Ad Tech’s Data Leakage Problem Begins with Contract Talks

The mysterious exchange of people’s online information starts with pen and paper.

Contract negotiations between buy-and sell-side advertising platforms are what kickstart the aggregation and selling of user data for the purpose of serving targeted ads, but lawmakers and regulators are ramping up scrutiny of these opaque data practices, since data can easily fall in the hands of bad actors.

Supply-side platforms typically disallow or limit secondary uses or retention of data, which is gathered from a publisher during a real-time ad call, in their standard contracts with demand-side platforms.

However, a DSP—especially one with significant buying power—can set its own terms with an SSP and ask to use that valuable data collected during an ad auction however it sees fit. The two sides are then locked in negotiations around data usage, with the large DSP usually winning out since the SSP can’t afford to lose the DSP’s business.

Kelly McMahon, svp of global operations at SpotX, said there are typically negotiations around privacy clauses stating what a DSP can do with the data it gathers during the real-time bidding process. She said SpotX is “very strict on our language” with DSPs, which are only allowed to use data gathered from its platform for targeted advertising purposes.

Privacy clauses could stipulate that data is deleted immediately upon use or after 30 days, for example.

Data ethics vs. financial incentives

Lawmakers want to regulate ad tech's data collection and sharing process, since information gathered from online ad auctions can easily be used for non-advertising purposes, like selling location data to the government to track immigrants or to target people based on their race or religion.

An SSP's standard contract may have strict language to prohibit such unsavory secondary uses, but that language often gets changed when negotiating partnership terms with large DSPs.

"That [language] does get changed, and that's probably the biggest contentious point of negotiation, is data usage," an SSP executive who asked to speak anonymously because negotiations with vendor partners are private, said.

DSPs make money on take rates, a percentage of media they earn for every ad they help fill. They also make money selling data, packaging information gathered from the bidstream as audiences that are sold to third-party data brokers, brands or agencies.

SSPs typically have audit clauses in their contracts with DSPs, which allow sell-side entities to examine a partner's data practices in the event of a possible misuse or breach of contract. These audit clauses incentivize vendors to behave, but they're rarely enacted because it's hard to tell when data misuses occur and from where they originate.

"If you put data audit rights at a log-file-level … in a contract, they [the DSP] fear it," Paul Cimino, data strategy lead at Prohaska Consulting, said. "But I don't think a lot of that goes on, and I've never heard of anyone auditing anybody in the digital advertising space."

Both McMahon and the source said their companies have audit clauses with DSPs, but neither have triggered them.

Publishers have said data leakage undermines their business. Since SSPs represent publishers, they stand to protect their data.

Not all SSPs are innocent, however. Cimino explained that since SSPs often resell inventory and aren’t directly connected to publishers, they often have sizable data-selling businesses to help those practices.

Ad-tech companies can gather bidstream data, such as a user’s location and IP address, without bidding on an ad. SSPs can limit this practice by instituting spend minimums, which drive smaller DSPs or data companies with small media practices off their platform.

Continue Reading

https://www.adweek.com/programmatic/ad-techs-data-leakage-problem-begins-with-contract-talks/