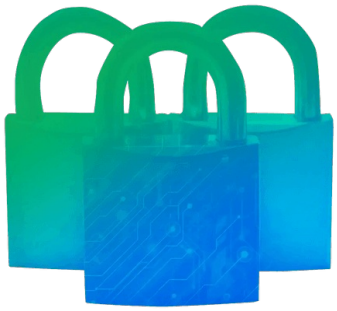

Practical Privacy: Lessons from the Front Lines

Laura Riposo VanDruff, Aaron J. Burstein, Caroline T. Schmitz

August 31, 2023

With the continuing onslaught of state privacy laws, it's easy to become overwhelmed by the number of new legal obligations while also trying to stay focused on identifying and mitigating the most pressing legal and business risks. Over the past couple of months, we've had the opportunity to meet with privacy professionals to hear about their top challenges and offer some practical perspectives of our own.

Three of the topics that stood out during these discussions – there were several others – were: understanding and managing data protection impact assessments (DPIAs), assessing sensitive personal information (SPI) risks, and implementing data deletion obligations. This post shares some of the tips that emerged from these sessions.

Data Protection Impact Assessments

Four states require DPIAs today for certain processing activities, and laws that go into effect in five additional states beginning in 2024 will require them, too. Across most of these states, the activities that trigger the need to conduct a DPIA include targeted advertising, data sales, and sensitive data processing. Beyond these clearly defined starting points, however, practical challenges abound. What form should a DPIA take? Who should be responsible for drafting the assessment? What are the best practices for keeping DPIAs up to date?

One way to look at these questions is that DPIAs tell the story about how a company uses personal data. Regulators will be one audience for these stories. Some states' laws allow the attorneys general to request production of DPIAs from organizations. California law requires businesses to submit their DPIAs to the CPPA on a "regular basis" (with details now set forth in draft regulations). Regulators will expect to see (in the words of the Colorado Privacy Act's implementing regulations) a "genuine, thoughtful analysis" of the benefits, potential harms, and mitigations in a company's data practices.

At the same time, although some state privacy laws provide protection for attorney-client privilege and confidentiality, we expect DPIAs to generate investigations and to have their privilege and confidentiality protections challenged. Carefully planning the diligence and drafting stages of a DPIA – and taking care to maintain safeguards for communications that involve legal advice – is critical to ensuring that DPIAs are accurate and comprehensive while minimizing additional risk to the company.

Finding internal champions and identifying key stakeholders are also critical steps. DPIAs take time away from IT, engineering, business, legal, compliance, and privacy teams who have day jobs. In most cases, their contributions are essential to assemble an accurate picture of the activity that's at the center of a given DPIA.

The message that spurs these teams to participate meaningfully in the DPIA process will vary. In some cases, buy-in might arise from a shared understanding that the company needs to align on whether its current practices are sufficient to protect against known risks. In other instances, a clear message of support from the top of the organization might be necessary.

In short, there isn't a single format or process that will work for everyone. However, recognizing that the stakes involved in DPIAs are significant and planning accordingly are first steps toward identifying which processing activities to tackle first and how to go about it.

Sensitive Personal Information

In addition to triggering a DPIA obligation, SPI processing under state laws and emerging enforcement precedent may require opt-in consent. Identifying SPI collection and use is therefore a growing priority for many privacy professionals.

But the expansive definition of SPI under state privacy laws is only part of the equation. Sector-specific laws, such as the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the Illinois Biometric Information Privacy Act, expand the range of sensitive data that receives heightened protections. These laws have become an increasing focus for regulators and the plaintiffs' bar at the same time that data from these sectors is becoming more valuable for new services and, in some instances, advertising.

Where SPI is used in marketing and advertising, companies face compliance challenges and potential exposure to private suits. Using alternatives to SPI can mitigate these risks. For example, in lieu of SPI, some companies are exploring the use of *aggregated* demographic data to power insights or target advertising based on non-sensitive purchasing behavior.

Practical approach to SPI

- Cataloging data starts with thoughtful DPIAs and a robust understanding of the business use cases with SPI.
- Consent is the baseline expectation for SPI processing. Consider building a consent management infrastructure that accounts for both direct collection and sourced (or inferred) data.
- Explore emerging alternatives to SPI and implement mitigation measures in the meantime.
- Think for today and for tomorrow. Short-term and long-term plans are crucial for developing a comprehensive and durable risk-management strategy. Set a cadence to revisit the plans.

Data Deletion Obligations

All comprehensive state privacy laws that have been enacted so far give consumers the right to request deletion. State laws vary in the level of detail they provide about deletion – regulations in California and Colorado are quite specific in their procedures – but all provide significant leeway to retain data for internal purposes that are reasonably aligned with consumers' expectations. In practice, it is not uncommon to preserve some data to meet operational needs or comply with legal

obligations.

This leads to two challenges. First, companies need to communicate clearly with consumers, service providers, and third parties about how they're fulfilling deletion requests. Second, companies need ways to ensure that data they keep under an exemption is not used for other purposes.

A few practical steps can help:

- Prior to developing a process for responding to deletion requests, map out your data to understand what personal information you have, where it is located, and with whom you share it. Identify any legal obligations surrounding how long you must keep it, including any *minimum* retention periods.
- Develop and maintain systems to notify service providers and third parties about data deletion requests. Methods for sending deletion requests to partners vary widely, from self-serve, automated interfaces to ad hoc requests that are handled case-by-case, so be prepared to work with a wide range of processes.
- Communicate clearly with consumers about deletion requests, whether the request will be approved in whole, in part, or not at all.

If Kelley Drye can help your organization develop a practical approach to building and maintaining a robust privacy program, please contact any member of our Privacy Group.