LEGAL UPDATES

AI & Privacy Laws are Changing Fast – Are Your Websites, Mobile Apps and Contracts Keeping Up?

01/24/2025 | 5 minute read

The new year serves as a reminder that – at least annually – businesses of all sizes should review their websites, applications and other data-related resources to ensure that they are up to date. Scheduling a regular cadence for review of your company's documents and policies will help keep you on the right track to address new legal developments and mitigate risk. For quick reference, we have provided a short list of critical updates and areas to review.

AI

Legislation on artificial intelligence is evolving. The FTC, EEOC and other federal agencies have provided some guidance, generally warning of discriminatory impacts in outputs and urging developers to seek and respect user consent. There is no comprehensive national law governing AI, such as the EU's AI Act. As with other areas of data law, states are rushing in to fill the void. In 2024, 45 US states introduced almost 700 different AI bills.

The new AI laws tend to focus on disclosures around how the AI models work, seek to prevent bias (particularly in areas of employment), and require ethical development with human oversight. The Colorado AI Act, which goes into effect on February 1, 2026, will require specific disclosures, documents and impact assessments for high-risk AI systems that play a substantial role in making "consequential decisions" relating to education, employment, financial services, housing, health care or legal services. One of California's new AI laws, for example, will require developers of generative AI systems to publish a summary of the datasets used to train such systems on their website.

These laws require changes now. Companies should include language around how both their business data and personal data can or cannot be used by their vendors' AI model. If your business uses AI in its offerings or has its own AI offering, it is important to allocate risk and tailor ownership language and rights around inputs and outputs.

Related People

Tedrick A. Housh, III, CIPP/US, CIPP/E
Partner
Kansas City
816.460.5642
tedrick.housh@lathropgpm.com

Chiara Portner, CIPP/US
Partner
Redwood Shores
650.804.7672
chiara.portner@lathropgpm.com

Related Services

Data Privacy & Cybersecurity Compliance
Intellectual Property
Corporate & Business
Labor & Employment

To Do:

- *Review processes and contracts regarding use of AI and training data.*
- *Assess AI outputs for discriminatory impact.*
- *Prepare AI transparency notices and related documents.*

Privacy Policies and Notices

As businesses of every size collect personal information, all states now have data breach notification laws, and more than half have passed comprehensive data privacy statutes. Even if your company has not triggered coverage under the EU's General Data Protection Regulation (GDPR) or California's California Consumer Privacy Act (CCPA), chances are that another state will assert jurisdiction. If any of your data practices have changed or involve any of the parameters that could bring you under the purview of certain laws that have changed, it is time to reassess and update your policies. Indeed, certain laws require that your privacy policy be updated annually.

Regulators not only act on consumer complaints but do their own website reviews more deeply than ever before. Together with class action lawyers, they evaluate whether certain trackers are being used or privacy signals are being properly followed. Companies must take stock, inventory online and offline data, and address the processing of such data in their external privacy policies. Companies must stand up their external-facing policies with proper training and internal policies.

Vendor contracts must also be part of this review. Various laws – such as the Gramm-Leach-Bliley Act, the CCPA and the GDPR – even require specific language to be included in contracts with third-party vendors that are not processing data on behalf of a business and that use data for their own purposes.

To Do:

- *Review and revise policies at least annually.*
- *Require vendors to agree to data protection provisions.*

Tracking, Cookie Popups and Consents

Pixels often begin to track website visitors before they encounter a cookie banner or other consent mechanism. Seizing on this scenario, there has been a surge in novel claims against businesses under the California Invasion of Privacy Act (a wiretapping statute) as well as the federal Video Privacy Protection Act. Companies using these tracking pixels should assess their usage and value proposition. If a business determines it is worthwhile to retain usage of these trackers, then it will be important to provide clear disclosures and consider how to implement user consents.

In the US, online consumers are not as used to cookie banners popping up on every website, and companies are loathe to place any impediments to the user experience, but they are becoming more and more prevalent. What your cookie banners say and the choices you give consumers depend on which laws apply to your business and how you are using and disclosing data.

To Do:

- *Evaluate the pixels and tracking mechanisms in use.*
- *Consider whether and how to implement a cookie banner.*

Terms of Use

Many states have automatic renewal laws, such as the FTC's Click to Cancel rule we discussed in November. When offering subscriptions, companies may now need to provide additional notices on signup and reminder notices regarding automatic renewals of subscriptions and memberships. Companies will also need to provide more transparent immediate options to cancel or opt out of automatic renewals.

There is some basic blocking and tackling required.

To Do:

- *Update user terms to ensure links and contact information are properly populated and to delete arcane terms such as fax notice provisions.*
- *Ensure you have clear legal language that matches the call for action so that your terms of use, terms of service or other similar online user agreements are more likely to be enforceable and binding.*
- *Make sure your action buttons match the operative text. For example, you should not tell users that by proceeding they agree to the Terms of Use when your click-button simply says "Submit" or "Signup."*

Employee Privacy

Employee data can be among the most sensitive data in a company's possession. As we explained last year, the 2023 amendments to the CCPA made it applicable to employees, so covered businesses should have a specific privacy notice on their career page for applicants and others. Other privacy laws apply to data collected from individuals in the employment context, including from employees, contractors and board members. Employees may have additional rights to access data, ensure inaccurate data is corrected and to have data deleted, depending on the state.

To Do:

- *Companies will need to adjust their employee handbooks, internal policies, and consider the notes and other data they create in their hiring and review efforts.*

Accessibility

In 2024, plaintiffs filed over 4,000 Title III ADA Accessibility cases, claiming disability discrimination against websites as "places of public accommodation." There is no federal regulation setting forth an accessibility standard for websites, although the WCAG standards issued by the World Wide Web Consortium (W3C) have been urged as such. Given the

growth of these and other class actions arising from online activity, the consideration of arbitration clauses and the use of jury trial and class action waivers becomes even more important.

To Do:

- *A company should engage in an assessment of its website and make a plan for improvements, as this may convince a court that an injunction is not required.*

Next Steps

- *Put a data privacy review reminder on your calendar.*
- *Update the "To Do" items above as a checklist.*
- *Coordinate changes with the C-suite, IT, Security and HR.*

Tackling these issues and getting your corporate house in order takes time. Time spent now, however, will likely prevent or reduce future liability from litigants and regulators. It is a worthwhile investment. If you have questions about the health of your business's data resources with regard to privacy regulation changes, please contact either Chiara Portner, Tedrick Housh, or your regular Lathrop GPM attorney.