

Guidance from European Data Protection Board Requires Consent for Tracking

December 28, 2023 – *The TMCA*

by Dustin Berger

The European Data Protection Board (EDPB), a board comprised primarily of representatives of the data protection supervisory authorities of the European Union's member states, issued surprising new guidance in mid-November explaining how a key component of the European Union's ePrivacy Directive applies to variety of commonly used technologies used for tracking on the internet.

Article 5(3) of the ePrivacy Directive^[1] (EPD) has long been a cornerstone of internet and privacy law in the European Union (EU). Under the directive, EU member states were required to pass laws that limited "the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user" to situations where the subscriber or user has been provided "clear and comprehensive information" about the practice and, thus informed, provided consent. The sole exceptions to this requirement are as necessary to transmit the user's communication over a network or "as strictly necessary in order for the provider of [a service] explicitly requested by the subscriber or user to provide the service."

Related People

- Dustin Berger

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation



This aspect of the EPD has long been understood to apply to the cookies stored in users' web browsers. Indeed, the EPD is often colloquially referred to as the "EU Cookie Directive." It was logical that the EPD applied to cookies because cookies were designed with the express intention of allowing a website provider to store information in a user's web browser for later retrieval.

Cookies, however, are not the only ways in which a website operator or mobile app provider can store or access information in a user's terminal equipment. Earlier guidance from the EDPB also confirmed that the EPD also applied to the tracking of a user through the practice of "device fingerprinting."

The EDPB's new guidance, entitled "Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive," goes further. It clarifies that the EPD also applies to many newer tracking technologies, many of which are ubiquitous components of the ad-supported internet. The guidance clarifies that the EPD always applies when four criteria are met: (1) the operation in question relates to information; (2) the operation relates to a subscriber's or user's "terminal equipment"; (3) the operation is made in the context of a publicly available electronic communications service on a public network; and (4) the operation involves "gaining of access" or "storage." The EDPB guidance interprets all of these elements broadly enough to cover most or all tracking technologies in use on the internet.

For instance, the EDPB's guidance explains that the EPD applies to tracking of users by means of tracking pixels or tracking links. Tracking pixels are hyperlinked resources that are embedded into content to enable the collection of information about the users of the content. The information might be collected by the sender of the content or by a third party that aggregates tracking data. Tracking pixels also often contain additional information that facilitate tracking across pages, websites, and devices. Tracking links are web links that include additional information to facilitate tracking. The EDPB explains that tracking links are used, for instance, to enable e-commerce partners to identify and

pay commissions to referral sources. In both contexts, the EDPB finds that the tracking meets all four of the criteria for the applicability of the EPD: information is both stored on and accessed from the user's terminal equipment in the context of a public internet service.

The EDPB guidance reaches the same conclusion with regard to tracking based on "local processing" or "processing instructed by software distributed on users' terminal, where the information produced... is then made available to selected actors" by the software. The EDPB explains that if local code sends information "back over the network... such an operation (instructed by the entity producing the client-side code...) would constitute a 'gaining of access to information already stored.'" This reasoning almost certainly implicates many common tracking technologies, such as Google Analytics, that operate through JavaScript code that execute within a client's web browser. It also would almost certainly implicate tracking embedded in mobile apps running on users' tablets and smartphones.

The EDPB also explains that, under analogous reasoning, tracking via IP addresses and unique identifiers (even identifiers that are inherent in user authentication) also falls within the technical scope of the EPD.

Of course, the fact that these tracking technologies fall within the scope of the EPD does not mean that these technologies cannot be used. However, it does require the providers and operators of these tracking technologies to provide users with information about the tracking and to collect users' consent to the tracking before it begins. This will require providers and operators of tracking technologies to modify their websites and mobile apps to provide this information and to obtain and track users' consent. Because the EDPB's guidance is an interpretation of existing law, users of tracking technology will have no grace period to enact these changes before enforcement efforts can begin.

[1] The directive was originally issued as "[Directive 2002/58/EC](#) of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector" and amended in 2009 by "[Directive 2009/136/EC](#)."