Real Time Bidding (RTB) - An Unprecedented Privacy Breach

Oct 12th 2020

A typical programmatic Real Time Bidding (RTB) transaction begins with a user visiting a website or loading an app. This triggers a bid request that can include various pieces of data such as the user's demographic information, browsing history, past purchase and search histories, location, and the page being loaded. The bid request goes from the publisher to an auction house, known in the industry as an ad-exchange. At each ad-exchange, tens or hundreds of tech companies who represent prospective advertisers, merge the presented bid request information with prior knowledge each of them "owns" about the individual to decide whether to place a bid to show an ad. The impression goes to the highest bidder and their ad is served on the page. This all happens in an instant (less than 100 milliseconds).

The problem with the RTB "supply chain" is that it comprises many different actors and service providers, with a significant lack of transparency due to the inherently private nature of auctions. Once the bid request information is broadcast to the very large number of auction participants, the website publisher permanently loses control of the data. The core privacy concern is that oftentimes, the data contained in the bid request is sufficient to infer the individual's ethnicity, sexuality, income, health, and other highly personal and private information. Furthermore it is in the self-interest of each auction participant to build up, and store in perpetuity, a detailed dossier on each individual by piecing together multiple bid requests over time.

Given the scale and scope of breach of privacy that it facilitates, RTB is (finally) attracting attention from privacy regulating bodies such as the UK's Information Commissioner's Office.

Source : ICO Report