BCLP. Client Intelligent

Insights

FEDERAL COURT REJECTS MOTION TO DISMISS WIRETAP CLAIMS USING HIPAA TO SUPPORT CRIME-TORT EXCEPTION ALLEGATIONS

Aug 16, 2024

It has now become commonplace for Plaintiffs' attorneys to bring claims alleging that routine marketing techniques, including the deployment of behavioral advertising cookies and pixels, constitute wiretaps in violation of state and federal wiretap laws passed before the internet came into existence. Adjudication of these claims, especially at the motion to dismiss stage, has been inconsistent at best, but what has been consistent to date is that claims against the website publisher under the Federal Wiretap Act are doomed to fail because the publisher cannot "intercept" their own communications with the website user (i.e., the plaintiff). *See* 18 U.S.C. 2511(2)(d). Plaintiffs attempt to plea around this defense by claiming that the website publisher "aided and abetted" the interception by another third party (usually the pixel/cookie provider). This claim is especially prevalent in two party consent states, like California.

But there is another exception under the Wiretap Act. A party to a conversation can be held liable for an unlawful interception if the interception occurs for the purpose of committing a crime or a tort. *See Caro v. Weintraub, 618 F.3d 94, 97 (2d Cir. 2010)* (citing 18 U.S.C. §§ 2520, 2511(1), 2511(2)(d)). Recently, in *Cooper v. Mount Sinai Health Sys.*, 2024 WL 3586357 (S.D.N.Y. July 30, 2024), a District Court denied a motion to dismiss a wiretap claim by relying on this so-called crime-tort exception, but what is most notable is the criminal statute at issue was the Health Insurance Portability and Accountability Act ("HIPAA"). Specifically, the Court held that the use of a Meta pixel and certain other tracking technologies by a healthcare provider and HIPAA Covered Entity, as alleged by Plaintiff at the motion to dismiss stage, was sufficient to constitute a properly alleged federal crime, and that therefore the Defendant could not avail themselves of the consent exception to the Act. *Id.* at *8 (citing 42 U.S.C. § 1320d-6, "[the allegations] plausibly support the inference that Mount Sinai, for commercial ends, intentionally disclosed individually identifiable patient health information, and thus violated HIPAA, which makes it a crime for a health care provider to disclose individually identifiable health information for commercial gain").

This ruling is particularly concerning because it is as of yet unclear whether any data transmitted by pixels and the like actually constitutes Protected Health Information. Recent guidance from the Department of Health and Human Services has suggested that in some cases such data can

constitute PHI, but that guidance has been challenged in court by the American Hospital Association, among others. The *Cooper* opinion goes a step further than even the HHS guidance, in suggesting that use of common marketing techniques like cookies and pixels can constitute a federal crime, *even when the data is derived from first party data*. All that is required, according to the Court, is an allegation regarding the interception of the data in question and a claim that the website publisher intended to profit from the unlawful disclosure of PHI.

At present, the *Cooper* decision stands as an outlier (and has no precedential weight) but it certainly has the potential to encourage other Plaintiffs to bring similar claims regarding very common marketing practices. Covered Entities under HIPAA in particular should take note of the decision and review marketing practices on digital properties, especially where it is possible that individually identifiable health information could be caught up in other marketing data transmitted to third parties. Such data flows should, if possible, be supported by Business Associate agreements or HIPAA authorizations, although the latter can be very difficult to implement in digital contexts as a practical matter.

Should you have any questions concerning these issues, please do not hesitate to contact the authors below.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Daniel T. Rockey

San Francisco

daniel.rockey@bclplaw.com
+1 415 268 1986
