Adtech Privacy Pain Points: Top 7 List for Effective Opt-Out Compliance

Kelley Drye

As privacy enforcement ramps up, effectively managing opt-out requirements under state privacy laws is a top risk mitigation measure. But complying with opt-outs is not just a matter of providing a consumer-facing opt-out mechanism. It is equally as important for businesses to implement a comprehensive behind-the-scenes framework to ensure consumer choice is consistently registered on the backend. This includes embedding consumer preference signals in data governance and the many channels that communicate with third-party tools and systems in scope for opt-outs. Failing to do so puts businesses at risk of only superficially addressing statutory requirements and facing legal claims that they have not discontinued the sale and/or sharing of personal information, or use for targeted advertising.

In practice, these "gaps" may take on different forms. For instance, an opt-out mechanism may *appear* on the surface to enable consumer choice, but on closer inspection, trackers may still be set and/or information may continue to be transmitted for retargeting, post opt-out. Likewise, a "Your Privacy Choices" link may redirect consumers to a form enabling an opt-out from offline sales that does not address device-based ("client side") targeted advertising. These are just a few examples of what could be considered non-compliance red flags.

To avoid these gaps, consider this top 7 list of business considerations:

1. **Understanding Sale/Share/Targeted Ads Data Flows.** Effective compliance with opt-out requirements is a significant challenge for a business that cannot answer: what personal information is disclosed, to whom, and why. In California, for instance, the concept of "selling" personal information is very broad. Understanding the purpose, scope, and means of all external disclosures of personal information (particularly for marketing and analysis use cases) is critical to categorize vendors by type (e.g., service provider, third party), carve-out sensitive information that requires an opt-in (or that cannot be disclosed) in some states, and communicate consumer preferences across a business's ecosystem for logged-in consumers. This is also the only way to ensure that mandatory contract terms are consistently in place – notably in California, which requires specific terms for each type of recipient.

2. **Leveraging the Right Tools**. A business must also understand *how* it is selling or sharing information. For instance, do you share deterministic identifiers (e.g., email addresses, phone numbers, along with or without other attributes) directly with partners, or engage in cross-context behavioral advertising using client-side technologies (e.g., cookies, tags, and pixels) – or likely both? Where the business knows who the consumer is (e.g., logged into an account), the business must provide consumers with an opt-out that covers all sales/sharing activities, each driven by different types of information across touch points. When leveraging a third-party consent management tool (CMP), it is important to perform diligence and confirm

whether the CMP facilitates the implementation of controls around data processing across all sale/sharing use cases in a manner that complies with statutory requirements, or if the business will need to directly address what the CMP does not cover. Particularly on this point, businesses need to get behind CMP marketing claims and confirm if the opt-out tools are limited to client-side technology (i.e., limited to browser and device specific opt-outs), or if they also provide an automated means of including identifier-based sales and shares. Not all CMPs offer equivalent coverage here.

3. **Configurations.** From a technical perspective, processing opt-outs requires several steps. First, when it comes to client-side sales and sharing, third-party integrations (e.g., advertising tools/integrations) must be properly configured to ensure the opt-out mechanism signals to all third parties that the consumer has opted out. Notably, opt-out requirements are not simply about blocking cookies. Blocking cookies does not stop further processing of information, it merely stops cookies from being set. Although cookies were once the prevailing method for tracking users, targeted advertising and other types of sales leverage tools that are not limited to cookies, and regulators are inquiring about all of the ways a business may sell/share personal information or use for targeted advertising. Separately, recognizing Universal Opt-Out Mechanisms (e.g., Global Privacy Control) is a standard requirement of most U.S. privacy laws, and businesses are obligated to recognize the signal on web browsers (today) and other platforms in the future as technology evolves.

4. **Dark Patterns.** The California Privacy Protection Agency's (CPPA) 2024 Advisory and recent enforcement action against Honda leave little doubt that "dark patterns" are one of the CPPA's priorities. Symmetry in choice is one area of focus. Both the 2024 Advisory and the Honda settlement order make clear that the path for a consumer to exercise a more privacy-protective option must "not be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option." Offering an "Accept All" with one click while requiring multiple clicks to opt out does not provide symmetry in choice. Auditing the privacy opt-out experience will help address this common issue. Practical tip: it's also not just the CPPA that is inquiring on this topic.

5. **Monitoring.** Privacy compliance is dynamic, and routine monitoring is an important step toward ***staying*** compliant as both data processing and statutory requirements change. A scalable process should be implemented to verify that new advertising vendors, tools, and channels are consistently and timely brought into the fold. Likewise, regularly auditing your sale/share compliance to confirm that opt-outs are operational and quickly escalating and resolving bugs help maintain effective opt-outs. For instance, businesses using Google Tag Manager can and should leverage Google Tag Diagnostics to ensure that tags are firing in accordance with consumer choice. Maintaining change logs to record updates and changes is also important to demonstrate your efforts to address compliance even when errors occur. It also is prudent to identify who internally at the business is responsible for auditing the opt-out process and remediating issues. Relying on CMP vendors to proactively spot and address problems is likely not covered in your services agreement with the CMP, and regulators are unlikely to accept this as a justification for failing to comply. Likewise, while the ubiquitous "cookie scan" provides some insight into backend occurrences, it does not resolve the core issues. With that said, some providers are responding to these concerns, and there are new software tools available that are responsive to today's legal requirements in their scanning and what actions they generate for resolution. If this topic is a pain point for your organization, it may be worth

allocating budget for an automated solution versus relying on human effort, but either way, you want to have a clear understanding of what your process is, and how it will instill confidence that your opt-outs are working as intended.

6. **Training.** Businesses must train their teams and maintain records of such training. Practical note: the training should be specific to the business's privacy compliance versus only a general privacy awareness tutorial. If employees are neither provided with a framework and directives, nor armed with the right tools, they cannot properly identify issues let alone address them. Training and documented processes not only provide guidance that can withstand operational siloes and employee turnover, but they also demonstrate the business' efforts to comply in the event of a government investigation. Both should be routinely updated to align with new laws (or updates to existing ones) and changed business practices. For instance, the proposed CCPA Regulations require that if a business uses advertising technology on its website that instantaneously sells and shares personal information and can restrict the transfer of personal information instantaneously, the business ***must*** do so immediately upon receipt of an opt-out rather than within the 15-day compliance timeframe. Such seemingly minor changes may impact technical implementation and should be reflected in documentation provided to employees.

7. **Confirming Scope.** A reminder that the CCPA uniquely applies to job applicants (and employees) and B2B contacts who are California residents, and businesses would be wise to include opt-out health checks for dedicated careers and job applicant pages and B2B digital properties, to the extent applicable. Further, several states – including California, Connecticut (due to a recent amendment), Minnesota, Oregon and Montana (in effect October 1, 2025) – focus their Gramm-Leach-Bliley Act exemption on how the data is processed, and not (or not solely) based on the entity. Accordingly, opt-out compliance on financial service-related sites should also be reviewed and up to date.

By applying a comprehensive strategy, businesses can more effectively spot potential gaps and enhance their opt-out compliance efforts, shifting valuable resources from time-intensive and costly defense tactics to proactively advancing core business priorities. It also can provide the additional valuable benefit of helping businesses mitigate risks from escalating wiretapping (CIPA) claims and more targeted laws with stricter rules or prohibitions on personal information disclosures for targeted advertising.

Alysa Hutnik
Partner & Chair, Privacy & Information Security Practice
ahutnik@kelleydrye.com

Céline Guillou
Special Counsel
cguillou@kelleydrye.com