BCLP. Client Intelligent

Insights

PRESSURE-TESTING YOUR PRIVACY PROGRAM FOR 2025

Jan 28, 2025

With the onslaught of new privacy, AI and cyber legislation coupled with promises for enforcement and class action litigation, running a well-functioning and flexible privacy and cyber program is increasingly a critical component of an organization's overall risk compliance strategy. As part of this process, companies must pressure-test their privacy programs regularly to make sure they appropriately address existing and emerging risks while maximizing business gains. To help companies develop a strategy tailored to 2025, we have highlighted a few key issues below that will be particularly relevant over the coming year.

After 2025, nearly half of US states will have enacted comprehensive consumer privacy laws:

- Jurisdictions with existing privacy laws: California, Colorado, Connecticut, Florida, Montana, Nevada, Oregon, Texas, Utah, Virginia, Washington
- Jurisdictions with new privacy laws in effect in 2025: Delaware, Iowa, Maryland (October 1, 2025), Minnesota (July 31, 2025), Nebraska, New Hampshire, New Jersey, Tennessee (July 1, 2025)
- Jurisdictions with privacy laws scheduled for 2026: Indiana, Kentucky, Rhode Island

These laws do not account for the myriad AI, cyber, data broker and biometric laws that will inevitably impact programs as well. The sheer breadth and scope of these laws will require to companies to think about data systematically and strategically and to recalibrate on an annual basis.

UPDATED PRIVACY NOTICES

In many ways, website privacy policies are old news in the privacy world. Many policies got a full update when the EU GDPR took effect in 2018, with a fresh round of revisions triggered by the arrival of the CCPA in 2020. With the implementation of new and/or updated privacy laws, organizations have grappled with how to sync up similar but not identical notice obligations and whether to provide specific disclosures for each state and/or jurisdiction. For instance, while most privacy laws tend to follow the same formula for the disclosures required in a privacy policy, several

recently effective laws are outliers and require either an expansion of the description of certain rights (e.g., Oregon's right of access), or specific language to be included to the extent that sensitive or biometric personal information is sold (e.g., Texas).[1]

These fast-paced changes have led to apparent and understandable privacy fatigue, and it is not uncommon to see websites with privacy policies that have not been updated for several years in spite of potentially new content obligations that should be reflected in the policy (either on a consolidated basis or as a stand-alone section). Website privacy policies are, however, public-facing and the content requirements for such policies serve as the backbone for most state privacy laws. Therefore, identifying and enforcing on deficient privacy policies is low-hanging fruit from an enforcement perspective (particularly where specific language is required in that jurisdiction), making this an issue that should not be ignored.

Likewise, the use of cookies and similar technologies on a website require public-facing mechanisms and/or disclosure. In evaluating how to approach cookies and related technologies, companies should first determine whether they would prefer a globally compliant approach (e.g., an opt-in for all non-essential cookies to comply with European requirements), or a jurisdictional approach. Where companies are subject to the laws of multiple states, for instance, companies will need to determine whether to take an opt-out approach for all behavioral advertising cookies, whether to recognize universal opt-out signals, and/or whether to make an opt-out link available across jurisdictions. As described in greater detail below, companies should take care in approaching the use of cookies on their websites.

SENSITIVE DATA OBLIGATIONS

Most US state privacy laws impose additional obligations on organizations that collect and use certain types of sensitive personal information, including health and medical data, or data revealing racial or ethnic origin, religious or philosophical beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, citizenship or citizenship status, genetic or biometric data and/or information about a known child (generally a child under 13). For example, some state privacy laws require that organizations provide consumers with the right to opt-out of certain uses of sensitive data (California, Iowa, Utah), while others require that organizations obtain affirmative opt-in consent to the collection and processing of sensitive data (Colorado, Connecticut, Delaware, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, Virginia). These laws also require that entities processing sensitive personal information conduct data protection impact assessments, which are assessments of whether the benefits from processing personal information outweigh the risks associated with that processing. In certain states, such as Colorado, these assessments must be provided to regulators upon request.

Even where the scope of sensitive personal information was previously settled, amendments to existing privacy laws have expanded the scope of what constitutes sensitive personal information (e.g., California, Colorado). In particular, entities processing biometric data in Colorado may be

subject to new procedural requirements moving forward, including an expansion of protections applicable to employees. Our more detailed summary regarding these new Colorado rules is available here.

In 2024, two comprehensive consumer health data laws went into effect (e.g., in Nevada and Washington). During that same period, we saw several states expand the scope of personal information subject to protection to include consumer health data. Several laws that were proposed in 2024, but did not pass, also included this expanded scope of personal information. Looking forward, we can expect more states to take the broader approach of including health data within the scope of sensitive personal information, particularly as more and more companies that collect and use health information are outside the scope of the federal health privacy law, HIPAA.

To help mitigate enforcement and class action risks associated with sensitive personal information, particularly health data, companies should focus on understanding what sensitive data they collect, use and disclose, and determine how best to develop or implement related disclosures and consent mechanisms. Companies should also pay close attention to state enforcement actions brought against entities that collect sensitive personal information.

ADVERTISING TECHNOLOGIES AND LEAD GENERATION

The use of online tracking technologies for online behavioral advertising, analytics and related activities has come under increasing scrutiny by regulators and the plaintiffs' bar in the US, Europe and elsewhere. Even as cookies management tools have become common, and there is generally increased understanding of how these technologies work, it is not unusual for companies to make mistakes in implementing or configuring the tools. Importantly, these implementation challenges come at a time when enforcement at the global and US state level is focused specifically on digital advertising and the related protections provided to consumers, creating meaningful risk that should not be ignored. Companies should take this issue seriously by understanding the technologies deployed on their websites and mobile apps, appropriately describing them and configuring related technical solutions in a way that meets applicable legal obligations (e.g., offering a right of opt-in to all non-essential cookies in Europe or offering an opt-out right for behavioral advertising cookies via a "Do Not Sell or Share My Personal Information" or "Your Privacy Choices" link where required in the US).

As part of this process, companies must confirm that the solution does what it says it will do. For example, if consumers are provided the right to opt-in to certain cookies, those cookies should not drop if and until a consumer consents to those cookies. Companies must also tackle with their providers how best to recognize universal opt-out signals sent by browsers themselves, particularly as new options hit the market and are recognized by regulators (e.g., Global Privacy Control in Colorado). We have provided additional information regarding the appropriate implementation of cookies solutions.

Relatedly, as with sensitive personal information, the use of behavioral advertising cookies and similar tracking technologies can trigger the requirement to conduct a data protection impact assessment. These assessments are generally required where the entity engages in targeted advertising or profiling if the profiling presents a reasonably foreseeable risk of unfair or deceptive treatment of consumers, financial, physical or reputational injury to the consumer, an intrusion upon the seclusion of consumers that would be treated as offensive to a reasonable person, or other substantial injury. This may arise, for instance, where targeted advertising is used to target consumers with different prices for the same product. European law also requires entities to conduct assessments where personal information is processed through automated means, including profiling, where the processing is used to produce significant effects for the relevant individuals and is not subject to human review.

We have also seen a continuation of class action litigation being brought in response to the use of targeted advertising cookies and related technologies. For instance, the use of behavioral advertising cookies continues to be treated as an alleged violation of wiretap laws in states that require two-party consent for recordings (e.g., California and Pennsylvania). Under the California Invasion of Privacy Act ("CIPA"), the plaintiff's bar has argued that the use of tracking technologies to collect and disclose IP addresses is sufficient to be treated as an unlawful pen register that violates CIPA. Likewise, some of these tools can fall within the scope of session replay software, or software that closely tracks a user's interactions with the website to the point that their interactions with the website can be recreated. These tools have been targeted under the same wiretap violation theory. To limit potential exposure under these types of claims, companies have put in place mechanisms to both carefully disclose the use of the technologies, and obtain affirmative consent to their use prior to collecting information about individuals through the tools. Additional information regarding these emerging class action risks is available in our previous insight, VPPA trends: considerations for limiting exposure.

TELEPHONE CONSUMER PROTECTION ACT

Telephone Consumer Protection Act ("TCPA") class actions continue to be a major risk for businesses that market via text messaging, autodialed/prerecorded/artificial voice calls, or faxes. The TCPA provides for statutory damages of $500-$1,500 per unwanted message, with no requirement to show actual injury, and is frequently litigated in the class action space. TCPA lawsuits routinely settle in the seven-to-eight figure range, so businesses should take note.

2025 already promises to be an exciting year for the TCPA. On January 24, 2025, the Federal Communications Commission ("FCC") stayed the effective date of its new rule requiring telemarketers to obtain 1:1 consent for robocalls and texts, which was scheduled to take effect on January 27, 2025. The "1:1 Consent Rule" had struck fear into the hearts of lead generators and businesses alike, since it would have meant that businesses relying on leads generated prior to January 27, 2025 would no longer have the "prior express written consent" required for marketing.

Many predicted a spike in TCPA litigation based on the new rule, and heaved a sigh of relief with the stay.

Literally moments later, the Eleventh Circuit ruled that the FCC had overstepped its authority with regards to the 1:1 Consent Rule as well as a new requirement that telemarketing must be "logically and topically related with the interaction that prompted the consent." The Court vacated the new rule and remanded it to the FCC for further proceedings. In the coming weeks and months, expect further developments as the FCC addresses the Eleventh Circuit ruling.

Additionally, on April 11, 2025, the FCC's new consent revocation rules will be implemented, allowing consumers to revoke consent via "any reasonable method," and requiring that businesses honor revocation requests within ten business days. We have prepared articles providing background on the 1:1 Consent Rule, the FCC's stay and the Eleventh Circuit decision, as well as recent updates relating to revocation of consent, and how these obligations may affect businesses.

ARTIFICIAL INTELLIGENCE

Although not strictly a privacy issue, the use and development of products utilizing Artificial Intelligence or AI, particularly Generative AI, will almost certainly continue to be a key area of focus for companies and regulators in 2025. Due to the overlap with privacy, AI compliance efforts are frequently starting in the privacy office, such that privacy professionals should expect and advocate to be a leading force in guiding their organizations' AI efforts. To help prepare and to maximize the rewards of new AI technologies while mitigating related risk, companies should start by understanding where and for what purposes they are or are likely to use AI and begin to build a right-sized compliance framework based on these uses. Elements should include a cross-functional governance structure, clear guidelines on permissible uses, appropriate procurement processes to address AI specific issues and risks (e.g., prohibitions on the use of customer data for training of models, strong audit rights, potential use of a private offering, and appropriate IP and data breach protections). To begin assessing which elements may be helpful in internal AI procedures moving forward, companies may look to the European Union Artificial Intelligence Act (effective as of August 1, 2024) and the up-coming Colorado AI Act (effective February 1, 2026) as guides of how other jurisdictions may approach AI regulation.

Organizations that deploy AI products or services will also need to focus on transparency around the functionality of the products as well as on efforts to address key issues including bias and inaccuracy. Our state law legislative tracker can help companies track new developments at the state level, and we will continue to provide updates regarding activity at the federal level.

CYBER SECURITY AND INCIDENT RESPONSE REQUIREMENTS

We have seen increasing efforts at the federal level to regulate cyber and information security and security incidents. The SEC has issued additional guidance concerning its material incident

reporting requirements. HHS has published a Notice of Proposed Rulemaking regarding revisions to the HIPAA Security Rule. And in the EU, the Cyber Resilience Act came into force, mandating the hardening of certain software and hardware products.

Publicly traded companies will continue to be subject to the SEC's material reporting requirement and will likely face additional scrutiny now that the rules are more than a year old. Under the Final Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, publicly traded companies must report material cyber security incidents on Form 8-K within four business days of determining that an incident is material, and must also include in the annual 10-K filing additional disclosures about cybersecurity policies and procedures and cyber threat oversight by management and Board of Directors. Already, we have seen the SEC take steps to enforce related reporting requirements. In one set of enforcement actions alone, the SEC brought civil penalties against four companies that totaled $7 million altogether, as described here.

For covered entities subject to HIPAA, HHS published a Notice of Proposed Rulemaking to the Federal Register in early 2025 which, if finalized, would require certain regulated businesses to implement substantial cybersecurity procedures. These include, among other requirements, obligations to map how ePHI moves through the entity's systems, consider more specific criteria when conducting a risk assessment, put in place enhanced security measures (e.g., MFA, network segmentation, removal of extraneous software, etc.), and take steps to verify the technical measures in place among business associates and any subcontractors.

While not expected to become effective until 2026, entities that offer goods or services in critical infrastructure sectors should also be mindful of upcoming reporting requirements under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). We have prepared further information about CIRCIA and which sectors are considered critical infrastructure, including the health care, information technology, and financial services sectors.

For entities subject to these federal information security and breach notification obligations, a review of existing information security procedures should be undertaken to assess compliance with the latest federal requirements.

And apart from compliance considerations, 2024 once again confirmed that data breaches, ransomware, and other threats are not going anywhere. According to one estimate, the average cost of a data breach increased 10% year over year, making 2024 the most expensive year ever for victims of cyberattacks.[2] Therefore, companies should continue to prioritize incident preparedness through a refresh of incident response policies and procedures, training, including table top exercises and an annual review of cyber insurance coverage.

DATA BROKER REQUIREMENTS

Beyond the traditional privacy legislation discussed above, we saw a trend toward increasing data broker regulations in 2024, which we expect to continue through 2025.

At the federal level, President Biden signed the Protecting Americans' Data from Foreign Adversaries Act of 2024 into law. The law prohibits data brokers from selling, transferring, or providing access to Americans' sensitive data to certain foreign adversaries (e.g., North Korea, China, Russia, or Iran) or entities controlled by them. The Consumer Financial Protection Bureau also proposed a rule that would, if made effective, expand the scope of entities subject to the Federal Credit Reporting Act ("FCRA") by treating certain data brokers as consumer reporting agencies. The CFPB also published a Circular clarifying that the FCRA applies to workplace surveillance in some instances.

Regardless of whether the new administration builds on recent moves to federally regulate data brokers, we have seen similar efforts at the state level. More states have implemented data broker registration requirements (e.g., California, Texas, Vermont), with some also requiring data brokers to undertake certain disclosure requirements (e.g., Vermont). Though not effective until 2026, at least one state (California) has also created a formal mechanism through which consumers may submit deletion requests applicable to all data brokers operating in the state. Additional information regarding the pending "Delete Act" is available here.

Which entities are treated as data brokers vary at the state level, but we have seen increasing enforcement actions against entities that fail to register as data brokers in the past year. In particular, the Texas Attorney General notified over 100 entities in June 2024 of their apparent failure to register as data brokers in Texas. We can expect this trend to continue into 2025 as new states grapple with data broker regulations.

There is no one-size-fits-all approach to maintaining and improving privacy compliance programs, and an effective strategy must reflect the broader DNA of the organization itself. Nevertheless, taking a step back and looking at the current regulatory environment as well as evolving market practices are key elements to reducing risk and keeping the program relevant. 2025 promises to be a year worth watching in the privacy and AI space, and organizations that start this process sooner rather than later will certainly put themselves in a much better position by the time enforcement and class action litigation kick into gear.

---

[1] In fact, a recent cause of action brought by the Texas Attorney General against an insurer contains allegations specifically referencing this requirement in relation to driver data.

[2] Cost of a data breach 2024 | IBM.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Goli Mahdavi

San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448

Martha Kohlstrand

Boulder

martha.kohlstrand@bclplaw.com
+1 303 417 8516
