

OFFLINE TRACKING



WHAT IS “OFFLINE TRACKING”?

Offline tracking is the way you can be tracked using other information than your online communications data. The location of your device (tablet, phone, pc) can be easily and accurately identified if it is connected to, for example, a public Wi-Fi or to a cell tower. Sometimes, this tracking is technologically impossible to evade: If you want to receive a call in your cell phone, your phone provider needs to find your phone in order to send you the call. In other situations, the location of your device as you move through a specific location (for example, a shopping mall) is used for different purposes (such as trying new ways to catch your attention, to analyse which shops are most visited...).

WHY IS THIS IMPORTANT?

This type of technology is highly intrusive. It is already widely in use and is not limited to busy shopping malls but is also used, for example, to map traffic flows on roads. The collected data not only reveals the behaviour of passers-by, but also includes individuals living in the neighbourhood. Moreover, in some contexts, such as in the vicinity of a religious establishment, a medical clinic or a sex shop, this information should be considered to be sensitive by default. The European Commission proposes permitting this type of tracking, provided there is some sort of notification to the individual. EDRi believes that the notification to the individual does not contribute to the essential protection of the rights and freedoms of the individual. Also, the Commission’s proposal makes the incorrect assumption that there would be so few tracking networks that such an opt-out system could work in practice.

EDRi recognises that location services can provide benefits to society, for example traffic planning in cities based on measurements of traffic congestion and travel times between different points in the city during the day. However, obtaining this information through tracking of individual citizens poses severe privacy risks and possibilities for abuse (including the risk of mass surveillance by commercial or law enforcement entities).

WHAT SHOULD THE E-PRIVACY SAY ABOUT IT?

EDRi believes that the text around location privacy should be strengthened. The current e-Privacy Directive was drafted with concerns about the expansion of location based services, at the time based on proximity to GSM phone masts. The Directive treats location data as a separate category with more stringent rules, requiring clearer information on processing and extra opportunities for opting out.

In most cases, there are better solutions to obtaining location-based information than centralised tracking of individual citizens. Smartphone apps can obtain the device location (e.g. through GPS) without leaking it to a third party. Technical solutions based on local computation in the end-user’s device should always be preferred over centralised tracking. The ePR should provide an incentive to develop technical solutions where citizens can provide location data to services without any privacy risks (privacy by design).

Do you want to know more? Check out our series of blogposts [“Your privacy, security and freedom online are in danger”](#) and our [Document pool on e-Privacy!](#)

