MULTICHANNEL MERCHANT

MARKETING SPECIAL REPORT

Navigating the Two-Way Street of Trust in a Post-Cookie World

by **Mike O'Brien,** Multichannel Merchant

Having an accurate view of customers, their likes and dislikes, purchase behavior and history, is critical to success in retail. For customers, personalization is king, and relevance rules. For merchants, identity verification and real-time assessment of spending power helps them find and convert the right prospects and properly manage fraud and chargeback risk.

And in what will soon be a post third-party cookie world – with Google scheduled to sunset them this year, following Apple and Mozilla – and more stringent privacy regulations, the proposition is getting trickier. This means marketers need a holistic approach to identity management that is increasingly consent based in order to balance privacy restrictions with the need for personalization.

In the realm of omnichannel retail, trust is a two-way street. Retailers need verifiable information, and consumers want to know they're dealing with someone who knows who they are and what they want, respects their privacy and can deliver a consistently great experience with the least friction possible.

"Consumer identity plays a big role in enhancing the customer experience and building trust," said Brigette Korney, Director of Payments and Fraud at Groupon. "This not only streamlines account sign up, log in and checkout, but also can result in more personalized shopping experiences."

Korney added that reliably resolving consumer identities allows Groupon to distinguish between known, trustworthy customers and potentially fraudulent bad

actors. "With the right technology, this can be achieved seamlessly behind the scenes, with no added friction," she said.

With Google set to disallow 3P cookies on Chrome by 2022, the search giant has been testing a browser extension API called Federated Learning of Cohorts (FLoC), part of its TurtleDove privacy sandbox initiative. Google said in late January 2021 that tests of FLoC on audience reach demonstrated it can generate at least 95% of conversions per dollar compared to 3P cookie-based advertising.

Shannon Wu-Lebron, senior director of diversified markets for TransUnion, said until now personalization has been achieved at the segment level using anonymous behavior. But GDPR in the European Union and CCPA in California are changing how companies think about balancing personalization and privacy.

"They're definitely having a very profound impact, and companies are just starting to take it into consider-

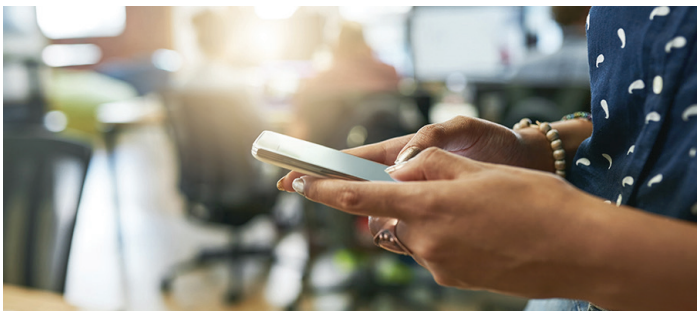
CONTINUED ON PAGE 2

FEATURED IN THIS REPORT

ation in their strategy," Wu-Lebron said. "And consumers want relevance and personalization, but also want their privacy to be protected."

She said marketers have been forced to adopt a consent-based approach, throwing up banners to first-time visitors to opt in or out of third-party cookies and building that into their business processes.

"In the new world, they're thinking of consumer identification in a much broader scope, as a digital ID that includes elements like social, email and device data," she said. "More retailers are realizing the importance of that, and are starting to think about how to manage all that information."



This new world, while challenging for marketers, presents greater opportunities to redefine how consumer identities should be managed, using a holistic, omnichannel view instead of an ad hoc one. While people naturally shop across channels, flitting from one to another, a lot of retailers still don't have the right tools or processes to help them manage all that data properly.

For instance, a shopper may have multiple profiles or versions of the same ID with a single retailer, based on factors like email and phone. And large retailers with multiple brands often maintain separate customer databases, meaning they're not doing a good job of data linking across the enterprise to ensure precise targeting and customer data management.

"At the end of the day they don't know what data is outdated, and some of them might not be real consumers," Wu-Lebron said. "So-called synthetic IDs, common in banking and financial services, involve setting up a fake ID and credit history to defraud banks and insurance companies. We're starting to see it in retail, although there's not as much money to be made on the theft of goods. But for retailers to truly understand who their real customers are, they need to find a way to link those multiple versions. There's still a lot of work to be done."

In the heyday of 3P cookies and their wealth of behavioral data, the focus has been more on the acquisition side vs. customer retention, and that's part of the problem, said Fatemeh Khatibloo, a vice president and principal analyst with Forrester Research.

"I call it lazy digital marketing," Khatibloo said. "Instead of focusing on retention, it's been so much easier for companies to buy up ad tech, using programmatic real-time buying to get all kinds of new people, vs. using your own first-party data to target properly and use digital to retain customers."

Mark Rose, senior director of strategic planning for TransUnion, agreed with Khatibloo and went a step further. While acquisition programs were important, he said, the last-click nature of attribution logic tends to overstate their relative value, as they're targeting shoppers based on previous intent.

"The pandemic accelerated ecommerce growth, and the emphasis is now shifting to its profitability," Rose said. "Smart marketers are investing in CRM capabilities and using those insights as a starting point for designing people-based marketing programs around strategic KPIs such as retention and lifetime value."

Three Primary Approaches Addressing 3P Cookie Sunset

In a post-3P cookie world, there are three primary approaches to digital marketing that are consent-based and can achieve the necessary scale in order to be effective.

Walled gardens such as Facebook and Amazon have massive audience scale based on authenticated first-party data, and advertisers benefit from significant reach and targeting opportunities. The downside: No cross-channel activation or omnichannel view of consumers.

So-called "private gardens" are the next tier down. Large retailers like Target and CVS have built their own private exchanges or networks on the foundation of their unique assets, including first-party data and successful loyalty programs.

In general, retailers and ecommerce companies that have invested in building a successful loyalty program will have a significant leg up on the competition in a post-3P cookie world, said Khatibloo.

"If their loyalty programs are robust, they have enough personal information to create a mechanism to market to those consumers, even retargeting to some extent, especially within their own sites," she said. "They're better positioned to build direct relationships with publishers and target consumers based on their loyalty data and relationships."

Data consortiums involve technology partners pooling their data to create a common ID in order to achieve the necessary scale. Consent-based consumer data becomes a shared identity resource that is interoperable and accessible to all members, with no sole beneficiary or owner in the group. Given the right data governance, a consortium can drive scale outside the walled gardens, giving consumers the appropriate consent and privacy controls.

Critically, a universal ID within a consortium environment provides a shared identity without reliance on 3P cookie syncing, as it's based on first-party and offline data. Unlike 3P cookies which use probabilistic matching based on various data sets and algorithms, universal IDs apply deterministic matching (i.e., matching the same user profiles together). Publishers and advertisers can display the right ads while consumers will not be served irrelevant ads that are instantly ignored.

Device fingerprinting is another targeting approach used by many digital marketers. This involves the use of tools that gather Javascript parameters about a device's browser, zeroing in on a unique combination of identity keys (browser name and version, screen resolution, list of fonts and plugins and IP address and location, etc.). By this method, companies can identify unique users with 99% accuracy.

Khatibloo warns marketers, however, that device fingerprinting is already running afoul of privacy regulations. For instance, she said, the open-source Brave browser blocks fingerprinting by preventing third-party sites from accessing functionality frequently used to fingerprint users. While Brave doesn't have anywhere near the market share of Chrome, Firefox or Safari, she said it is influential as other browser makers often follow its lead on privacy measures.

"Brave is already subverting device fingerprinting in the way it sends information," she said. "Certainly, in Europe, fingerprinting is already a violation of GDPR as there's no consent or notice, so it flies in the face of its requirements."

In addition to compliance issues, Rose said there's another problem with reliance on device IDs. "Marketers that focus on devices or individual identity keys, instead of actual people, risk poorly performing campaigns because they don't understand their customers' media behavior and thus lack insights from it," he said.

The Rise of People-Based Marketing

Wu-Lebron said reliance on 3P cookies and attribution, with its behavioral-based approach, moved away from the actual person. It also enabled marketers to avoid the use of personally identifiable information (PII) that violated privacy regulations.

"The industry was saying in effect, 'I'm just sending emails to people who exhibiting this particular behavior, or flashing banner ads to people that are cookied,'" she said. "But as 3P cookies go away, they're not able to do that effectively at all. They need to go back to the actual person, in a way that allows you to respect their privacy and manage consent, using the different (identity) elements responsibly."

There are three key aspects to people-based marketing:

- Multi-key identity: In the face of channel and device fragmentation, identifiers will come and go, so a multi-key approach makes the most sense. Marketers need the flexibility to ingest and match against new keys, increasing match rates and audience accuracy. Identity graphs with an accurate and comprehensive traditional PII footprint and multi-key approach will provide the strongest support in a people-based ecosystem.

- No universal ID: While companies may develop their own internal, customized identity graphs, there will be a handful of interoperable people-based identity graphs that can function as tradable ID currencies. They will be able to translate identity signals across the ecosystem and meet scale, accuracy and connectivity demands of a people-based identity marketplace.

- Consent at the core: A focus on consumer trust and consent is key to future-proofing solutions as privacy legislation and consumer demands for control increase.

At the end of the day, a people-based approach has the potential to achieve a real win-win for retail and brand marketers, building more trust and providing a better shopping experience while at the same time not dealing with 3P cookies and their anonymous data.

In terms of PII, Khatibloo noted how that concept is somewhat dated in an era when smart devices are so ubiquitous, throwing off much more data that zeroes in on users than traditional identity markers like name, address, telephone and email.

"It's a term that served us really well as a market for a long time," she said. "It's not just about the inevitability of an individual identified user but about the information that can be connected back to them, an approximation of a person connected to that device. According to CCPA, cookie history is personal information, as are biometrics. Suddenly, you have to deal with a much bigger pool of data than PII when talking about privacy regulations and data sharing for ad targeting."

Customer Data Management Is Key

Customer data management of first-party information within a CRM, already important, will become that much more critical in a post-3P cookie world. And a lot of that data is stagnant and badly in need of scrubbing: According to Forrester, 30% of 1P customer contact information becomes obsolete and fails every year.

"For instance, in 2020 a lot of retailers had to post information on new store hours, new operations and delivery or pickup options," Wu-Lebron said. "How do you get those communications out beyond traditional mass channels? So, having accurate customer contact information allows them to retain their relationships better."

Using first-party and consortia-based creation and sharing of customer data, Khatlibloo said, retailers can more easily build direct relationships with publishers as well as consumers, foregoing layers of ad tech.

"In many ways it's the future of digital advertising, because of privacy regulations and technology company restrictions," she said. "It's going to cause pain for some retailers and brands that don't have either the means to manage all that data, or don't have the scale to make it worth going out to premium publishers. The big data players are trying to create ID solutions in a privacy compliant way that brands can piggyback on to get more scale. But it remains to be seen whether privacy regulators respond to that or not."

It's All About the CX and Security

Consumers are primarily looking for convenience and relevance: A shopping process that's smooth, simple and quick regardless of channel, with product, price, availability and fulfillment options clearly indicated. On the other hand, they also demand security and peace of mind, knowing their payment and personal information is protected and secure.

According to a holiday 2020 shopping survey from TransUnion, nearly half of the respondents said they were worried about online fraud.

"That result underlines how top of mind security and fraud risk is," Wu-Lebron said. "Consumers understand that ecommerce can't be completely friction free. We like to think of it as 'friction-right.' They're willing to put up with a degree of checkout friction if it ensures their experience is a safe one. And in a post-cookie world, that means retailers relying more on first-party data, people-based marketing and a holistic approach to identity management."