BCLP. Client Intelligent

Insights

PRESSURE-TESTING YOUR PRIVACY PROGRAM FOR 2024

Jan 04, 2024

SUMMARY

With the onslaught of new privacy legislation and cyber threats coupled with upticks in enforcement, running a well-functioning and flexible privacy program is now, more than ever, 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. A comprehensive review is not always possible, but it is important to keep in mind that the last several years have seen a wave of new state privacy laws as well as activity at the federal level that promises to challenge even the most well-developed privacy team. To help companies develop a strategy tailored to 2024, we have highlighted a few key issues below that will be particularly relevant over the coming year.

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 in California and a number of other US states, 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. 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). In spite of this fatigue, however, website privacy policies are publicly 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, making this an issue that should not be ignored.

While approaches to these obligations will vary based on the applicability of differing laws, risk tolerance, data collections and related issues, companies should continue to reevaluate their

privacy notices to make sure they are not only accurate and complete but also reflect the changing notice requirements.

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, Utah), while others require that organizations obtain affirmative opt-in consent to the collection and processing of sensitive data (Colorado, Connecticut, 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.

The Washington My Health My Data Act (WMHMD) also becomes operative in March of 2024 for most organizations. The WMHMD imposes broad obligations on organizations that collect and process certain health related data, including detailed notice and strict and far-reaching consent obligations, and contains very limited exceptions to data subject rights and other requirements. While the application of most health privacy laws is limited to entities that process traditional health data, the WMHMD applies broadly to any entity that processes personal data that could reveal a health condition, perhaps going so far as to regulate entities that sell cold medicine or crutches. Critically from a risk perspective, the WMHMD includes a private right of action that leaves organizations trying to understand and implement the law's complicated requirements vulnerable to the class-action lawsuits that are almost certain to follow once the law comes into force.

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. They should also continue to track guidance and enforcement activities related to these issues to further refine solutions to best fit current interpretations of state laws.

DIGITAL ADVERTISING AND RELATED TECHNOLOGIES

The use of online tracking technologies for online behavioral advertising, analytics and related activities has come under increasing scrutiny by regulators 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 absolutely 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., 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. Under new California regulations, an assessment will be required where an entity uses behavioral advertising cookies to collect personal information about a website visitor for third party marketing purposes (*i.e.*, a "share" under California law). In other states, these assessments are 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.

Companies should also be cognizant that related website 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. In some states, technologies that track users in this fashion have been targeted in class actions due to alleged wiretap violations. There has also been a dramatic uptick in similar class actions against website operators collecting video watching data through embedded videos on their website, or through the collection of data through an interactive chat bot feature. Additional information regarding these emerging class action risks is available in our previous insight, VPPA trends: considerations for limiting exposure.

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 be a key area of focus for companies and regulators in 2024. 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).

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.

SEC CYBERSECURITY RULE AND INCIDENT RESPONSE

The SEC published its Final Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure on July 26, 2023. Among other things, the rule requires publicly traded companies to report material cyber security incidents on Form 8-K within four business days of determining that the incident is material and also to include in the annual 10-K filing additional disclosures about cybersecurity policies and procedures and cyber threat oversight by management and Board of Directors (read our summary). These new obligations took effect on **December 18** of 2023, and the SEC has signaled in recent charges against SolarWinds Corp. that it is taking cyber issues seriously (as summarized in BCLP's recent blog post). With the new reporting deadlines fast approaching, companies should start preparing by evaluating incident response processes and procedures, developing guidance for determining when a security incident might be material, establishing an internal reporting structure in the event of a material incident and also developing the necessary disclosures for the 10-K reporting process. Even companies with sound existing incident response plans should revisit them in view of the new disclosure rules, and all public companies should be working on the new annual cybersecurity disclosures now.

Taking these steps will also help companies prepare for the ever-present threat of cyber attacks and security incidents, risks that cannot be ignored in any year.

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. 2024 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.

RELATED CAPABILITIES

- 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

Gabrielle A. Harwell

Chicago

gabrielle.harwell@bclplaw.com
+1 312 602 5143
