BCLP. Client Intelligent

RetailLawBCLP

SURVEY OF PRIVACY PRACTICES: ONE QUARTER OF U.S. RETAILERS BLOCK EUROPEAN VISITORS

Jan 31, 2020

Our Survey of the Retail Industry's Privacy Practices discloses that 25 percent of U.S. retailers have decided to block European visitors from reaching their websites.

There are two situations in which the GDPR purports to apply extraterritorially to companies that have no contact to the European Union. The first situation, described in Article 3(2)(a) of the GDPR, occurs when a company that has no contacts with the European Union "offer[s] goods or services" to a person that is located in the European Union. The second situation, described in Article 3(2)(b) of the GDPR, occurs when a company that has no contacts with the European Union "monitor[s]" the "behaviour" of someone "as far as their behaviour takes place within the Union."[1]

While the GDPR implies that merely having an internet website that is accessible to European Union residents is not enough for the GDPR to attach, there is uncertainty about whether a European supervisory authority might attempt to apply the GDPR to a website that is accessible to European Union residents. Some companies have attempted to mitigate that risk by geofencing their websites – i.e., blocking any individual from visiting their website from a European IP address.

In order to help companies understand and benchmark industry practices, BCLP randomly selected a sample of 33 percent of the Fortune 500 companies identified as being predominantly within the "retailing" sector and then visited their homepages from a server with an IP address in the United States and from a server with an IP address in Europe.[2] As of January 13, 2020, 25 percent of Fortune 500 retailers had blocked their websites from being visited by European IP addresses.

Configuration of Cookie Notices

The European Data Protection Board has issued guidance that states that the application of Article 3(2)(b) "could . . . encompass a broad range of monitoring activities, including in particular: Behavioural advertisement . . . [or] Online tracking through the use of cookies or other tracking techniques such as fingerprinting."[3] This suggests that a website that does not offer a good or service to Europeans might still be subject to the GDPR if it deploys tracking cookies. The EDPB went on to say, however, that in order for monitoring jurisdiction to apply, it is "necessary to consider

the controller's purpose for processing the data and, in particular, any subsequent behavioural analysis or profiling techniques involving that data."[4]

As website operators typically do not have access to the data collected via third party cookies (e.g., behavioural advertising networks) and, therefore, are arguably not controllers with respect to that data (let alone capable of analyzing or profiling data subjects from the data), the EDPB's guidance suggests that a website operator may not trigger the application of the GDPR by permitting a third party tracking cookie to be deployed. In connection with first party tracking cookies (i.e., those owned and controlled by the website operator), the guidance suggests that the GDPR would only be triggered if the operator used the information obtained from a cookie in order to conduct behavioral analysis specific to the data subject. The guidance did not specify, however, the extent to which a company must engage in behavioral analysis before jurisdiction under Article 3(2)(b) would be triggered. For example, there may be a distinction between a website that deploys a first party cookie which is intended to track a user over time and across multiple websites that are owned by a single company in order to create a long-term profile, and a single session cookie that may profile a user and provide recommendations based upon the users' behavior over a short period of time (e.g., one session).

One strategy considered by many United States companies for mitigating the risk that a supervisory authority might determine that a United States retailer that deploys behavioral advertising cookies is subject to the GDPR is to deploy a geofenced cookie banner – i.e., one that seeks opt-in consent before the deployment of cookies from website visitors that utilize a European IP address, but does not require opt-in consent before the deployment of cookies from website visitors that utilize a United States IP address.

Based on BCLP's survey of a randomly selected sample of 33 percent of the Fortune 500 companies identified as being predominantly within the "retailing" sector , as of January 13, 2020, 5 percent of Fortune 500 retailers deployed a geofenced cookie banner that required opt-in consent from European visitors, but did not require opt-in consent from United States visitors.

Frequency of Cookies

While some companies block European visitors from accessing their websites, and other companies configure a cookie notice to prompt only European visitors for opt-in consent, other companies choose to simply drop a smaller quantity of cookies on European visitors.

As part of BCLP's survey, after excluding from the sample population those companies that blocked European visitors or sought the consent of European visitors to the deployment of cookies, BCLP measured the quantity of advertising cookies that were deployed.[5] As of January 13, 2020, Fortune 500 retailers deployed, on average, 18 percent more advertising cookies on visitors with a United States IP address as compared with visitors with a European IP address.

This article is part of a multi-part series published by BCLP to help companies understand and implement the General Data Protection Regulation, the California Consumer Privacy Act and other privacy statutes. You can find more information on the CCPA in BCLP's California Consumer Privacy Act Practical Guide, and more information about the GDPR in the American Bar Association's The EU GDPR: Answers to the Most Frequently Asked Questions.

---

[1] GDPR, Article 3(2)(b).

[2] Websites were visited from as server in Paris France with the following IP: 139.28.219.252.

[3] EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation (16 Nov. 2018) at 18.

[4] EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation (16 Nov. 2018) at 18.

[5] Cookies were identified and classified using Ghostery for Chrome Version 8.4.4.

RELATED PRACTICE AREAS

- Retail & Consumer Products

MEET THE TEAM

Merrit M. Jones

San Francisco

merrit.jones@bclplaw.com
+1 415 675 3435

---

consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.