U.S. Companies Should Think Twice Before Inflicting A Cookie Banner On Their Website Visitors.

August 25, 2020

- Europe's "Cookie Law" is primarily responsible for the cookie banner blight afflicting everyone's web surfing.
- Even if a U.S. business is subject to Europe's General Data Protection Regulation (GDPR), it's not necessarily subject to the Cookie Law.
- The California Consumer Privacy Act (CCPA) doesn't expressly require a cookie banner, but it does require a notice "at or before" collection of "personal information," which may include "cookies" and "internet or electronic network activity."

You've probably noticed that most websites intrude on your web surfing with a pop-up banner informing you that the site uses "cookies." Some even ask you to "consent" to the use of cookies, or boldly insist that your consent will be implied from continued browsing. These pop-ups have become so ubiquitous in the U.S., it's easy to assume that they're required under U.S. law. They're not. The proliferation of cookie banners is due primarily to the European Union's ePrivacy Directive, also known as EU's "Cookie Law," and a failure to appreciate that the ePrivacy Directive is not the same thing as the EU's General Data Protection Regulation ("GDPR"). While the GDPR clearly applies, in some instances, to U.S. companies who have no presence or operations in the EU, the ePrivacy Directive largely does not. Each U.S. company should carefully consider how it uses cookies, and its unique legal obligations, before inflicting a cookie banner on its website visitors.

What are cookies and cookie banners?

A "cookie" is a small text file that is stored in a visitor's web browser to allow the party placing the cookie to distinguish the visitor's browser or device from others. Generally speaking, there are four categories of cookies: essential (for necessary website functionality), preferences (for remembering a visitor's preferences during a browsing session or across browsing sessions), analytics (for analyzing how the site is used), and marketing (typically used to track users across different sites to deliver cross-context behavioral advertising). First party cookies are placed by the operator of the site. Third party cookies are placed by a party who doesn't operate the site—such as an analytics provider, adtech company, or social network—and whose presence on the site may not be obvious to the visitor.

A cookie banner is a pop-up notification that appears on the website, usually when the site first loads in the user's browser, to inform the user that cookies are being used. Some banners include information about who is placing the cookies, the purpose of the cookies, and what information is being collected or shared. Many of these banners appear to declare the presence of cookies as an unavoidable fact of life, but a small percentage ask the visitor to provide specific and affirmative consent to non-essential cookies.

How does the ePrivacy Directive come into play?

The EU passed the ePrivacy Directive in 2002 and amended it in 2009. Its nickname is misleading because it's not actually a law. Rather, it's a Directive to all EU member states to adopt their own laws concerning the Directive's subject matter. In a nutshell, and for purposes of this discussion, the ePrivacy Directive mandates

laws that require covered businesses to give notice, and obtain the user's informed consent, before placing or reading non-essential cookies in a visitor's web browser. And thus, the cookie banner was born.

How do the ePrivacy Directive and GDPR work together?

The EU's General Data Protection Regulation took effect in 2018. Unlike the ePrivacy Directive, the GDPR is a real law; it creates enforceable rights and obligations in EU member states without those states having to pass their own implementing legislation. The GDPR broadly regulates processing of "personal data," whereas the ePrivacy Directive focuses on the electronic communications sector, regardless of whether the processing at issue involves personal data.

The GDPR regulates cookies indirectly, to the extent their use involves the processing of personal data. The GDPR prohibits covered businesses from processing personal data unless one of six "lawful bases" for processing applies. In practice, this often means that a company must obtain a consumer's unambiguous and specific consent prior to the collection of their personal data. This requirement is an indirect driver of cookie banner proliferation.

Because of the overlap between the ePrivacy Directive and GDPR, the European Data Protection Board ("EDPB") issued an opinion in 2019 attempting to clarify that the ePrivacy Directive both particularizes and complements the GDPR, such that the Directive will take precedence over the GDPR where it provides for more specific rules on a particular overlapping matter. However, the GDPR will still apply to the extent the ePrivacy Directive does not displace the GDPR.

In the context of cookies, this means it's possible for both sets of rules to apply where a website is storing and retrieving information that can be considered personal data through the use of cookies. To illustrate this point, the opinion provides an example of a data broker who engages in profiling on the basis of information collected by the use of cookies, which may also include personal data obtained via other sources. The EDPB explains that to be lawful, the placing or reading of cookies must comply with the ePrivacy Directive and the subsequent processing of personal data through cookies must comply with the GDPR. The latter involves having a legal basis for processing the personal data, which can be satisfied through the user's unambiguous informed consent.

What does all this mean for U.S. Companies?

If your company has no physical presence or operations in the EU and isn't a provider of electronic communications services, it may not need a cookie banner at all. That's because the ePrivacy Directive doesn't clearly have "extraterritorial" scope. It applies to activities "in the Community," i.e., the European Union.[1]

Unlike the ePrivacy Directive, the GDPR clearly has broad extraterritorial scope. It reaches not only processing of personal data relating to a business's establishment "in the Union," but also processing of personal data by a business "not established in the Union, where the processing activities are related to" the "offering of goods or services" to EU data subjects or "the monitoring of their behaviour as far as their behaviour takes place within the Union." Simply having a website that's accessible in the EU doesn't bring your business within the GDPR's scope. But if your website targets EU consumers at least in part by, for example, accepting ecommerce payments in Euros as an alternative to U.S. dollars, or if the site's use of cookies amounts to intentionally "monitoring" the behavior of visitors who are in the EU, the GDPR likely applies, and you should at least consider the need for a cookie banner to help comply with the GDPR's notice and consent requirements.

1 Some commentators interpret the ePrivacy Directive to apply to at least some providers of electronic communication services established outside the EU. *See, e.g., The Protection of Computer Privacy Under EU Law*, 21 Colum. J. Eur. L 71, 86 (2014).

The EU has long planned to replace the ePrivacy Directive with a new ePrivacy Regulation, which is still in draft form but would have extraterritorial reach to match that of the GDPR. Due in part to delays resulting from the COVID-19 pandemic, it's unlikely the ePrivacy Regulation will be finalized and adopted any sooner than 2021, at the earliest.

What does the CCPA have to say about cookies and cookie banners?

The California Consumer Privacy Act ("CCPA") is similar to the GDPR in many respects, but it doesn't require a "lawful basis" for processing personal information. It covers any for-profit organization doing business in California that: (i) has annual revenues of more than $25 million, or (ii) annually collects the personal information of more than 50,000 California residents, or (iii) makes more than half of its annual revenue from selling Californians' personal information.

The CCPA doesn't expressly require a cookie banner. But, it defines personal information to include, among other things, "cookies, beacons, pixel tags, mobile ad identifiers or similar technology," and "internet or electronic network activity," to the extent that data "could reasonably be linked, directly or indirectly, with a particular consumer or household." The CCPA also requires a covered business to provider notice to consumers "at or before the point of collection" of the categories of personal information to be collected and the purposes for which they will be used. The CCPA's implementing regulations, which took effect on August 14, 2020, specify that when "a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing" the information required in a notice at collection. The regulations offer an example of "a pop-up window when the consumer opens the application."

What should my business do?

Every business subject to the CCPA should carefully consider whether its use of cookies amounts to collection of personal information from website visitors or mobile app users. If it does, the business must further consider whether a "just-in-time" notice is required to satisfy the notice at collection requirement. A pop-up banner is one way to provide a just-in-time notice, but it should emphasize the categories of personal information collected and the purposes for which they'll be used, rather than simply informing the consumer that the site or app uses cookies. Remember, unlike the GDPR and ePrivacy Directive, the CCPA generally doesn't require affirmative consent to use cookies or collect personal information, only advance notice of collection to the consumer, so the CCPA may leave some leeway for less intrusive pop-ups.[2] The business should consult with an expert legal advisor to confirm that a proposed pop-up banner, or other notice at collection, is consistent with both the CCPA and its implementing regulations in the context of the business's overall operations and data flows. At Stradling, we've counseled many companies on these issues and would be happy to help yours.

Authors:

Travis P. Brennan
949.725.4271
tbrennan@sycr.com

Mayant Luk
949.725.4057
mluk@sycr.com

2 The CCPA does require opt-in consent from minors (under 16) or their parent/guardian (for minors under 13) if the business intends to sell the minor's personal information.