LITIGATION MINUTE: THE NEXT WAVE OF WEBSITE PRIVACY LAWSUITS

PIXEL TOOL LITIGATION SERIES: PART ONE

Date: 15 August 2023

By: Michael J. Stortz, Laura K. Veith

WHAT YOU NEED TO KNOW IN A MINUTE OR LESS

The rise in session replay litigation has paved the way for a new wave of website privacy lawsuits: pixel tool litigation. Plaintiffs have increasingly challenged the use of this technology, such as the Meta Pixel, on consumer-facing websites across a variety of industries—including healthcare, financial services, and online video services.

As with session replay litigation, claims challenging the use of pixel technology typically allege violations of federal and state wiretapping statutes, common law claims such as invasion of privacy, and, in some instances, violations of the federal Video Privacy Protection Act. However, pixel tool litigation presents unique challenges, particularly given the nature of the underlying technology and increased regulatory activity addressing its use in particular contexts.

In a minute or less, here is what you need to know about this litigation trend.

What is a Pixel Tool?

A pixel tool is a small piece of code, installed on a website to measure user interactions with the site and improve online experiences while targeting online advertising. Pixel tools are customizable, enabling website owners to select data to collect, analyze, and share. Pixel tools are often made available to website owners by third parties, who can access and analyze the data collected on behalf of website owners.

Why Does It Matter?

Plaintiffs claim this technology results in the illegal sharing of personal information without consent. While any company using pixel tools may be sued, leading targets thus far have been in industries subject to industry- or field-specific statutes that protect user data. For example, plaintiffs may claim a healthcare website's pixel tool could share data that arguably constitutes personal health information protected by the Health Insurance Portability and Accountability Act (HIPAA). Plaintiffs may further allege that this information is shared not only with the platform providing the pixel tool, but also with advertisers and other third parties, so as to compound the alleged illegal sharing of protected information.

The risk to defendants is significant, as the claims seek statutory damages for each alleged violation, regardless of proof of actual injury. Plaintiffs have sought to leverage this threat through class action lawsuits that

©2005-2026 K&L Gates LLP. All Rights Reserved.

seek aggregated class damages, as well as pre-litigation demand letters and threated mass arbitration campaigns.

What Defenses Are Available?

A number of courts have held that website visitors may consent to the use of pixel tools through online disclosures in privacy policies. Site users also may have consented to data sharing through their accounts with the platforms offering pixel technology. For example, a website visitor with a Facebook account may have provided consent via Meta's Terms of Service and Data Policy.

Even when companies provide disclosures, however, plaintiffs have challenged these as insufficient to constitute valid consent to sharing information, including regulated information such as personal health or financial information. Despite ever-increasing demands for privacy disclosures, regulators and the plaintiffs' bar have criticized online privacy policies as overly dense or confusing to the “reasonable user.”

As a result, preventative measures (such as configuring pixel tools to avoid collecting confidential information) can add a layer of protection to defenses against these claims. Companies should review their privacy policies for disclosures of the website tracking technology, the information collected, and the parties with whom it is shared. If an update is appropriate, the format of the update and notice of the updated policy should conform to regulations dictating the content, format, and placement of privacy notices for users in states with recently enacted comprehensive privacy laws.

What is Next?

In upcoming editions of this series, we will discuss how these pixel lawsuits and claims have been asserted in specific industries. Broadly speaking, however, every company with a public-facing website deploying pixel technology—regardless of industry—should carefully review its related privacy policies and disclosures, evaluate the scope of user consent, and assess whether further configuration may be appropriate to address the potential sharing of confidential or sensitive information.

KEY CONTACTS



MICHAEL J. STORTZ
PARTNER

SAN FRANCISCO
+1.415.882.8011
MICHAEL.STORTZ@KLGATES.COM



LAURA K. VEITH
PARTNER

PITTSBURGH
+1.412.355.7456
LAURA.VEITH@KLGATES.COM

©2005-2026 K&L Gates LLP. All Rights Reserved.

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.