Drinker Biddle


December 1, 2017

# App Privacy Claims Based on Federal Wiretap Act Survive Motion to Dismiss

*By Justin O. Kay, Michael J. Stortz and Brendan P. McHugh*

In a closely watched case under the Electronic Communications Privacy Act, 18 U.S.C. §2510, *et seq.* (the "Wiretap Act"), a California district court has held that the plaintiff rectified the shortcomings in her original complaint, and that her claims can now proceed against both the provider of a smartphone application (Signal 360, Inc. f/k/a Sonic Notify, Inc.) and the NBA franchise on whose behalf the application was developed (Golden State Warriors, LLC), but not the app developer (Yinzcam). *See Satchell v. Sonic Notify Inc.*, 16-cv-04961 (N.D. Cal.).

According to the plaintiff, the Warriors organization offers an app that delivers scores, news and other information to fans. The app delivers content based in part on a user's physical location, which is allegedly determined through the use of Signal360's audio beacon technology, which uses radio beacons to emit a unique audio signal that the app captures. But in order for the app to capture that signal, a user's smartphone microphone must be on. The crux of the plaintiff's original complaint was that the app turned the microphone on without her knowledge during private conversations and recorded those conversations in violation of the Wiretap Act, which provides a cause of action "to any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used," absent a statutory exception (e.g., the consent of the parties).

In its decision dismissing the original complaint without prejudice, the court explained that the complaint fell short for three reasons: (1) while she had adequately alleged that Signal 360 "intercepted" a communication, she could not rely on a theory of "concerted action" to take the place of allegations specific to the other defendants; (2) she failed to allege that any of the defendants intercepted any "oral communication" because her allegations that the app intercepted "private conversations" were mere legal conclusions; and (3) she failed to allege that any of the defendants "used" any oral communication because those allegations, too, were mere legal conclusions.

In reviewing the plaintiff's second effort, the court held that the amended complaint sufficiently alleged that Signal360 intercepted oral communications within the meaning of the Wiretap Act by citing four specific instances when the plaintiff's private conversations were purportedly recorded through her smartphone's microphone: conversations between plaintiff and her spouse, discussions at a business meeting, conversations with a loan officer, and conversations with a banker. The court also held that the amended complaint sufficiently alleged a claim against the Warriors based on plaintiff's additional allegations that the Warriors "had access to information generated" by the app. The court, however, again rejected the "concerted action" theory of liability, noting that it "respectfully disagree[d]" with the reasoning in *Rackemann v. LISNR, Inc.*, No. 17-cv-00624-TWP-MJD, 2017 WL 4340349 (S.D. Ind. Sept. 29, 2017)—a similar case involving the Indianapolis Colts.

With regard to Yinzcam, the court dismissed the plaintiff's claims, finding plaintiff's allegations that Yinzcam integrated Signal360's source code into the app and tested the app did not sufficiently allege that Yinzcam had either intercepted an oral communication or "procured" an interception. In so ruling, the court again distinguished the holding in *Rackemann*, stating that in that case, the complaint included more details about how the app functioned and alleged that the developer provided the rules that dictated when the microphone would be activated.

Surviving a motion to dismiss does not mean that the allegations are true, and it remains to be seen whether the allegations can survive summary judgment. The Warriors certainly do not think so—they have described the allegations as "purely fanciful and wholly without merit." That will now be tested in discovery. In the meantime, however, this decision and the decision in *Rackemann* provide a roadmap for plaintiffs and their counsel to plead enough to withstand a motion to dismiss and proceed into discovery. The prospect of a plaintiff poking around in one's technology in discovery, along with the Wiretap Act's draconian damages ($10,000 in statutory damages per violation), should give businesses pause when considering implementing technology that uses smartphone microphones.

# Primary Contacts


**Justin O. Kay**
Partner
Chicago
(312) 569-1381
justin.kay@dbr.com

**Michael J. Stortz**
Partner
San Francisco
(415) 591-7583
michael.storz@dbr.com

**Brendan P. McHugh**
Associate
Philadelphia
(215) 988-2597
brendan.mchugh@dbr.com