

Privacy First CDP activation across authenticated and unauthenticated users.

Carsales created a IPD segmentation & Identity strategy that utilises advanced encryption algorithms to protect consumers, the Carsales business & their partners from data exposure risks.



OBJECTIVES

Carsales wished to move beyond simple CDP / IPD data management.

With increased regulations and growing device/browser limitations; a need to flexibly activate and control data compliantly across existing and future ecosystems was required..



CHALLENGES

- CDPs themselves are not an ID generation and management solution (some CDPs can manage IDs to varying extents, but they are not fit for purpose, truly owned, and privacy preserving to drive sustained long-term value)
 - CDPs will only build a cohesive view of your customers by stitching to an owned 1st party Identity solution. The really good CDPs will dynamically reconcile identity-based on multiple fragments in real-time
 - Moving into a world where CleanRooms and Data Partnerships are required, IPD identity management becomes vital.

AT A GLANCE

- Using an AdFixus ID, Civic Data & Carsales ensured the consumer's digital identity is stored in a first-party context, with their consent, on their consumer device.
- This is protected from exposure risks through the utilisation of advanced encryption algorithms (the same as those used in blockchain).
- Data exchange occurs in a first-party, controllable environment, and enables activation through regular programmatic channels as well as direct sales channels.
- Providing a foundation upon which collaborative data partnerships can be built.



REMOVING PII RISKS ASSOCIATED WITH FORCED AUTHENTICATION

Today most browsing on the internet is unauthenticated, with relevancy being driven through the use of cookies.

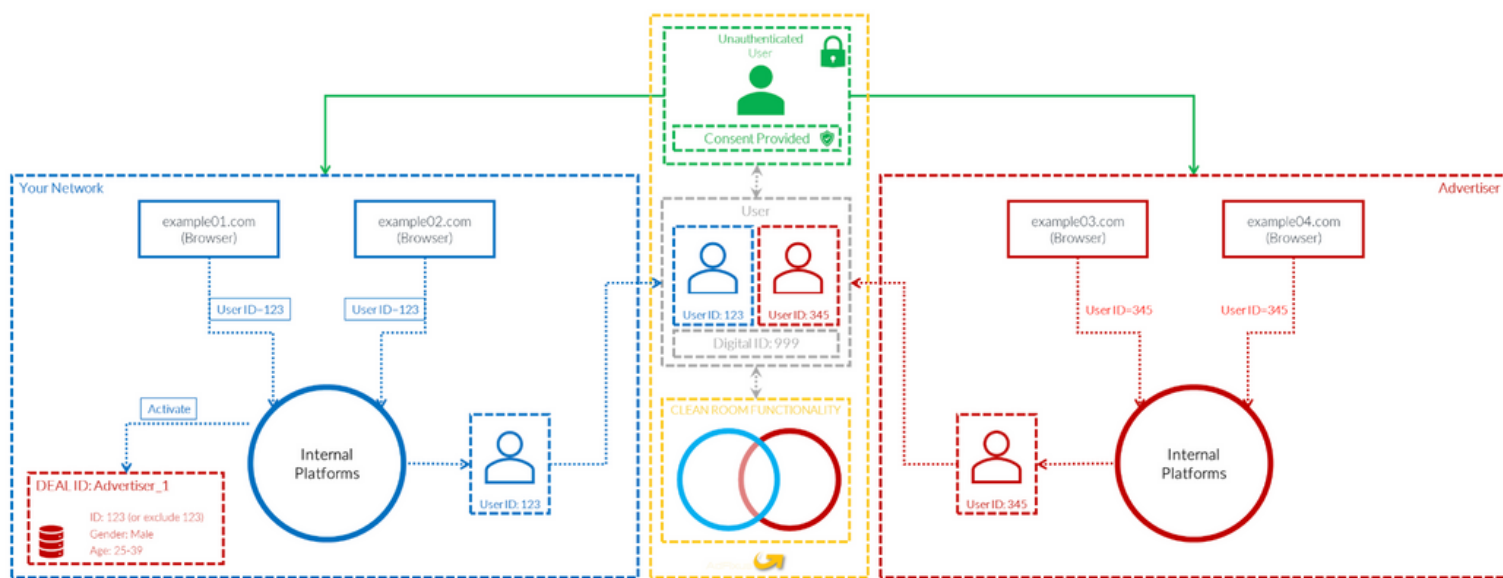
Diminishing support for third party cookies is making providing relevant content to unauthenticated users challenging, forcing businesses to drive consumers to log-in and provide their Personal Identifiable Information (PII) for marketing purposes.

Increasing the number of logged-in users is just one strategy. This will never be all encompassing for the vast majority of online businesses.

There will also always be limitations on the utilisation of PII data for marketing purposes like retargeting, matching and activation

Recent developments related to decentralised technologies, increased privacy regulation and tightened privacy protection at a device and browser level illustrates a future where Internet users remain to be largely anonymous.

The future for a privacy-preserving internet economy suggests the necessity for robust control of the varying forms of PII data (OPD, IPD, 2PD, 3PD, etc.). At the same time, organisations must maintain a relationship with an anonymous consumer in a compliant manner to deliver relevant experiences & power future proofed revenue models.



The above approach, using Adfixus' encrypted first party identity solution as part of the ecosystem, allowed Civic Data to provide Carsales with a methodology that connects all their brands together, even across separate domains, through a single identity. It enabled them to maintain a relationship with the consumer, regain reach & frequency visibility across domains, whilst ensuring that they secure their first party data & user trust at all times.