Privacy Issues: Avoiding the Wrong Side of these Tracks

NORTON ROSE FULBRIGHT

Co-authored by McGriff ERA and Norton Rose

Tags, cookies, pixels, session replay, and online chats. These are the tools of the trade for digital marketing that allow businesses to track, target, and interact with potential customers. Recent trends in the courts, however, suggest that companies need to closely consider how, when, and where they are utilizing these tools. In the last two years, we've seen a significant uptick in consumers attempting to utilize federal and state wiretapping and privacy laws to combat internet tracking tools.

As courts apply privacy laws to the modern software that companies rely on to market themselves to or track the web activities of their online consumers, organizations need to be aware of their risks. If you're heading into a cyber insurance renewal in the next few months or if you are considering purchasing for the first time, you'll want to prepare for new underwriting questions around your organization's utilization of these various customer engagement and tracking tools. You'll also want to be sure your organization is complying with privacy laws and ensure oversight of your vendor's compliance.

Tags, Cookies, and Pixel Tracking

Tag, cookie, or pixel tracking occurs when organizations embed (or allow third-parties to embed) certain code on their websites that discretely collects and sends user information for an organization's own use or a marketing partner's use. Between February and September of 2022, almost 50 class actions were filed claiming that Meta's pixel-tracking tool sent consumers' personal video consumption data from online platforms to Facebook without their consent, a violation of the federal Video Privacy Protection Act. Class action lawsuits have also been filed in multiple states against healthcare organizations alleging illegal sharing of sensitive patient information with Facebook, Instagram, and other third-parties for advertising or consumer engagement purposes in violation of the federal Wiretap Act and state analogue laws (*e.g., In re Advoc. Aurora Health Pixel Litig.*, 2023 WL 2787985 (E.D. Wis. Apr. 5, 2023); *In re Meta Pixel Healthcare Litig.*, 2022 WL 17869218 (N.D. Cal. Dec. 22, 2022)). The consumer privacy concerns and litigation are not limited to healthcare. Indeed, businesses that employ tags, cookies, or pixel tracking on their website to monitor consumer activity—irrespective of industry—may face an increased risk of drawing consumer litigation (*e.g., Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121 (3d Cir. 2022) (retail); *Stark v. Patreon, Inc.*, 2023 WL 2090979 (N.D. Cal. Feb. 17, 2023) (ecommerce)).

Session Replay

The use of session replay software is also being challenged in courts for allegedly violating privacy laws. Session replay software is often used on websites to record user's behavior, including every click and mouse movement. While the idea behind the software is to improve a user's digital experience and provide targeted advertising more effectively, its use has been the subject of lawsuits, particularly in states that require all-party consent (*i.e.*, consent by both the user and the website owner) for recording or capturing communications (*e.g., Makkinje v. Extra Space Storage, Inc.*, 2022 WL 80437 (M.D. Fla. Jan. 7, 2022); *Hazel v. Prudential Fin., Inc.*, 2023 WL 3933073 (N.D. Cal. June 9, 2023)).

Online Chat Functions

Most of us have encountered offers to engage with online retailers and other service providers via the “chat” feature that allows the business to address customer service questions more efficiently rather than directing the customer to make a phone call or send an email. Many of these chat tools use automated chatbot technology that often collects basic information about the customer, the product being purchased, the order number, and other specifics to assist in handing the inquiry or complaint. Like session replay, data collected and saved through these online chat functions is kept in logs that businesses use to optimize overall customer experience. There has also been a marked increase in class action lawsuits against companies that employ and record online chats, where consumers are asserting similar claims for alleged privacy violations under state and federal law (*e.g., Byars v. Goodyear Tire & Rubber Co.*, 2023 WL 1788553 (C.D. Cal. Feb. 3, 2023)).

Cyber Underwriting Questions

As you head into a cyber insurance renewal or if you are considering purchasing for the first time, it's likely you will receive questions about your organization's utilization of these various customer engagement and tracking tools and how your organization is complying with privacy laws as well as your oversight of your vendor's compliance.

Common questions include:

- Have you conducted an analysis of your website's use of tags, cookies, or pixels?
- Have you internally assessed the risks of third-party data sharing?
- How does your website collect user content?
- Have you conducted a comprehensive scan of your website(s)?
- Have you reviewed user consents in light of this?
- When adopting new technologies or marketing tools, is a privacy and legal review undertaken as standard practice?

These questions are specifically related to recent issues related to the use of such tracking tools to monitor user activity and share user data. Failure to provide satisfactory responses to these questions will likely result in a policy exclusion for this type of litigation. One carrier adds an exclusion that applies to the breach response, privacy and security liability, media liability and regulatory defense and penalties insuring agreements. It expressly does not cover claims that may arise out of "the use of a pixel, code, or similar technology on a website that transmits or redirects, or causes to be transmitted or redirected, information from an individual to a third-party."

In addition to cyber insurance, companies should review their professional liability, errors and omissions, stand-alone media liability policies, and commercial general-liability coverage. Without definitive exclusions for this new litigation, defense costs and possibly judgments or settlements may be covered to some degree, depending upon the allegations in the complaint. If your organization receives a demand or complaint for invasion of privacy, it is best practice to notify all insurance policies that may contribute to loss and/or defense costs, subject to the notification provisions and other conditions in each of the policies.

Final Thoughts

So far, it is too early to determine what frameworks lower courts will use to apply state and federal privacy laws to the many digital tools companies rely on to market to online consumers. Uncertainty and risk will likely continue until appellate courts start weighing in. Privacy violations and resulting lawsuits create a minefield for underwriters as many cyber policies cover legal liability and regulatory investigations for privacy violations beyond those associated purely with an alleged failure in network security or a data breach.

Outside counsel representing clients in these cases are noting that some companies have not thoroughly briefed their Corporate Marketing personnel on the litigation risk these marketing/technology tools present, and the need to adopt conforming best practices in updating their online Privacy Policies. Likewise, some companies are not providing full disclosure to their customers on information collection, securing informed consent from their customers prior to tracking any information, giving website users cookie opt-out options, and maintaining logs on user requests. As a result, organizations need to carefully evaluate how they utilize these tools and assess their data compliance policies, particularly as they consider their cyber insurance coverage and potential for exposure.

For more information, visit McGriff.com or contact:

McGriff

Suzanne Gladle, ARM
SVP, Cyber Practice Leader, ERA
(540) 565-0113
SGladle@McGriff.com

Natalia Santiago, JD
SVP and Claims Manager, ERA
(713) 402-1410
nsantiago@McGriff.com

Lisa Frist, JD
Vice President, ERA
(404) 497-7590
LFrist@McGriff.com

NORTON ROSE FULBRIGHT

Jason K. Fagelman
Head of Dispute Resolution and Litigation, Dallas
(214) 855-8120
jason.fagelman@nortonrosefulbright.com

Patrick Doyle
Associate
(214) 855-7404
Patrick.Doyle@nortonrosefulbright.com