



Wrongful Collection of Data

SUMMARY

Wrongful collection of data refers to the unlawful or unethical gathering of personal information without proper consent, notice, or adherence to data protection laws. This includes instances when individuals have not been informed about data collection, lack the ability to opt out, or when data is shared with third parties without appropriate consent. Websites using "pixels" to track user behavior across other sites without informing users or obtaining consent can constitute wrongful data collection.

Tracking pixels are tiny, invisible image files embedded in web pages or emails, used to collect data about user behavior, such as website visits, email opens, and link clicks. Pixels are commonly used to improve marketing campaigns, optimize website traffic, and measure advertising effectiveness. However, they raise significant privacy concerns due to their potential to collect user data without clear consent or awareness.

LEGAL RISKS & PIXEL TRACKING PITFALLS

Financial institutions facing lawsuits for wrongful data collection may find themselves caught off guard. Without a comprehensive federal privacy law in the United States, what constitutes "wrongful" data collection varies depending on state laws and regulatory guidelines. Given the evolving regulatory and legal environment, businesses may unintentionally mishandle data.

Uses of Tracking Pixels:

- Track ad effectiveness, identify user preferences, and personalize online advertising.
- Analyze website traffic, identify navigation patterns, and optimize user experience.
- Measure email open rates, click-through rates, and identify engaged users.
- Track conversions (e.g., purchases) attributed to specific marketing campaigns.

Privacy Concerns:

- Users are often unaware of pixel tracking, as pixels are invisible and require no interaction.
- Pixels can collect extensive user data, including IP addresses, device types, and locations.
- Data gathered by tracking pixels may be shared with third-party advertisers or marketers without explicit user consent.
- Pixels and similar tracking technologies are vulnerable to breaches, potentially exposing sensitive data.

RISK MITIGATION FOR DATA COLLECTION

To mitigate litigation risk related to data collection, financial institutions should prioritize transparency, security, and consent by clearly communicating their data practices, complying with relevant laws, and securing user data. In addition, financial institutions should also:

- Clearly disclose data collection practices and obtain explicit, affirmative consent before collecting, processing, using, sharing, or selling personal data.
- Limit data collection to only what is necessary for its intended use.
- Provide the ability for users to opt-out of data collection.
- Implement robust security measures to protect data from unauthorized access, usage, disclosure, or modification.
- Stay informed and comply with applicable data privacy regulations and laws.
- Establish strong vendor management practices to ensure third-party compliance with data protection requirements.
- Provide employees with comprehensive training on technology use, data security, and privacy legislation.
- Regularly audit data collection practices and security controls to identify and remediate vulnerabilities.
- Employ a risk-based approach to data privacy compliance, focusing on mitigating significant vulnerabilities.
- Develop clear data governance policies to ensure compliance with legal and ethical standards.
- Implement robust incident response plans for addressing data breaches and security incidents.
- Consider incorporating class action waivers in contracts to reduce the risk of extensive litigation.
- Mandate arbitration for data-related disputes as a more efficient alternative to litigation.
- Include forum selection clauses in contracts specifying the jurisdiction for resolving disputes.

RISK MITIGATION RESOURCES

- [Financial Institutions' Use of "Meta Pixels" Targeted in Latest Class Action Trend](#)
- [Tracking Pixel Secretly Transmits Chase Applicants' Financial Data to Facebook, Class Action Lawsuit Says](#)

- [Financial Institutions' Use of "Meta Pixels" Targeted in Latest Class Action Trend](#)
- Helpful links:
 - [Sign up](#) for our Let's Talk Fraud quarterly webinars
 - [View](#) additional risk resource

Need assistance or want to request a consultation? Contact our risk specialists at risk_specialist@alliedsolutions.net

The image contains two side-by-side promotional banners with a blue background and a globe graphic. The left banner is titled "Allied Insights" and features a red button with a white right-pointing arrow and the text "LEARN MORE". Below the button, it says "Forward-thinking content and original insights into the markets you serve, to help you grow, protect and evolve your business." The right banner is titled "Stay Informed" and features an orange button with a white right-pointing arrow and the text "SUBSCRIBE". Below the button, it says "Sign-up for our newsletters to receive expert education and insights on top-of-mind industry topics and receive resources coming to your inbox."



LinkedIn

The information presented in this email is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this email.