NOVEMBER 2021

PART 1 OF 4

PRIVACY IN PROGRAMMATIC

EVOLVING DATA PRIVACY FOR ALL OF US

AUTHORS

Daniel O'Connor, Quantcast

June Oh, MediaMath

Kevin Taulera, Smart Ad Server

Addy Cutts, Oracle Advertising

Eimear O'Rourke, Xandr

This is the first of a four part series, where we will be looking at the journey to date on privacy in programmatic and the implications for programmatic buyers, sellers and data providers in the future. The first of this series explores where we are and how we got to this point.

The world of data privacy has always been important for our industry, and the end user that funds the majority of the online content we enjoy. However, in recent times, the microscope has zoomed in on the way users' data is used, what is being collected, and the users' options when it comes to consent. This is a good thing as, up until the last couple of years, a large proportion of the online audience weren't fully aware of how their personal data was being used, and for what purpose. One of the key challenges is getting the consumer to understand the value exchange between personalised advertising online and the content and entertainment they enjoy.

REGULATIONS FROM GOVERNING BODIES

The major shifts in data privacy for the online world began in 2018 with the introduction of the General Data Protection Regulation (GDPR), which is a strict privacy and security law that was drafted and passed by the European Union (EU). It imposes obligations onto organizations anywhere, if they target or collect data related to people in the EU. It is a similar story in California, whereby they followed suit shortly after and passed their own version of a consumer data privacy act, the California Consumer Privacy Act.

Looking to Asia, on 1 May 2021 China's top regulators made it more challenging for apps to collect personal data such as location and biometrics. This new series of laws will ensure leading enterprises are more cautious in their methods of collecting user data. In Southeast Asia, Thailand looks to be the first to adopt similar regulation to the EU/US with the (delayed) introduction of the Personal Protection Data Act, the first local law that governs data protection in the digital age. It's fair to assume that other countries in Asia could follow a similar path, where consent from the users and choices on how their data is to be used will become more prominent.

BIG TECH SHIFTS THEIR POSITIONING ON PRIVACY

Increased regulation is one of the major reasons we are seeing such a seismic shift in internet browser settings and the associated targeting and tracking of advertising. The major browser change that has occurred since 2017 has been the removal of 3rd party cookies. Third party cookies are small blocks of data created while a user is browsing a website and placed on the user's device. They have been the default method, albeit a bit archaic, to track browsers' behaviour across the web. While Firefox and Safari have essentially been third party cookie free since 2018, last year Google announced they would also be removing them from their browser Chrome. This will mean a vast majority of web browsers will not have third party cookies running.

In June 2020, Apple announced iOS 14 updates that, among other changes, require apps to ask users for permission to collect and share data using Apple's unique device identifier (the ID for Advertisers or "IDFA"). App developers using the newest version of the mobile operating system must comply with Apple's AppTrackingTransparency framework, which requires app developers to use a permission prompt for activities that Apple calls "tracking". This framework requires all apps to ask users for permission to (1) receive and use Apple's IDFA and (2) link certain data the developer receives from third parties. Applications not complying with the Framework risk being blocked from the App Store. iOS penetration is around 15% in Southeast Asia and 3% in India.

With these changes to browsers and mobile devices coming into effect, advertisers and their partners will find it harder to reach people who have expressed interest in their brands, to deliver ads that feel relevant or useful to their customers, optimise their ads towards conversion and accurately measure, attribute and report campaign results.

These changes also have an impact on the overall user experience for ads. While 97% are somewhat or very concerned about protecting their personal data, 91% of consumers say they are more likely to shop brands who recognize, remember and provide them with relevant offers and recommendations.

With strict data and privacy frameworks being rolled out, consumers are at risk of experiencing a digital world going back to a higher volume of non personalized ads characteristic of mass media and creating a less than ideal experience. It is important for businesses and their customers to strive for both data privacy and personalization, so that people are getting the benefit of relevant advertising and have more confidence that their data and privacy choices are protected.

WHAT NEXT?

As an industry, we need to explore better methods to protect users' privacy and inform them of how their data is being used. When it comes to programmatic, new identity solutions are being formed. The likes of LiveRamp , Lotame and Unified ID2.0 are gaining popularity in Asia, which are built from hashed and encrypted email addresses and/or unauthenticated signals like timestamps. Google is opting for a cohort approach whereby individual browsers are bucketed into cohorts or groups of users, to keep the individual anonymous, but still enabling targeted advertising. Facebook is investing in a multi-year effort to build a portfolio of technologies that minimize the amount of personal information it processes, while still allowing advertisers to show people relevant ads and measure ad effectiveness. These are all upgrades on the 3rd party cookie and other existing technologies, but most importantly are a far more secure and privacy-first approach for the consumer. It also helps the consumer continue to enjoy the free content and platforms on the web that is predominantly funded by advertising.

So, what does this all mean going forward? Well, there are going to be a lot of considerations that publishers, marketers, agencies and data providers will need to address. If we are going to continue to be able to operate and offer targeted advertising to the user, companies need to get used to these different ID solutions, and different privacy laws that are likely to come into effect in Asia. Much like they have in both the EU and the US, data privacy is only going to become stricter on how it is able to be used across the open web. Part Two of this series will explore the implications from a publisher perspective, and what this means to them.