BLANKROME

Privacy Class Action Defense

AUGUST 19, 2024

Navigating New Theories of Liability: Arizona's Communication Service Records Act

INTRODUCTION

In today's digital landscape, the line between marketing analytics and privacy infringement vis-à-vis state privacy law is increasingly blurred. At the heart of this debate is the use of tracking "pixels"—and the latest claims arise out of analytics software embedded in e-mails to track user behavior. This alert examines the recent uptick in class action lawsuits that pivots on this very issue, whereby plaintiffs sue retailers and others, citing a violation of Arizona's Telephone, Utility, and Communication Service Records Act (A.R.S. § 44-1376). This litigation, primarily concentrated among two plaintiffs' firms, serves as a litmus test for a potential new theory of liability, pitting evolving technology against existing state statutes. As discussed below, standing principles established in *Spokeo, Inc. v. Robins,* 578 U.S. 330 (2016), and *TransUnion LLC v. Ramirez,* 594 U.S. 413 (2021), third-party doctrines articulated in *State v. Mixton,* 250 Ariz. 282 (2021), and other statutory interpretations could provide defenses as courts attempt to balance consumer privacy interests and avoid unintended consequences from applying outdated state laws to modern practices.

BACKGROUND

Using the federal Telephone Records and Privacy Protection Act of 2006 and Arizona's own stringent statute sought to safeguard the sanctity of communication records, plaintiffs are arguing that use of tracking and analytics pixels tied to marketing e-mails—also referred to as deliverability metric software—is an intrusion of privacy that is both unconsented and deceptive in its means. The litigation thus far is concentrated under Arizona's statute, but e-mail pixel claims have also been filed under the federal Telephone Records and Privacy Protection Act of 2006 and California's Invasion of Privacy Act ("CIPA").

THE NEW THEORY OF LIABILITY

The crux of the complaints is that the alleged undisclosed insertion of pixels into marketing e-mails to track when, where, and if they are opened—without the recipients' explicit consent—qualifies as "knowingly procuring communication service records." The litigation advances an innovative lens through which to interpret the existing statute, potentially broadening its application to encompass modern tracking technologies that were not widely considered at the time of the statute's enactment amid increasing concerns surrounding unauthorized disclosure of phone records by telecommunications carriers.

THE DEFENSES' PERSPECTIVE, THUS FAR

Challenging the plaintiffs' contention, at least two retail defendants targeted by these lawsuits have moved to dismiss the complaints, positing two critical arguments: the plaintiff's lack of concrete harm and, therefore, Article III standing, alongside the claim that the Arizona Statute's scope does not encompass e-mail pixels. Defendants have asserted that the statute was a measure aimed at telecommunication carriers that does not provide for a seamless application to

digital marketing strategies. Anchoring their defense on the consent ostensibly given by users through acceptance of the marketer's privacy policy and terms and conditions at e-mail provision or sign up, the defendants seek to delineate the statutory text away from the digital measures employed in their marketing strategies. Through this, defendants put into question both the plausibility of the complaint's new theory of liability and the legitimacy of its legal basis.

LEGAL ANALYSIS

The defense arguments invite a familiar examination of the requisites for standing, hinging on the argument that to the extent the statutorily prescribed interest is analogous to intrusion upon seclusion, the violation must constitute a "highly offensive" injury to a reasonable individual. *Six v. IQ Data Int'l Inc.,* 673 F. Supp. 3d 1040, 1045 (D. Ariz. 2023) (citing Restatement (Second) of Torts § 652B). Defendants allege that a customer's browsing history, viewing activity, or purchasing habits may not constitute personal information or private facts to a sufficient degree that would establish a tangible harm. The pivotal cases of *Spokeo* and *TransUnion* underscore the necessity of tangible harm beyond statutory violation for standing. Indeed, in *Hartley v. Urb. Outfitters, Inc.,*---F.Supp.3d----, 2024 WL 3445004 (E.D. Pa. July 17, 2024), a federal district court recently dismissed the plaintiff's complaint for lack of standing.

Further, parsing the definition of a "communication service record" is crucial, positing that the acquired information does not align with the statutory language and its legislative history. In addition, the Arizona law only prohibits businesses from "procuring" communication service records. If, as the plaintiffs' allegations go, a defendant is using the pixel to create a record while a plaintiff reviews an e-mail, is a record actually being "procured" within the meaning of the statute?

Another potential defense is that the third-party doctrine applies. Arizona courts have noted that the Fourth Amendment does not protect IP addresses and ISP subscriber information because such information falls within the exception created by the "third-party doctrine." *Mixton,* 250 Ariz. at 294. The third-party doctrine is premised on the concept of privacy and holds that a person has no reasonable expectation of privacy in information voluntarily shared with a third party, here, the marketer, particularly at e-mail sign up.

Defendants may also argue that the plaintiffs' civil action is time-barred. Section 44-1376.04 of the Arizona Revised Statutes provides that a civil action under the Telephone, Utility, and Communication Service Records Act may not be commenced more than two years after the date on which the claimant first discovered or had a reasonable opportunity to discover the violation. To the extent the plaintiffs fail to identify the dates on which they opened e-mails, how they discovered that the tracking, or how the company was using any particular pixel at the time of those e-mails, there may be a limitations argument.

IMPLICATIONS FOR PRIVACY AND DIGITAL MARKETING

These cases extend far beyond the confines of legal skirmishes into a broader dialogue about individual privacy in an age where digital marketing software and customer experience depend on key bytes of data. This intersectional friction beckons a necessary reevaluation of both marketing practices and protective legislation on a state-by-state basis. Courts must now grapple with the ever-growing concerns surrounding consumer privacy as well as the potential harms of broadening the application of state statutes that were adopted without modern tracking technologies in mind. So far, most "pixel" tracking cases preceding the recent wave of e-mail pixel cases—whether arising out of analytics technology, targeted advertising tools, or customer service functions—have shown challenges for the plaintiffs insofar as the evidence tends to require expert analysis and testimony to tie the software to the individual, which then needs to translate into enough cohesive facts to convince the courts that certification of classes around theories of invasion of privacy are warranted. This is a tall hill. Regardless, retailers and others who utilize tracking and analytics pixels in their marketing strategies should take additional measures in ensuring all the boxes are checked as these litigation matters move forward.

For more information or assistance, contact Harrison Brown, Ana Tagvoryan, or another member of Blank Rome's Privacy Class Action Defense group.

Harrison Brown
424.239.3433 | harrison.brown@blankrome.com

Ana Tagvoryan
424.239.3465 | ana.tagvoryan@blankrome.com