AD TRUTH &
3rd PARTY COOKIES FACT SHEET

INTRODUCTION

Struq is in partnership with Adtruth who are a thought leading provider of Device Fingerprinting

WHAT IT IS

AD TRUTH

By collecting information from your device, such as the IP address, device model and device settings, finger printing is able to create a unique user ID for each device. When a user visits a website the information is collection and stored. When the user returns to the website the ID is matched. IDs normally last for about 30 days.

3rd PARTY COOKIES

These have become the cornerstone of the digital advertising industry. A 1st party cookie belongs to the user. When a user requests a website to remember their login, a 1st party cookie is created. It is a way for the users computer and the website to reconise each other in the future. A 3rd party cookie is a cookie created by a outside source, such as retargeting company. They use the cookies to track the users activity on a website. Retargeting companies use this information to retarget ads.

WHAT IT ISN'T

Ad Truth does not collect any personable identifiable information. The device ID is stored on clients severs and not consumers devices and as a result does not leave residue on the device

Cookies also do not collect any personally identifiable data. A cookie knows what you look at and what you do BUT doesn't know who you are, your gender, where you live etc.

HOW IT WORKS FOR ADVERTISING?

Retargeting site visitors and buyers has not been historically possible on mobile devices due to their lack of support of third party cookies. With device finger printing, companies can track a device's ID and retarget ads according to the information they have previously collected.

When a user visits a website, a 3rd party cookie is stored on their device and records their activity. A retargeting company can then use this information to retarget ads based on the users previous activity, personalising ads and delivering only ads relevant to the user.

WHAT CAN'T IT DO?

Device fingerprinting can't track a device that travels between geos: If a user looks at a website at work on their mobile device, it is recorded to that location's ID. When they return home and use their mobile device, the information is not carried over from their work location ID. If the user went back to work the next day, the device ID would match that of the previous day, so in this way the life-span is location specific, but not time-limited.

Cookies can't access places that don't support 3rd Party cookies i.e. cookie blocked browsers, mobiles or tablets

HOW GOOD IS IT FOR PERSONALISATION?

Device Fingerprinting is a very strong indicator within the cookieless environment and enables Struq to:

- Better target ads and deliver relevancy based on demographics and user history.
- Improve online audience targeting across any Internet connected device to enable more efficient advertising spend.
- Struq to set frequency caps.
- Link more digital activity to recognised devices over a longer period of time.

Superb as it enables Struq (or other 3rd Party cookie providers) to understand what a user is interested in and allows us to personalise the ad to the user.

WHAT HAPPENS WITH MULTIPLE SIMILAR DEVICES IN THE SAME LOCATION. I.E. A HOME WITH THREE IPADS ALL USING IOS7?

The likelihood of all the 3 devices having the same AdTruth ID is possible only when all the 3 devices are new and bought at the same time. Even if all 3 devices are using iOS7, the settings within those devices will be different to each other (the chances of the 3 devices being the exactly same are minimal) thus generating different AdTruth Ids.

Cookies are stored directly on the device, giving each device a unqiue history.

AND WHAT HAPPENS IF ONE USER MOVES DEVICES IN THE SAME LOCATION?

Device fingerprinting doesn't offer anything for cross-device tracking, given it's very nature. It identifies devices. Seperate technology would be required to track users across devices, for example first party data.

Cookies are unable to track across different devices. Cookies only track the activity of the user on which the 3rd party cookie