only its reluctance to review this issue, but also the growing pressure on it to do so.

DATA BREACH STANDING OVERVIEW

Standing to sue is a doctrine rooted in our constitutional understanding of a "case or controversy."[3] The doctrine limits the category of litigants who can sue in federal court to seek redress for a legal wrong. To show standing, litigants must (1) have suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.[4]

For plaintiffs suing after a data breach, proving injury in fact can be difficult. Between the three elements, injury in fact has been the primary focus in data breach standing disputes. In particular, litigants debate whether a mere breach of someone's personal data—without evidence of the subsequent misuse of that data—satisfies the injury in fact element. Plaintiffs previously argued that the unauthorized use of consumer data automatically constitutes injury, if the act violates a statutory right. For example, in cases where a statute prohibits the unauthorized disclosure of data and provides victims

* Jenny R. Buchheit (jenny.buchheit@icemiller.com) is senior counsel, Derek R. Molter (derek.molter@icemiller.com) and Stephen E. Reynolds (stephen.reynolds@icemiller.com) are partners, and Christian Robertson (christian.robertson@icemiller.com) is an associate, at Ice Miller LLP.

[1] *Frank v. Gaos*, 586 U.S. —— (March 20, 2019).

[2] *Zappos.com, Inc. v. Stevens, Theresa, et al*, —— U.S. ——, (March 25, 2019).

[3] *See* U.S. Const. art. 3, § 2, cl. 1.

[4] *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560, 112 S.Ct. 2130, (1992).

with a right to sue when the statute is violated, plaintiffs previously argued that violating such statute automatically satisfied the injury in fact requirement.

In 2016, however, the Supreme Court rejected this argument in *Spokeo v. Robbins* by finding that "standing requires a concrete injury even in the context of a statutory violation."[5] In essence, the Supreme Court held that more was required to show the plaintiff suffered an injury in fact.

Since *Spokeo*, federal district and appellate courts have been split on whether data breaches or unauthorized disclosures alone satisfy the injury prong of standing.[6] The U.S. Courts of Appeals for the Ninth, Sixth, Seventh, and D.C. Circuits have all found that a mere data breach may be a sufficient injury, for purposes of standing, if the breach results in an "increased risk of future harm" even without evidence of actual financial loss.[7] Conversely, the U.S. Courts of Appeals for the Fourth and Eighth Circuits have found that a mere increased risk of future harm, without more—such as an actual financial harm—is not enough to confer standing.[8] Notwithstanding this circuit split, the Supreme Court has appeared reluctant to revisit this issue.

SUPREME COURT REAFFIRMS *SPOKEO* INJURY IN FACT STANDARD IN *FRANK*

On March 20, the Supreme Court reiterated its ruling in *Spokeo* that a statutory right to sue does not automatically prove injury in fact. In *Frank v. Gaos*, the Supreme Court vacated the Ninth Circuit's decision concerning a settlement for Google's unauthorized disclosure of consumer data and remanded the case for the lower courts to determine whether the plaintiffs had in fact showed injury necessary to confer standing.

The case arose from a class action brought against Google for allegedly violating the Stored Communications Act ("SCA") by sharing individuals' search terms with websites the individuals visited. Google argued before the lower courts that the plaintiffs failed to show any injury resulting from the SCA violation notwithstanding the statutory right to sue provided under the Act. Both the district court and Ninth Circuit

---

[5] *See Spokeo, Inc. v. Robbins*, —— U.S. ——, 136 S.Ct. 1540, 1544 (2016).

[6] *See Kuhns v. Scott*: Eighth Circuit Court of Appeals Weighs in on Standing for Data Breach Class Actions and *Attias v. CareFirst*: D.C. Court of Appeals Weights in on Standing for Data Breach Class Actions.

[7] *See In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018); *see also Galaria v. Nationwide Mut. Ins. Co.*, 663 Fed. App'x. 384 (6th Cir. 2016); *see also Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015); *see also Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017).

[8] *See In re SuperValu, Inc.*, 870 F.3d 763 (8th Cir. 2017); *see also Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), cert. denied sub nom. *Beck v. Shulkin*, —— U.S. ——, 137 S.Ct. 2307, 198 L.Ed.2d 728 (2017).

disagreed and found that the SCA automatically satisfied the injury in fact requirement by granting a statutory right to sue when violated.

After accepting the appeal on a separate issue, the Supreme Court found the lower courts had erred by relying on a pre-*Spokeo* ruling which provided standing automatically under a statutory right to sue. In vacating the lower court's decision, the Supreme Court explained that, under the *Spokeo* standard, a mere statutory grant to vindicate one's rights under the SCA did not satisfy the injury in fact standing requirement.

SUPREME COURT REJECTS REVIEW OF DATA BREACH INJURY IN *ZAPPOS*

Five days after its decision in *Frank*, the Supreme Court declined to review the Ninth Circuit's ruling in *Zappos.com, Inc. v. Stevens, Theresa, et al.* In *Zappos*, plaintiffs brought a class action against the online company for privacy breaches resulting from hackers gaining access to and allegedly stealing over 24 million online customers' names, email addresses, billing and shipping addresses, phone numbers, credit card numbers, and passwords. Many of the plaintiffs, however, claimed they were harmed by the hacking incident itself without showing any subsequent misuse of their data.

At trial, Zappos argued the plaintiffs lacked standing to sue, because they had failed to show any concrete injury in fact, such as financial loss. However, the district court and the Ninth Circuit found the "increased risk of future harm" resulting from the data breach was sufficient to establish injury and confer standing.

On March 25, having considered Zappos's appeal, the Supreme Court declined to review the data breach injury issue and to resolve the circuit split.

CONCLUSION

In data security litigation, standing remains a significant threshold issue. Litigants continue to debate whether a data breach or unauthorized disclosure alone constitutes sufficient injury to confer standing. Although the circuits are split, the Supreme Court has yet to provide additional clarification since its 2016 decision in *Spokeo*. However, the recent appeals in cases like *Frank* and *Zappos* indicate the growing pressure on the Supreme Court to revisit the data breach standing issue.