THOMPSON HINE

WEBSITE AND MOBILE APP COMPLIANCE & LITIGATION CHECKLIST

Businesses today must have a dynamic and informative online presence to communicate their products, services, and developments. Many organizations rely on their corporate websites, mobile applications, and other online platforms (collectively, "Online Services") to engage directly with existing and potential customers and investors through real-time chat features, email, and interactive forms. Additionally, how individuals interact with these Online Services can provide valuable analytics and insights into consumer behaviors and preferences, which are crucial for shaping business and marketing strategies.

However, Online Services present several legal and regulatory challenges, and there has been a sharp rise in litigation from consumer protection advocates alleging that improperly configured Online Services violate individual privacy rights and accessibility standards.

The Website and Mobile App Compliance & Litigation Checklist is designed to identify privacy statements, legal terms and conditions, and technology and accessibility configurations that are commonly required pursuant to United States federal and state laws, statutes, and regulations, or invoked in consumer protection-related litigation. Adhering to this Checklist can assist your organization in complying with the law and decrease the likelihood of litigation.

Issue	Description
Cookie Banner	Online Services should include a cookie banner to inform end-users about the collection, processing, and use of their personal data. This banner is intended to satisfy notice-at-collection requirements and can also be used to obtain consent before deploying cookies, pixels, and similar tags.
Consent for Non-Essential and Online Tracking Technology	Online Services that deploy non-essential cookies, pixels, and tags, such as online tracking technologies, need to identify whether they require opt-in or opt-out consent for such tools.
Notice at Collection	Online Services should include an acknowledgement link to a privacy policy wherever personal data is collected, such as registration pages, contact-us forms, or marketing sign-up forms. Alternatively, the link to the privacy policy should be placed in close proximity to any disclosure of personal data.
Homepage and Conspicuous Links	Online Services should include clear and conspicuous links to their privacy statements in easily accessible areas.
Cookie Management Tool	Online Services should include a cookie management tool (often named "Privacy Choices" or "Do Not Share My Information") allowing end-users to adjust their cookie preferences at any time.

Chat Features and Interactive Communications	If Online Services offer chat features or interactive forms, they should include disclaimers about recording communications content and how such content may be used or shared with third parties, including via social media and other online tracking technologies.
Third-Party Video Playback	Online Services that collect and share personal data on end-user interactions with embedded videos may require specific consent before sharing this data with third parties, such as advertising partners.
Age Gating	If Online Services collect information from minors or feature age-sensitive content, they should implement an age verification popup (age gate) requiring end-users to explicitly confirm they meet the minimum age before accessing the Online Services.
Biometric Data	If Online Services collect biometric data, such as facial recognition or scans (e.g., digital "try-on" features), they should require affirmative (opt-in) consent before collecting, using, or sharing the data, and include specific clauses for biometric data processing.
Health Data	Online Services that collect health data, such as adverse event reporting, may be required to obtain specific written consent before collecting, using, or disclosing such information.
Privacy Policy: Types of Personal Data Collected	A privacy statement should include a description of the types and categories of personal data processed by the organization, including data collected through website activities.
Privacy Policy: Data Sources	A privacy statement should outline the sources of personal data, whether derived from first-party or third-party sources.
Privacy Policy: How Personal Data is Used and Shared	A privacy statement should explain how the organization uses personal data in its custody and control (e.g., to provide and maintain its services, for marketing) and how it discloses such data (e.g., intra-group sharing, service providers, unaffiliated third parties, law enforcement, or during corporate restructuring).
Privacy Policy: Privacy Rights	A privacy statement should describe the privacy rights available to consumers, how they can exercise those rights, and how the organization processes and responds to privacy requests.
T&Cs: Dispute Resolution & Class Action Waivers	Online Services should include terms and conditions requiring end-users to agree (i) on how disputes will be resolved (e.g., arbitration or a designated court) and (ii) to waive their rights to file a class action claim.

T&Cs: Limitations of Liability	Online Services should include terms and conditions requiring end-users to agree to limits on the amount of damages they can claim as a result of using or accessing the Online Services.
T&Cs: End-User Reps	Online Services should include terms and conditions requiring end-users to confirm the minimum age threshold, have authority to be bound by the terms and conditions, and are located in appropriate jurisdictions.
Information Security Disclaimers	Online Services should generally describe the security measures in place to protect personal data, how the organization will furnish legally required data incident notifications, and include a liability disclaimer for its security practices.
Website Accessibility	Online Services should be accessible to individuals with visual, hearing, or other sensory disabilities, in compliance with the Americans with Disabilities Act (ADA), Website Content Accessibility Guidelines (WCAG), and other website accessibility standards.

Thompson Hine's nationally recognized **Privacy & Cybersecurity practice** is an interdisciplinary group of lawyers with experience in complex national and international privacy, data protection, information security, records retention, employment and labor law, consumer protection, internet law, insurance law and intellectual property matters. We help businesses develop, implement and benefit from globally compliant data-management practices and provide strategic counseling, regulatory compliance and litigation services to clients in a wide range of industries, with a keen eye on business information needs.

About Thompson Hine LLP. Thompson Hine LLP, a full-service business law firm with over 400 lawyers in 11 offices, is recognized for its innovative approach to the delivery of legal services, including being ranked number 1 in "Most Innovative North American Law Firms: New Working Models" by the *Financial Times* and shortlisted for *The American Lawyer's* inaugural Legal Services Innovation Award. Featured by Bloomberg and named a Legal Technology Trailblazer by the *National Law Journal,* the firm's commitment to innovation is embodied in SmartPaTH Plus™, the culmination of more than a decade of investment in legal project management, process efficiency, value-based pricing, flexible staffing and data analytics — now enhanced with purpose-built AI tools integrated into everyday workflows. For more information, please visit ThompsonHine.com and ThompsonHine.com/Innovation/SmartPaTH_Plus.

For more information, please contact:

Steven G. Stransky, Partner
Co-Chair, Privacy & Cybersecurity
Cleveland: 216.566.5646
Washington, D.C.: 202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/United States (CIPP/US)
Certified Information Privacy Professional/Government (CIPP/G)

Kim Sim Sandell, Partner
Privacy & Cybersecurity, Business Litigation
Los Angeles: 310.998.9100
Kim.Sandell@ThompsonHine.com