October 8, 2025

Medallia Digital Experience Analytics (DXA) and State Wiretapping Laws

Overview

Medallia Digital Experience Analytics (DXA) provides insight into how users interact with websites and applications, enabling organizations to identify friction points and improve digital journeys. Because DXA records interaction data, customers sometimes ask how tools of this kind relate to state privacy and communications laws, particularly the California Invasion of Privacy Act (CIPA) and the Florida Security of Communications Act (FSCA).

This article outlines the regulatory context, describes how courts have evaluated similar technologies, and explains the privacy-by-design safeguards built into DXA. It also sets out recommended practices for customers deploying the product.

Important: This article is provided for general informational purposes only. It does not constitute legal advice, may not reflect the most recent developments in the law, and should not be relied upon as a substitute for advice from qualified counsel. Customers are responsible for obtaining their own legal guidance to ensure that their deployment of DXA complies with applicable laws.

Regulatory Context

CIPA and FSCA were drafted long before digital analytics existed. Both statutes were designed to regulate unlawful interception of communications, but in recent years some plaintiffs have sought to extend them to cover technologies such as session replay. Courts reviewing these arguments have focused on three recurring questions: (1) whether interaction data qualifies as the protected “contents” of a communication, (2) whether users were provided clear disclosures and consent, and (3) whether plaintiffs could show actual harm rather than only a statutory violation.

Judicial Trends

When claims involving digital analytics have been tested in court, most have not advanced beyond the early stages. Judges have generally concluded that ordinary browsing interactions such as clicks, scrolling, and navigation do not amount to the type of protected communication envisioned by wiretapping laws. Courts have also emphasized that lawsuits must demonstrate real, concrete harm, and allegations that analytics code was present on a site are not enough on their own. In addition, when organizations disclosed their use of analytics in privacy policies, banners, or consent tools, courts viewed that transparency as inconsistent with the idea of surreptitious interception.

Taken together, these trends show that the outcome of litigation often depends on whether sensitive content is being captured, whether users were informed, and whether harm can be shown.

DXA Privacy and Security Safeguards

DXA is engineered with privacy-by-design controls to support responsible use. Among its safeguards:

1. **Automatic keystroke masking** ensures that typed inputs such as passwords and payment card details are hidden by default.

2. **Configurable masking rules** allow customers to block additional fields, text, or images from ever being captured.

3. **Irreversible masking** replaces masked content with placeholders or blacked-out fields so the underlying value is never stored.

4. **Consent integration** enables DXA to function in alignment with consent management platforms, so collection occurs only after users have opted in.

5. **IP address anonymization** reduces the identifiability of sessions by anonymizing or excluding IP data.

6. **Encryption standards** secure data in transit with TLS 1.2 and at rest with AES-256.

Medallia maintains ISO 27001, 27017, 27018, and 27701 certifications. DXA is also designed to support compliance with frameworks such as GDPR, CCPA/CPRA, HIPAA, PCI DSS, and APEC CBPR/PRP.

Recommended Customer Practices

Customers play an essential role in deploying DXA responsibly. Best practices include integrating DXA with consent platforms so tracking begins only after permission is given, reviewing masking configurations regularly to ensure that sensitive or unnecessary fields are excluded, updating privacy policies and banners to explain the use of analytics and session replay, and auditing deployments as websites and apps evolve.

Key Points

- Courts have generally dismissed claims involving digital analytics where no sensitive content was captured, no actual harm was shown, and users received disclosures or consent opportunities.

- DXA incorporates privacy and security safeguards, including masking, anonymization, and encryption, to minimize the risk of sensitive data being collected.

- Customers who adopt recommended practices such as consent integration, configuration reviews, and transparent disclosures are well positioned to use DXA

responsibly and in alignment with evolving privacy expectations.

- While litigation theories continue to surface, DXA's design and Medallia's long-standing guidance not to collect personal data provide strong assurance that organizations can improve digital experiences without relying on sensitive user information.

Additional Resources

- Medallia Global Privacy Policy
- DXA Product Overview
- Medallia Blog: Session Replay and Customer Experience