Information Trust Exchange Project | www.infotrust.org

Cookies vs. Cohorts: Comparing old and new

Created March, 2016 by Don Marti
and Bill Densmore

Comparing third-party cookie-based digital advertising system ("old") with ITE shared-user network ("new")

	Old system: "Cookies" targeting individuals	**New system: Cohorts in profile books**	**Advantage**
Reaching users	Same user can be tracked to multiple sites	User can only be reached as part of a site audience	Take high-value sites out of competition with low-value and fraud sites to reach the same users.
Fraud	Legit sites depend on third-party services to show they have legit users. Fraud sites can and do use the same third parties.	Users share attributes only with sites they trust. Legit sites can aggregate attributes that fraud sites do not have access to.	New fraud metrics can depend on data where legit sites have an advantage over fraud sites.
Performance	Ad is matched to user in real time, while page loads. Dozens of "cookie calls" and scripts clog browser response and slow user experience.	Ads are matched to site audiences, asynchronously. Most processing occurs in server/cloud rather than in browser.	Move placement calculations off the critical path of page loading and rendering. Enable more sophisticated calculations for agencies, and improve page load times and responsiveness for users.
Signaling	An ad may be a low-information "cold call" that user has incentive to block. Ads appear unpredictably on sites that may be inappropriate.	Ad is matched to the content site, so many users in a local area or community of practice may see it. Ads "make sense" to viewer.	Less likely that ads are economically rational to ignore. Lower incentives to block ads.
Deceptive advertising	Easy for deceptive advertisers to buy low-priced, fraud-vulnerable user demographics.	All readers of the same content see the same ad.	Less cost-effective for deceptive advertisers to selectively connect with victims. Shift deceptive offers to other media.
Identity and "cookie" management	Third-party cookies allow a plurality of parties unknown to user to assemble and trade untrustworthy and varying profiles of user for unknown purposes.	User can deploy safe tracking protection services that block third-party cookies responsible for privacy challenges and slow user experience.	User can make their identity opaque to bad-actor advertisers, while managing enhanced identity for publishers and advertisers they choose to trust.
Price management	Users can be readily presented with different offers based on third-party data which affects price without their knowledge or consent.	Users choose what data to share, and can choose not to share attributes that could result in ending up in a higher-price category.	Make the medium more trustworthy. Increase user feeling of empowerment and lower incentives to block ads.
Service Management	Content and other services are presented in "silos" because there is no open standard for sharing user identity attributes that could provide for multi-site services.	Users can opt into collaborative subscription services enabled by the network logging and settlement of activity.	Allow transparent, competing offers of tiered pricing and content access based upon marketplace innovation and user demand.
Brand safety	Ads often appear in brand-unsafe places, such as on infringing or fraudulent sites	Ad buys are based on audience profile for an entire site or section.	Advertisers can protect the brand by choosing sites with a high fraction of legit users, by looking for sites that aggregate known good user attributes.