AN A.S. PRATT PUBLICATION
OCTOBER 2020
VOL. 6 • NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 **NUMBER 8** **OCTOBER 2020**

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 [245] (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 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.

Statutory Privacy Claims After *Spokeo*: Shaky Ground or Clear Path for Standing?

By Brian I. Hays, Taylor Levesque, and Molly McGinnis Stine [*]

In this article, the authors examine how several circuit courts of appeals have applied the U.S. Supreme Court's Spokeo *ruling to various privacy and cyber claims.*

Following *Spokeo, Inc. v. Robins*,[1] lower courts across the country were tasked with applying the Supreme Court's "concrete" injury standard to a wide range of privacy and cyber claims. These claims range from the improper retention of personally identifying information to the exposure of client or customer data after a breach.

Regardless of the type of claim or the factual allegations, the lack of a bright-line rule has forced lower courts to analyze standing resulting from technical statutory violations on a case-by-case basis. This case-specific analysis has created circuit splits that will likely continue unless and until a clear-cut rule is articulated by the Supreme Court.

THE FLEXIBLE "CONCRETE" INJURY STANDARD

In *Spokeo*, the Supreme Court noted that "Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing."[2] Thus, while a statute may provide a private right of action, the plaintiff must still prove that there was a concrete and particularized harm to establish standing. The Supreme Court stated that "'[c]oncrete' is not . . . necessarily synonymous with 'tangible[;]'" intangible injuries – and particularly those that Congress has elevated to be a legally cognizable injury – can also be concrete.[3] In other words, merely the "risk of real harm" may be sufficient to satisfy the "requirement of concreteness."[4]

The major effect of *Spokeo*'s flexible standard has been the inconsistent opinions coming out of lower courts. Both plaintiffs and defendants have found support for their arguments that there is, or is not, standing. This is clearly evident in privacy and cybersecurity litigation, and particularly in class actions, where plaintiffs often allege statutory violations and cite to the "risk" of real harm. We consider four of a number of recent cases.

---

* Brian I. Hays, a partner in the Chicago office of Locke Lord LLP, is chair of the firm's Telephone Consumer Protection Act ("TCPA") Litigation and Compliance Section. Taylor Levesque is an associate in the firm's Dallas office. Molly McGinnis Stine, a partner in the firm's Chicago office, is co-chair of the firm's Privacy & Cybersecurity Practice Group. The authors may be contacted at bhays@lockelord.com, taylor.levesque@lockelord.com, and mmstine@lockelord.com, respectively.

[1] *Spokeo, Inc. v. Robins*, ___ U.S. ____, 136 S. Ct. 1540 (2016).

[2] *Id.* at 1548 (quoting *Raines v. Byrd*, 521 U.S. 811, 820 n.3 (1997)).

[3] *Id.* at 1549.

[4] *Id.*

ELECTRONIC COMMUNICATIONS PRIVACY ACT; CALIFORNIA INVASION OF PRIVACY ACT

Campbell v. Facebook (9th Cir. 2020)

In *Campbell v. Facebook*, the plaintiff alleged that Facebook violated the Electronic Communications Privacy Act ("ECPA") and the California Invasion of Privacy Act ("CIPA") through the nonconsensual capturing, reading, and use of website links included in private messages sent or received by users.[5] In its March 3, 2020 opinion relating to a proposed class settlement, the U.S. Court of Appeals for the Ninth Circuit determined, in finding standing, that when "a statutory provision identifies a substantive right that is infringed any time it is violated, a plaintiff bringing a claim under that provision 'need not allege any further harm to have standing.'"[6] As to ECPA and CIPA, the Ninth Circuit stated that "[t]he harms protected by these statutes bear a 'close relationship' to ones that have 'traditionally been regarded as providing a basis for a lawsuit.'"[7]

The Ninth Circuit's analysis reveals that post-*Spokeo*, lower courts will look at the alleged statutory violation of a right to privacy in light of the privacy protections available at common law. Specifically, the Ninth Circuit explained that in the years since *Spokeo*, the circuit court has "identified several statutory provisions that guard against invasions of concrete privacy interests."[8] Legislation that proscribes harm for which there has historically been a basis for a lawsuit is more likely to meet the Article III standard for concrete harm.

Thus, as long as a party claims a violation of concrete privacy interests such as those protected under ECPA and CIPA, the Ninth Circuit says nothing more is needed to support standing.[9]

---

[5] *Campbell v. Facebook, Inc.*, 951 F.3d 1106 (9th Cir. 2020).

[6] *Id.* at 1117 (9th Cir. 2020) (quoting *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983-84 (9th Cir. 2017)).

[7] *Id.* (quoting *Spokeo*, 136 S. Ct. at 1549).

[8] *Id.*; *see, e.g.*, *In re Facebook, Inc. Internet Tracking Litigation*,956 F.3d 589 (9th Cir. 2020) (federal Wiretap Act, federal Stored Communications Act, and California Invasion of Privacy Act); *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1269, 1271-75 (9th Cir. 2019) (Biometric Information Privacy Act); *Eichenberger*, 876 F.3d at 981, 983-84 (Video Privacy Protection Act); *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1041-43 (9th Cir. 2017) (Telephone Consumer Protection Act).

[9] *See also In Re Google Referrer Header Privacy Litigation*, Case No. 5:10-cv-04809-EJD (N.D. Cal., Jun. 5, 2020) (court denied Rule 12(b)(1) motion to dismiss, citing *Campbell* and other Ninth Circuit authority, and stated that ECPA created "a concrete privacy interest in communications stored with electronic communication service providers – even if those communications cannot be linked to the user." (at p. 12)).

ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT

Bryant v. Compass Group USA Inc. (7th Cir. 2020)

On May 5, the U.S. Court of Appeals for the Seventh Circuit applied *Spokeo* in *Bryant v. Compass Group USA Inc*.[10] In *Bryant*, the plaintiff alleged that a vending machine owner and operator violated Section 15(b) of the Illinois Biometric Information Privacy Act ("BIPA") by collecting her fingerprint to enable the purchase of items without obtaining her written consent.[11]

In its opinion, the Seventh Circuit relied heavily upon a rubric outlined by Justice Thomas' concurrence in *Spokeo* – a distinction between the vindication of "private" and "public" rights.[12] Consequently, the Seventh Circuit determined that the "[plaintiff] was asserting a violation of her own rights – her fingerprints, her private information – and that this is enough to show injury-in-fact without further tangible consequences."[13]

In reaching this conclusion, the Seventh Circuit declined to follow the U.S. Court of Appeals for the Second Circuit's holding in *Santana v. Take-Two Interactive Software*.[14] Evaluating similar allegations of failure to secure informed consent before collecting biometric data, the Second Circuit concluded that "none of the alleged procedural violations raised 'a material risk of harm' to a plaintiff's interest in 'prevent[ing] the unauthorized use, collection, or disclosure of an individual's biometric data.'"[15]

In contrast to *Santana*, the Seventh Circuit found that the plaintiff in *Bryant* alleged more than a mere procedural violation and analogized the defendant's actions to an act of trespass. The Seventh Circuit also evaluated the allegations as a "type of informational injury."[16] From this perspective, the Seventh Circuit concluded that a "concrete" injury existed. Specifically, the circuit court stated that "injury inflicted by nondisclosure is concrete if the plaintiff establishes that the withholding impaired her ability to use the information in a way the statute envisioned."[17]

---

[10] *Bryant v. Compass Group USA Inc.*, 958 F.3d 617 (7th Cir. 2020).

[11] BIPA is a 2008 statute of Illinois' General Assembly that created a right to privacy in and control over an individual's biometric identifiers and biometric information. *See* Illinois Biometric Information Privacy Act (eff. 10-03-08), *available at* https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57%E2%80%8E.

[12] *Bryant*, 958 F.3d at 624.

[13] *Id.*

[14] *Id.* at 623 (declining to follow *Santana v. Take-Two Interactive Software, Inc.*, 717 F. App'x 12 (2d Cir. 2017) (summary order)).

[15] *Id.* (quoting *Santana*, 717 F. App'x at 15).

[16] *Id.* at 624.

[17] *Id.*

TELEPHONE CONSUMER PROTECTION ACT

Gadelhak v. AT&T Services, Inc. (7th Cir. 2020); *Salcedo v. Hanna* (11th Cir. 2019)

A circuit split has developed over the impact of *Spokeo* on a plaintiff's standing to bring a claim under the Telephone Consumer Protection Act ("TCPA").

In *Gadelhak v. AT&T Services, Inc.*,[18] the Seventh Circuit addressed the question of whether the receipt of a single unwanted text message caused a concrete injury. The Seventh Circuit noted that *Spokeo* instructed courts to look to both history and Congress's judgment to determine whether an intangible harm protected by a statute has a close relationship to a harm that has traditionally been regarded as providing a basis for suit under the common law.[19] The Seventh Circuit followed prior decisions from the Ninth and Second Circuits and held that the receipt of one or two text messages was sufficiently analogous to the common law claim for intrusion upon seclusion to create standing.[20] The Seventh Circuit acknowledged that at common law, courts required a substantial imposition on the privacy of the plaintiff from many calls.

However, the court reasoned that when *Spokeo* instructed courts to analogize to harms recognized by the common law, courts were only meant to look for a "close relationship" in kind, not degree. Congress has the power to "elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law."[21]

In reaching its decision, the Seventh Circuit rejected the U.S. Court of Appeals for the Eleventh Circuit's holding in *Salcedo v. Hanna*.[22]

In *Salcedo*, the Eleventh Circuit held that the receipt of a single text message advertisement did not create standing. The Eleventh Circuit noted that the text and legislative history of the TCPA is completely silent on the subject of text messages. The Eleventh Circuit also noted that Congress failed to include text messaging in any of the amendments to the TCPA over the years.[23] The Eleventh Circuit found that the common law claim for intrusion upon seclusion was not sufficiently analogous to the harm the TCPA was intended to protect when it came to cell phones.

---

[18] *Gadelhak v. AT&T Services, Inc.*, 950 F.3d 458 (7th Cir. 2020).

[19] *Id.* at 462 (quoting *Spokeo*, 136 S.Ct. at 1549).

[20] *Id.* at 462-63 (following *Melito v. Experian Mktg. Sols., Inc.*, 923 F.3d 85, 92-93 (2d Cir. 2019) and *Van Patten*, 847 F.3d at 1042-43).

[21] *Id.* (quoting *Spokeo*, 136 S.Ct. at 1549).

[22] *Id.* (rejecting *Salcedo v. Hanna*, 936 F.3d 1162, 1172 (11th Cir. 2019)).

[23] *Salcedo*, 936 F.3d at 1168-69.

In support of this conclusion, the Eleventh Circuit cited to the Restatement (2d) of Torts § 652B for the rule that "only when the telephone calls are repeated with such persistence and frequency as to amount to a course of hounding the plaintiff."[24] The Eleventh Circuit also noted that intrusion upon seclusion requires an intrusion upon the solitude or seclusion of an individual or his private affairs or concerns from such things as eavesdropping, wiretapping or looking through someone's personal papers.[25]

After assessing the qualitative harm, not the quantitative harm, from receiving a text message solicitation, the Eleventh Circuit concluded that receiving one text messages was not the kind of harm that constitutes injury in fact.[26] The court left open the question of whether the receipt of multiple unwanted and unsolicited text messages could create standing.

CONCLUSION

In light of the emerging circuit splits, plaintiffs are seeking and will likely continue to seek out specific jurisdictions they believe analyze standing in a way that appears favorable. Such litigants already include some people seeking relief under as yet untested statutes, such as the California Consumer Privacy Act ("CCPA"). However, the case-specific and statute-specific nature of most courts' analysis means that forum selection does not guarantee victory.

Until the Supreme Court provides further guidance, the only certainty is that district courts and circuit courts will continue to be most heavily influenced by the specific facts of each case, including the language of particular statutes, the severity of the incident, the amount and sensitivity of information collected, and the risks of future harm.

---

[24] *Id.* at 1171 (quoting Rest. (2d) Torts § 652B cmt. d).
[25] *Id.* (citing Rest. (2d) Torts § 652B cmt. b).
[26] *Id*. at 1173.