# Report from Dr Johnny Ryan – Behavioural advertising and personal data

*This is a translation of an extract of the full report available at:*
https://brave.com/Behavioural-advertising-and-personal-data.pdf

**How personal data are used in behavioural online advertising.**

Every time a "behaviourally" targeted advert is served to a person visiting a website, the system that selects what advert to show that person broadcasts their personal data to hundreds or thousands of companies. This system is known as "Real-time bidding", or sometimes referred to as "programmatic" (which simply means automatic) advertising. The personal data shown include the URL of every page a user is visiting, their IP address (from which geographical position may be inferred), details of their device, and various unique IDs that may have been stored about the user previously to help build up a long term profile about him or her.

Despite the grace period leading up to the GDPR, the AdTech industry has built no adequate controls to enforce data protection among the many companies that receive data.

**How personal data are "broadcast".**

A large part of the online media and advertising industry uses a system called "RTB", which stands for "real time bidding". There are two versions of RTB.

● "OpenRTB" is used by most significant companies in the online media and advertising industry.

● "Authorized Buyers", Google's proprietary RTB system. It was recently rebranded from "DoubleClick Ad Exchange" (known as "AdX") to "Authorized Buyers".

Google uses both OpenRTB and its own proprietary "Authorized Buyers" system.

The specification documents are publicly available for both versions. The documents reveal that every time a person loads a page on a website that uses real-time bidding advertising, personal data about them are broadcast to tens - or hundreds - of companies. Here is a sample of the personal data broadcast.

● What you are reading or watching

● Your location (OpenRTB also includes full IP address)

● Description of your device

● Unique tracking IDs or a "cookie match" to allow advertising technology companies to try to identify you the next time you are seen, so that a long-term profile can be built or consolidated with offline data about you

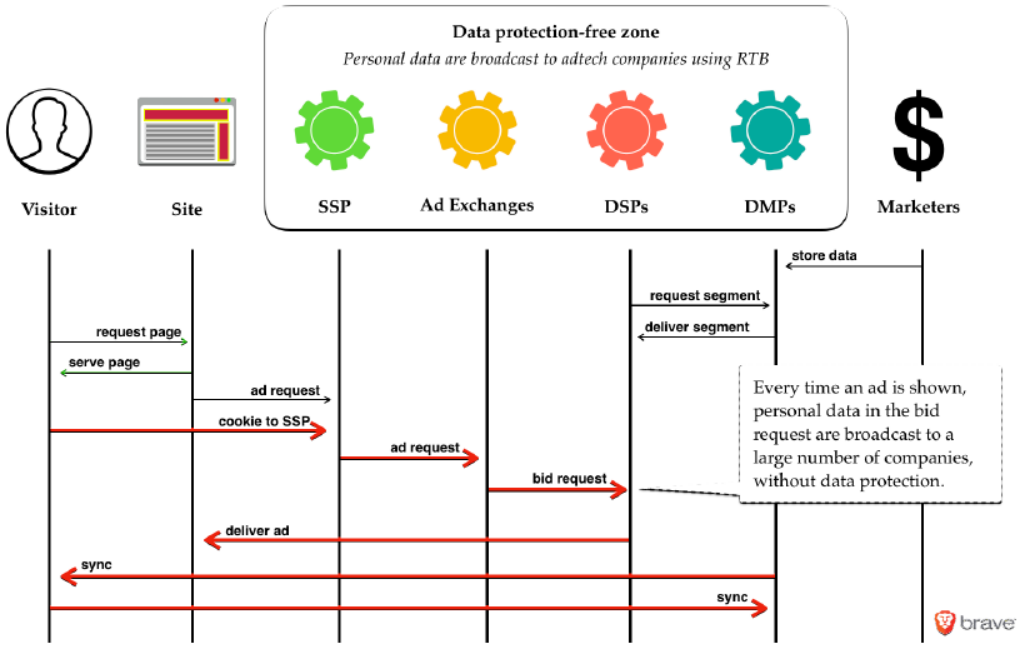
● Your IP address (depending on the version of "RTB" system)

● Data broker segment ID, if available. This could denote things like your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc. (depending on the version of "RTB" system)

A more complete summary of the personal data in bid requests is provided in the original English language report, in Appendix 1. and 2. Relevant excerpts from the specification documents are presented in Appendix 3 and 4.

**How it works**

A diagram of the flow of information is provided below.




The broadcast of personl data under RTB is referred to as an “RTB bid request”. This is generally broadcast widely, since the objective is to solicit bids from companies that might want to show an ad to the person who has just loaded the webpage. An RTB bid request is broadcast on behalf of websites by companies known as “supply side platforms” (SSPs) and by “ad exchanges” to multiple “demand side partners” (DSPs), which then decide whether to place bids for the opportunity to show an ad to the person in question. The DSP acts on behalf of an advertiser, and decides when to bid based on the profile of person that the advertiser has instructed it to target. Sometimes, Data Management Platforms (DMPs) can perform a “sync” that uses the data to contribute to their existing profiles of the person.

RTB establishes no control over what happens to the personal data once an SSP or ad exchange broadcasts a “bid request”. Even if bid request traffic is secure, there are no technical measures that prevent the recipient of a bid request from, for example, combining them with other data to create a profile, or from selling the data on. Once DSPs receive personal data they can freely trade these personal data with business partners, however they wish.

This is particularly egregious since the data concerned are very likely to be “special categories” of personal data. The personal data in question reveal what a person is watching online, and often reveal specific location. These alone would reveal a person’s sexual orientation, religious belief, political leaning, or ethnicity. In addition, a “segment ID” that denotes what category of person a data broker or other long-term profiler has discovered a person fits in to.

To summarize, in this system of advertising there is no personal data protection. This is a widespread and troubling practice. The scope of the industry affects the fundamental rights of virtually every person that uses the Internet in Europe.