BCLP. Client Intelligent

Insights

COOKIES BANNERS AND BEYOND: HOW TO AVOID COMMON MISTAKES

Nov 03, 2023

The use of online tracking technologies for online behavioral advertising, analytics and related activities has come under increasing scrutiny by regulators in the U.S., Europe and elsewhere. The obligations under various laws can contradict each other, and there is nothing easy about understanding how to apply the law to the technology. 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 U.S. state level is focused specifically on digital advertising and the related protections provided to consumers, creating meaningful risk that should not be ignored.

With this in mind, we have set out below a set of best practices to help companies better navigate this difficult space.

DO CONSIDER WHICH PRIVACY LAWS APPLY

The first step in the process is to evaluate which laws apply, because the notice and consent obligations vary across different laws. If website users are California residents, for instance, there may be California-specific obligations that must be reflected on the website (*e.g.*, a "Do Not Sell or Share My Personal Information" or "Your Privacy Choices" link, recognition of universal opt-out preference signals, specific disclosures in the website privacy policy), but such obligations apply only with regard to targeted or cross-contextual behavioral advertising cookies. Similar opt-out requirements apply across other new and emerging state laws, such as those of Colorado, Connecticut and Virginia, but the jurisdictional threshold of these laws is not the same as that of California such that they may not be in scope for smaller companies. In Europe, by contrast, organizations are required to obtain express opt-in consent for all but essential cookies. For that reason, it is important to carefully review applicable laws and their obligations to assess whether a global or jurisdiction-specific approach makes more sense, both from a business and a compliance perspective.

DO DECIDE WHETHER TO IMPLEMENT AN OPT-IN OR OPT-OUT APPROACH (AND UNDERSTAND WHY)

It is critical to take the time to understand what approach – opt-in or opt-out – is legally required and/or might offer consistency of approach across the organization, the most meaningful data and/or other benefits to the organization. Companies can also consider whether to put in place different approaches for different regions (opt-in for Europe and opt-out for the U.S.), but again, it is critical to understand why a particular approach is being utilized rather than just proceeding with default configurations or a confusing solution that includes, for example, a cookies banner but also a "Do-Not-Sell or Share My Personal Information" link.

DO PROVIDE EQUALLY WEIGHTED MECHANISMS FOR EXERCISING USER CHOICE

It is not uncommon to see cookies banners configured in a manner that pushes users to simply click "Accept All" and move on. Although it is understandable that companies would want to encourage users to allow them to track their activity on the site and potentially direct advertising their way, leading users to their choice is a pitfall that companies should work to avoid, particularly when opt-in consent is not even necessarily required. Under most privacy laws, consent obtained through coercive or unclear methods is typically not treated as an actual consent and may even be considered a "dark pattern", because it unfairly leads consumers to a particular decision. These missteps may be as simple as requiring users to click through more options to deny cookies than to accept cookies, or setting the color scheme of a cookie preference center in a way that would be difficult for users to read the less desirable option (for the company). Therefore, companies should work to make the options available to users as symmetrical as possible, rather than offering commonly seen solutions, such as "Accept All" and "Adjust My Settings". While this approach may initially be less popular with business teams, companies can expect to see further scrutiny from regulators on this issue in particular.

DO OFFER USERS WITH THE ABILITY TO REVISIT THEIR CHOICES, PARTICULARLY THEIR CHOICES REGARDING TARGETED ADVERTISING

Under most privacy laws, users must be provided with a meaningful opportunity to update their cookies preferences. In the U.S., this requirement generally only extends to targeted advertising cookies, but applies more broadly to all non-essential cookies in Europe *(i.e., behavioral advertising, analytics, performance, and functional cookies).* To do so, companies should provide users with the ability to update their preferences anytime through the website, such as through a persistent opt-out link or icon.

DO MAKE THOUGHTFUL DISCLOSURES ABOUT THE WEBSITE'S USE OF COOKIES

Disclosures about the use of cookies are typically accomplished through a cookie preference center or within a linked privacy or cookie policy. While providing users with disclosures about the website's use of cookies is required under certain privacy laws, it is always important to make sure that any disclosures are accurate and complete, even if not strictly required under applicable law. Therefore, organizations should work to strike the right balance between providing an appropriate level of detail regarding the categories or buckets of cookies and similar technologies used while providing some flexibility for changes in different types of cookies or providers. Certain laws may require more granularity with regard to specific cookies, but this issue can also generally be addressed via the cookies manager (*e.g.*, the listing of cookies in the pop-up screens offered by the cookies manager), which can usually be updated via automated means.

DO CONSIDER OTHER FORMS OF TRACKING TECHNOLOGIES

Online tracking technologies are not limited to cookies alone. There are also pixels, scripts, and similar technologies that may trigger the compliance obligations discussed above. Moreover, some of these technologies 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 risks is available in our previous insight, VPPA trends: considerations for limiting exposure. With these issues in mind, it is important to consider the universe of technologies deployed when developing the related compliance solution.

DO VERIFY THAT THE TECHNICAL SOLUTION FUNCTIONS PROPERLY

Once a cookies management solution has been implemented, it is critical to verify that it operates as intended and as promised to users. For example, if the users can opt-in to certain types of cookies, those cookies should **not** drop if and until the user accepts them. Moreover, if a consumer opts-out of the use of cookies, the relevant cookies must be disabled in accordance with the choice offered to the consumer. These steps should be undertaken even if applicable law does not require that users be afforded rights with regard to cookies, because companies must comply with the promises they make to consumers, even if the underlying promise is not required by law.

There are multiple factors to consider when implementing a cookies solution, and balancing business and legal concerns is not easy in this environment. There is no one-size fits all approach, but working through the process in a meaningful, balanced way will help you come closer to achieving the commercial goals while reducing regulatory risk.

If any questions arise, please contact the BCLP Global Privacy and Security team.

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

Gabrielle A. Harwell

Chicago

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