Foster Garvey

Legal Alerts

Beyond Cookie Banners: Understanding the Gaps in Privacy Compliance

11.02.26

As new technologies become increasingly embedded in business operations, the collection and use of personal information and other sensitive information, such as names and contact details, financial account information, Social Security numbers and sensitive health information, continue to raise privacy and security concerns. States are responding with broader consumer data protection laws, often building on established privacy frameworks to address how businesses manage personal and other sensitive information.

More than 20 states now have comprehensive consumer privacy laws in effect, with recent amendments expanding requirements and tightening certain exemptions. Enforcement activity has also resulted in significant settlements. The state of Texas obtained a $1.375 billion privacy settlement from Google for unlawfully collecting users' privacy data (e.g., geolocation, incognito searches, biometric data). California similarly entered into a $1.55 million settlement with Healthline centered on its online tracking technology on its health information website and failing to honor consumers' rights to opt-out of targeted advertising and inappropriate sharing of their health data with third parties. Federal enforcement has also produced some eye-popping results as the U.S. Department of Justice settled with TikTok and ByteDance for $400 million involving alleged violations of the Children's Online Privacy Protection Act.

Many businesses have responded by using consent management platforms to manage cookie banners and opt-out preferences, along with annual updates to their privacy policies. Although these measures address important consumer-facing requirements, they do not necessarily account for the internal systems and controls needed to support them. A compliance gap can remain when businesses lack documented assessments of how personal and other sensitive information is handled and whether their practices align with their disclosures.

The Missing Middle: Assessments, Inventories and Governance

Closing this gap requires a more comprehensive evaluation of a business's privacy practices. Consent management platforms can record consumer preferences, but businesses also need to understand how personal and other sensitive information moves through their systems and whether appropriate safeguards are in place.

© 2026 Foster Garvey PC. All Rights Reserved.

This begins with identifying what personal and other sensitive information is collected and how it is processed. Data inventories and mapping help establish where information resides, who can access it and how it is shared with third parties. Risk assessments and gap analyses can then identify vulnerabilities and determine whether existing practices meet applicable legal requirements.

The results of these evaluations can inform necessary operational changes. For example, businesses may need to update older systems to properly process consumer access or deletion requests, adjust consent mechanisms to recognize opt-out signals or revise their data retention practices. Vendor agreements should also address data processing responsibilities and appropriate liability protections, with businesses verifying that outside providers meet their obligations.

These assessments should continue as businesses introduce new technologies or make changes to their systems. Periodic compliance audits can help confirm that the resulting safeguards remain effective, while documenting findings and corrective measures provides a record of the work performed. Appropriate involvement from senior leadership can also help ensure that identified risks are addressed.

Businesses can look to existing privacy/cybersecurity and healthcare frameworks when conducting these assessments. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and NIST Privacy Framework provide structured methods for evaluating risks and developing appropriate safeguards. The Health Insurance Portability and Accountability Act (HIPAA) offers a practical example of this approach through its longstanding requirements for risk analysis and documented security measures in the healthcare sector. The U.S. Department of Health and Human Services' Office for Civil Rights has also published a crosswalk mapping the HIPAA Security Rule to the NIST CSF, which shows how the two overlap and can help businesses use one framework to inform work under the other.

For businesses just starting their privacy compliance efforts, these frameworks offer a useful place to begin because they apply across industries, not only in healthcare. The NIST CSF 2.0 and the NIST Privacy Risk Assessment Methodology (PRAM) offer step-by-step approaches to identifying and managing security and privacy risks. Using the NIST frameworks, a business can first describe its current practices (a "Current Profile"), then define where it needs to be based on its legal obligations and risk tolerance (a "Target Profile"). Comparing the two shows the gaps to close, and those gaps can be organized into a prioritized action plan.

Why Documentation Matters

Documented assessments and internal controls serve a purpose beyond meeting regulatory requirements. When privacy incidents or compliance questions arise, businesses may need to demonstrate what measures were in place and how identified risks were addressed.

Inadequate privacy and cybersecurity practices can also increase litigation exposure and affect cyber insurance coverage. Insurers increasingly examine security controls and documented risk management practices when determining coverage, making ongoing assessments relevant to a business’s broader risk

© 2026 Foster Garvey PC. All Rights Reserved.

management efforts.

Privacy Compliance Checklist

Businesses can take the following steps to evaluate their practices and address potential compliance gaps:

- **Conduct data inventories and mapping**. Identify the personal and other sensitive information collected and its legal basis, where it is stored, who has access to it and how it moves through internal systems or third parties.
- **Perform risk assessments and gap analyses**. Evaluate existing practices against applicable privacy requirements and identify areas needing improvement. Consider data protection impact assessments before certain activities involving sensitive information, targeted advertising or profiling.
- **Review technical controls and data management practices**. Verify that systems recognize opt-out signals and support consumer access or deletion requests. Review privacy disclosures and establish appropriate retention and secure disposal procedures.
- **Evaluate vendor agreements and compliance**. Review data processing responsibilities and contractual protections, including liability, indemnification and insurance provisions. Verify that outside providers meet their obligations.
- **Assess cybersecurity and insurance readiness**. Review existing security controls and incident response procedures against identified risks and applicable insurance requirements.
- **Maintain ongoing oversight**. Document assessments and corrective measures, assign responsibility for compliance and conduct periodic reviews with appropriate leadership involvement.

Perfection is not the standard, but documented, good-faith effort is increasingly what regulators, insurers and courts expect. The likelihood of avoiding consequences for inadequate compliance is narrowing. A business that begins this work now will be better positioned to manage regulatory risk, maintain insurance coverage, scale up to additional privacy law requirements, defend against litigation when incidents occur and protect its business reputation with consumers.

Businesses are encouraged to consult with experienced legal counsel to navigate these developing challenges and to ensure that website data and security measures are up to date. If you have any questions about these considerations, please reach out to Foster Garvey's Privacy, Data Protection & Cybersecurity team.

The information above involves complex legal considerations and is provided for general informational purposes only. It does not constitute legal advice. For guidance on specific legal matters, you should consult with an attorney. Foster Garvey requires engagement letters to establish the attorney-client relationship for new (or returning) clients and requires written confirmation to expand the scope of representation for existing clients.

© 2026 Foster Garvey PC. All Rights Reserved.

Foster Garvey

Authored by

Claire F. Hawkins

Principal|Seattle

206.816.1301 claire.hawkins@foster.com

Mikaela Louie

Counsel|Seattle

206.447.8891 mikaela.louie@foster.com

Andrew A. Schillinger

Counsel|Spokane

509.744.1806 andrew.schillinger@foster.com

Related Areas

- Business & Commercial Transactions
- Health Care
- Intellectual Property, Privacy & Technology
- Privacy, Data Protection & Cybersecurity

© 2026 Foster Garvey PC. All Rights Reserved.