AN A.S. PRATT PUBLICATION
JUNE 2017
VOL. 3 • NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 | NUMBER 5 | JUNE 2017

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 [159] (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

(2017–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.

Plaintiffs Face Challenges in Cellular Phone Application Privacy Litigation

By Michael J. Stortz, Justin O. Kay, and Jessica R. Medina*

The authors discuss challenges under the Wiretap Act.

A district court in the Northern District of California recently granted in part and denied in part a motion to dismiss a claim brought against three entities (including the Golden State Warriors) in a first-of-its-kind case testing the applicability of the Electronic Communications Privacy Act[1] (the "Wiretap Act") to smartphone apps.

SATCHELL V. SONIC NOTIFY, INC.

In *Satchell v. Sonic Notify, Inc.*,[2] the plaintiff, a Golden State Warriors fan, alleged that the team's mobile application (the "App"), developed by Yinzcam, recorded her conversations without her knowledge or consent, in violation of the Wiretap Act. According to the plaintiff, the Warriors partnered with Signal360 "to integrate Signal360's beacon technology" into the App, which provides users with scores, statistics, schedules, and news about the team. The "novel beacon technology" allows companies to provide consumers with targeted advertisements, promotions, and contents "by determin[ing] a consumer's precise location by listening for nearby Signal360 audio beacons" using the microphone on the consumer's smartphone. According to plaintiff, "Defendants programmed the App to instantly turn on the consumer's Microphone," and the App "listens to and records *all* audio within range—including consumer conversations" until the consumer closes the App or turns off the smartphone. The plaintiff further alleged that although "the App asks for certain permissions," including a request to use the device's microphone, defendants do not inform consumers that the "App uses audio beacon technology that surreptitiously turns on consumers' smartphone microphones and listens in." The plaintiff's complaint alleged that "because Plaintiff carried her smartphone to locations where she would have private conversations and the App was continuously running on her phone, Defendants [sic] App listened-in to private oral communications" without her consent or knowledge, violating the Wiretap Act.

---

* Michael J. Stortz (michael.stortz@dbr.com) is partner at Drinker Biddle & Reath LLP defending companies against claims of unfair competition, false advertising, consumer fraud, breach of warranty and product defect, and claims arising under the Telephone Consumer Protection Act. Justin O. Kay (justin.kay@dbr.com) is a partner at the firm defending complex civil matters in federal court, state court, and before federal agencies. Jessica R. Medina (jessica.medina@dbr.com) is an associate at the firm assisting corporate and nonprofit clients in litigating complex cases.

[1] 18 U.S.C. § 2510, et seq.

[2] 16-4961 (N.D. Cal.).

On November 1, 2016, each of the defendants moved to dismiss the complaint. According to the defendants, the plaintiff lacked Article III standing because her alleged injury—the wear and tear, battery consumption, and diminished use and enjoyment of her smartphone—is not a concrete injury-in-fact. Moreover, and in any event, the defendants argued that the plaintiff failed to state a claim for violation of the Wiretap Act, which provides a private right of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter."[3] The defendants argued that the plaintiff failed to allege facts demonstrating an "interception" of an "oral communication," within the meaning of the Act. Specifically, the defendants argued that because the complaint merely alleged that the App temporarily recorded audio that remained on the plaintiff's phone, the plaintiff failed to establish an "interception," which requires as a matter of law an "acquisition" or "coming into possession" of the contents of an oral communication. Further, the defendants argued that the plaintiff's claim of an alleged unlawful "use" also failed because the defendants did not "use" the contents of the plaintiff's communications, and instead, Signal360's beacon signals are the only audio data "used" by the App.

Judge Jeffrey White denied the defendants' motions to dismiss for lack of standing. According to the court, the intangible harm associated with invasion of the plaintiff's right to privacy was enough to show injury-in-fact, and to confer Article III standing. However, the court did grant the defendants' motions for failure to state a claim. The court found that the plaintiff failed to allege facts showing that either Yinzcam or the Warriors had "intercepted" an oral communication within the meaning of the Act.

As to Signal360, the court found that the plaintiff's allegations that Signal360 designed its beacon technology to turn on a smartphone's microphone and record were sufficient to allege that Signal360 "intercepted" the plaintiff's communications. The court nevertheless found that the plaintiff failed to allege facts sufficient to show that *any of the defendants* intercepted an "oral communication," because she offered only conclusory allegations that she carried her smartphone with her to places where she would have private conversations.

Finally, the court concluded that the plaintiff failed to state a claim based on "use" since she failed to allege any facts to show that the contents of her communications (as opposed to the beacon signals) were used to send her targeted advertising. The court granted the plaintiff leave to amend her complaint by March 13, 2017.

The plaintiff filed her first amended complaint on March 13, 2017. In her amended complaint, the plaintiff seeks to bolster her claims for violation of the Wiretap Act with 22 additional paragraphs of allegations, including four examples of private conversations that she claims she had while her phone was with her and the App was on. In

[3] 18 U.S.C. § 2520.

addition, the amended complaint alleges that the App was "bugged," and that the "Bug" can be used to intercept oral communications through users' mobile devices.

On April 10, 2017, each of the defendants moved to dismiss the amended complaint for failure to state a claim, this time with prejudice. The defendants argue that the plaintiff has again failed to allege an interception, since she has not alleged any facts to show that any defendant ever acquired the contents of her private conversations. In addition, the defendants argue that the plaintiff's amended complaint is more accurately understood as a claim of improper "manufacture[]" and "assembl[y]," which is barred by the Wiretap Act's limited civil remedy provision. The defendants' motions are set to be heard on June 16, 2017.

RACKEMANN V. LISNR, INC. ET AL.

The Indianapolis Colts are contending with substantially similar allegations in a putative class action initially filed in the District of Massachusetts, and later transferred to the Southern District of Indiana on defendants' motion. In this action, *Rackemann v. LISNR, Inc. et al.*,[4] the plaintiff, a user of the Indianapolis Colts' official application, claims that the Colts, along with the application developer (Adept Mobile, LLC) and another developer of the "beacon technology" used in the application (LISNR, Inc.), also violated the Wiretap Act by surreptitiously recording application users' personal communications. The defendants have moved to dismiss on the same grounds as the *Satchell* defendants. Briefing on the defendants' motions is concluded. Judge Virginia Kendall has preliminarily approved a settlement in another similar case pending in the Northern District of Illinois.[5] The case is stayed pending final approval, which is set for hearing on August 7, 2017.

IN RE GOOGLE GMAIL LITIGATION

Meanwhile, Google has been fighting challenges under the Wiretap Act and similar state statutes for over six years. In a series of cases consolidated in the Northern District of California as *In re Google Gmail Litigation*,[6] the plaintiff Gmail users claimed that Google's practice of scanning emails to create ad content violated the Wiretap Act and several state eavesdropping statutes. Judge Lucy Koh deemed the allegations sufficient to survive a motion to dismiss, but refused to certify a class because individualized issues of consent predominated over common facts. After the *Gmail* plaintiffs settled on an individual basis, a new putative class action was filed against Google under the Wiretap Act and the California Invasion of Privacy Act ("CIPA"), this time on behalf

[4] No. 17-624 (S.D. Ind.).
[5] *See N.P. v. Standard Innovation (US), Corp.*, No. 16-08655 (N.D. Ill. 2016).
[6] 13-md-2430 (N.D. Cal.).

of non-Gmail users. In *Matera v. Google Inc.*,[7] Judge Lucy Koh again denied motions to dismiss – both on the merits and on Article III standing. On March 15, 2017, Judge Koh also denied preliminary approval of a class settlement, finding that the proposed notice to class members was inadequate.

HOLLAND V. YAHOO! INC.

Yahoo faced similar challenges to its email processing under the Wiretap Act and CIPA in *Holland v. Yahoo! Inc.*[8] After Judge Koh certified a class of non-Yahoo users, the parties agreed to a settlement under which Yahoo would change its email processing practices and pay $4 million in attorneys' fees. Judge Koh approved a settlement last August.

CONCLUSION

While the ruling on the initial motions to dismiss in *Satchell* is good news for potential defendants, the true test of the viability of claims is now whether the plaintiff has amended her complaint to cure the deficiencies noted by the court. Regardless of the ultimate outcome, the recent filings under the Wiretap Act show that the plaintiffs' bar continues to push the envelope of the class action device and statutory damages of obscure statutes to attack companies that interact with or collect and process consumer information in innovative ways.

[7] 15-4062 (N.D. Cal.).
[8] 13-4980 (N.D. Cal).