2021 Privacy and Omnichannel

Marketing Handbook

What You Need to Know About the New Post-Cookie Landscape

infutor

What is omnichannel marketing?

The past few years have seen enormous growth in omnichannel marketing and consumer identity management (CIM). (To learn more about CIM, visit Infutor's Resource Center at infutor.com/resource-center) Omnichannel marketing is the coordination of ad messaging, targeting and ad campaign optimization strategies across multiple devices and content channels. Done well, it opens new marketing and campaign optimization possibilities for brands and agencies:

- **A brand's CRM data can be "onboarded" for ad targeting through multiple platforms and channels** – directing integrated ad messages to precise, pre-selected groups.
- **Campaigns can be coordinated across channels** – for instance, campaigns can be sequenced (or capped or suppressed) across web, mobile, social, connected TV, OTT and direct mail.
- **Campaigns can be measured and optimized through data-driven strategies** – for instance, by comparing campaign targeting data to in-store purchase data.

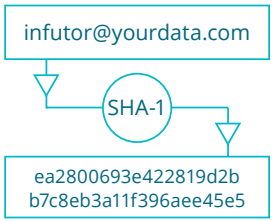
Using omnichannel marketing this way provides consumers with consistent messaging and experiences through each channel. It also creates a more engaged branding experience and shows consumers that a brand understands who they are. The consumer receives a seamless, personalized and compelling experience no matter where, when or how they interact with a brand.

How does identity data get matched across platforms to enable omnichannel marketing?

At any given hour, millions of users are logged into websites or apps through a provided email address. Many of those websites or app publishers work with online platforms to match anonymized or de-identified (usually, hashed) versions of those email addresses to cookies. They then link those cookies to other offline information about a particular user – for instance, that they use Brand X razors, drive a particular vehicle, or stay at Brand Y hotels.

What is a hash? A hash or a hash value is a string of letters and numbers of a standard length, which represents an actual word or phrase – for instance, an email address – that has run through a hashing algorithm. Common hashing algorithms are MD5, SHA-1 and SHA-2. Data run through a hash algorithm will always produce the same hash value.

For instance, when run through a SHA-hash, infutor@yourdata.com will always produce the hash value ea2800693e4228-19d2bb7c8eb3a11f396aee45e5.



Hashes are particularly useful for appending and matching data across platforms, because they serve as a reliable proxy for personally identifiable information while ensuring privacy. Hash algorithms can also be salted with added values, to make them even more proprietary and secure (such as to confine their usage).

Why have third-party cookies been so important for omnichannel marketing?

Big changes are coming to omnichannel marketing, because third party cookies are going away. We will describe that in section 4. **But first – what are third-party cookies and why are they important?**

Cookies, as you may know, are the small strings of data on your browser that, in coded form, represent certain values to a server that can read them – for instance, the web server of a website you visit. Cookies allow servers to recognize the same browser over multiple browsing sessions by, for example, storing a coded, unique identifier (not unlike a hash value) that matches a particular browser.

Third-party marketing platforms generally set "third-party" cookies through a variety of publishing partners (such as news websites, blogs, or any other web content, whom they may pay with money or in-kind services like analytics). In turn, this allows marketing platforms to create marketing profiles, target ads across websites, and measure and analyze those ads' effectiveness, i.e., "attribution."

But cookies can also be synced to other identifiers when that same consumer's browser is seen by other online platforms. With enough data points – log-ins, page views – these identifiers can all be connected across mobile, browser, social media, connected TV, email and even direct mail channels. For instance, if a browser and mobile device are nearly always seen on a common IP address, it is often (though not always) reasonably likely the browser cookie ID and the mobile ad ID belong to the same user or household.

This is sometimes called cross-device linking – and it's what enables omnichannel strategies. But it all relies on the simple browser cookie.

Different Flavors of Cookies – While third-party cookies' days are numbered, first-party cookies remain very much intact. As opposed to third party cookies, which are generally set by external marketing or analytics platforms, first-party cookies are set directly by the website you're on and work on the publisher's website only. Browsers support first-party cookies by default, although you can still choose to disable them, or delete them at any time. However, disabling them eliminates benefits such as site settings, preferences, or other functions like personalization.

Why are third-party cookies going away, and what will replace them?

Some browsers already block third-party cookies by default, unless the consumer enables them (usually through "settings" or similar option). Apple's Safari began doing this in 2017, and Mozilla's Firefox followed suit in mid-2018. But these browsers only have minority shares of the market. On the other hand, Google's Chrome accounts for some 60 to 70 percent of the browser market, and Chrome's announcement that it will phase out third-party cookies by 2022 has sounded a death knell for the third-party cookie.

Web browsers are working toward standards to allow for more limited methods of targeting and measuring advertising through a variety of methods including cohorts (i.e., groups of browsers instead of uniquely identified browsers) and on-device processing to keep data local to the browser without sharing it out to marketing platforms. These methods would still work on the open web (i.e., without email log-ins), but it's unclear whether they will be effective.

Thus, this is all causing uncertainty – and some anxiety – for marketers, as digital publishers and platforms scramble to consider what will replace the third-party cookie, and how that will alter the face of digital advertising, marketing models, and marketing spend. This anxiety is understandable: **marketers have relied on third-party cookies for nearly two decades** as the backbone of digital advertising, retargeting, campaign analytics and performance measurement, as well as a crucial identity matchpoint for cross-device linking and omnichannel marketing.

So what will happen when cookies ultimately go away?

There are several parts to this answer – though the truth is that no one really knows:

- **First-party "walled gardens," notably Google and Facebook, should benefit**, given their ability to utilize and match first-party and customer data across multiple platforms. However, as those platforms are under increasing scrutiny – on both antitrust and privacy grounds – they may find it harder to be as nimble and creative with their data and marketing strategies as they have in the past. Likewise, many advertisers have expressed dissatisfaction with the lack of transparency regarding audiences and ad performance that these players offer – which advertisers have grown accustomed to in open-web solutions.

- **Some platforms (especially multi-property publisher platforms) are building their own "walled gardens"** – and will likely offer competition to those mega-players. This will involve finding ways to collect more information – particularly emails – from their users.

- **At the same time, some platforms (LiveRamp and The Trade Desk, among others) are working on "unified" ID solutions**, which they anticipate will be based around hashed email addresses – IDs that would connect web-based, offline, mobile, and connected TV platforms.

- **And of course some marketing dollars will go towards channels other than digital** – such as connected TV and email marketing. (Yes, you will probably get a few more emails in your inbox – hopefully from brands you like and trust.)

All of these cases have one thing in common. In all of them, first-party data is crucial for marketing success. Publishers with first-party data can better enrich their ad inventory to offer advertisers more targeted advertising. Advertisers with first party data can match it to those publisher platforms – and do their own data enrichment and direct-to-consumer marketing. And data intermediaries need first-party data to place ads in the most relevant way, with the most relevant publishers.

How should your organization prepare for the "cookie-pocalypse"?

As cookies go away and first-party data becomes more important, you'll probably need to involve more players within your organization in your digital campaigns. Here are some likely key players:

A. Information Security

More first-party data means more data to protect. While CRM information such as email addresses is not as sensitive as credit card and social security numbers (and is generally not subject to data breach reporting statutes), there are still important reasons to protect it. For one, is it competitively sensitive. Additionally, CRM email databases can be (and increasingly are) misused by hackers and phishers to socially engineer consumers to give up account and other sensitive information.

This type of information is even made available for sale on "dark web" internet sites – which have led to embarrassment to and even lawsuits against some brands.

Thus, collecting and storing more first-party information comes with the responsibility of protecting that information, through careful information security protocols, audits, encryption, and employee training.

B. Data architecture

The rising importance of first-party data will in turn lead to the collection of more kinds of first-party data – online, offline, mobile, transactional, and even location data – and the combination of that data with "third-party" data (e.g., data licensed to, rather than collected by a brand). This will require brands to become more familiar with data tools and protocols for managing and linking divergent data groups.

For one thing, brands will need to become more familiar with the tools offered by consumer data platforms or CDPs – the platforms that house, link, and distribute data, to and within marketers' and their partners' databases.

Brands also may need to master data architecture strategies that honor privacy principles – which can be both complex and subtle. In particular, privacy best practices or contractual restrictions often require that certain kinds of data should not be merged with other data. For instance, sensitive information like location data or anonymized data often can't be directly merged with so-called personally identifiable information (PII) like a name or email address. But complex data architecture mechanisms – such as hashing (and "salting" hashes), encryption, use of data "safe harbors," data siloing, and data deletion and minimization protocols – can often support indirect merger strategies allowing value to be pulled from those same datasets in a more privacy-protective way.

C. Consumer Disclosures and Privacy Rights

When brands collect more first-party data, they will also need to be precise and transparent about how the information – for instance, email addresses – will be used. Key legal points will involve:

- **Privacy Disclosures.** Marketers doing omnichannel marketing are generally required by law – and often by their contracts – to disclose in an understandable way how they collect and use data. Some laws, particularly California's Consumer Privacy Act (the CCPA), require quite specific disclosures. For instance, the CCPA – and its successor legislation, the California Privacy Rights Act (effective in 2023) – require granular disclosures based on each data category – and how each particular type of data is collected, used, and (if applicable) sold. It also requires that certain consumer rights be clearly set out in privacy policies, among other disclosures.
- **Opt-Out.** It's also important to give consumers ways to opt out of omnichannel marketing. This is required by laws (e.g., the CCPA), self-regulatory codes, and in many cases agreements with partners, clients, or even vendor platforms. As new technologies replace cookies – for instance, technologies based on hashed emails – brands will need to understand and describe how these opt-out methods work, and to ensure that all relevant privacy policies and other notices are properly amended.
- **Financial Incentives.** Because consumers may be hesitant to provide their email addresses at sufficient scale to replace cookies, some companies (mainly publishers, but sometimes brands) may decide to give consumers benefits for providing more data. The CCPA potentially could require that certain analysis be done and certain disclosures be made if a consumer is offered a financial incentive in exchange for providing personal information. (The scope of this requirement is not entirely clear or universally agreed upon, so we recommend discussing any "data for benefits" strategy with privacy counsel.)
- **Honoring Consumer Rights.** The CCPA also requires companies holding personal information to honor "deletion" and "data access" requests of California residents – and many marketers have extended these rights to all US residents. (The European General Data Privacy Regulation, or GDPR, gives consumers similar rights.) As marketers collect, retain, and link together more information, they will need to devote more resources, analysis and care to honoring these rights – and to determine which consumer requests they should (and should not) respond to, and how to verify consumers' identities.

Privacy compliance teams sometimes use the terms PII and non-PII. Are those terms still relevant?

These terms are still relevant to some people, and are sometimes referred to in certain agreements, but legally speaking, they are losing relevance – as it's becoming hard to distinguish when information really is "personal" or "identifiable."

Until just a couple of years ago, marketers could rely on a clear distinction between:

- "personally identifiable information" (often called "PII")
- "non-personally identifiable information" (often called "non-PII")

This distinction has long been made, for instance, in industry self-regulatory codes (like those of the NAI and DAA) to distinguish between information that identifies people in traditional ways, like contact information (e.g., name, address, email address, phone number), and information that only refers to a device or network identifier not easily linked to an actual person. These codes in turn treat Information that can be used to identify someone by name differently from so-called "de-identified" or "anonymous" (or "pseudonymous") information.

But European privacy laws (such as the ePrivacy Directive and since 2018, the GDPR) apply to a far wider range of identifiers (cookie IDs, IP addresses, etc.), and new privacy laws have trended in that same direction. The California Consumer Privacy Act (CCPA), for instance, defines "personal information" to include any "unique" identifier, including online identifiers, as does its

successor California Privacy Rights Act (CPRA), and proposed US privacy legislation (such as the SAFEDATA Act) likewise would apply to those identifiers. Brazil has passed a new law based on the GDPR's broad definitions of "personal data," as well.

And in the US, certain sectors have their own nomenclature around personal data, with particular legal definitions. For instance, medical data (such as patient information collected by doctors, pharmacies, or acupuncturists) is usually covered by HIPAA and is referred to as "Protected Health Information" – but has very specific carve-outs regarding de-identification. Similarly, customer information held by banking information is referred to under the Gramm-Leach-Bliley Act as "Non-Public Information" or NPI, and has yet a different definition. This "sectoral" approach in the US can be confusing, and legal expertise is often needed to know what laws apply.

Remember: It's therefore important to always define terms like "personal information," "PII" or "personal data" when agreeing to a contract. Some contracts use terms like "Party X agrees not to deliver any personal information to Party Y" or "Party Y will encrypt all personal information" – but that's confusing unless the contract says what "personal information" is.

What should I ask my data provider about omnichannel marketing?

- **Ask how data is protected** – providers should be able to provide detailed security protocols, including annual audits and penetration testing.
- **Also ask about data minimization.** Data minimization means that once data is no longer useful, it should be deleted. Your service providers should delete your data once campaigns or services are concluded, or after 30 days. This mitigates potential damage and embarrassment from data breaches, leakage or misuse.
- **Providers should be able to provide standard policies** to reassure you that their platform – and your data – will be secure, such as incident response plans, disaster recovery plans, and (as noted above) data security protocols.
- **Ask how they can help you plan to transition away from third-party cookies** – for instance, by helping you activate your first-party data in a responsible way and provide alternatives to cookie-based targeting.

Why Infutor?

Infutor is the expert in Consumer Identity Management, 100% focused on enabling brands to know everything they need to about consumers, to instantly make informed marketing and risk decisions.

Our experience linking trusted data sources results in solutions that identify, verify and score inbound consumers, on demand, with as little as a single identifier; link customer data; update/add missing identifiers and enhanced attributes; and enable increased digital campaign reach through higher onboarding match rates.

Infutor gives brands a secure, privacy compliant foundation to improve inbound engagements and outbound marketing reach, and to minimize fraud and collections risk.

Infutor's own TrueSource™ Identity Graph is the most authoritative collection of consumer data, attributes and intelligence that makes cross-channel engagement personal – and measurably effective for brands. Our secure and privacy-compliant ID graph enables marketers to create relevant, real-time experiences in whichever channel people engage with a brand.

infutor.com

(312) 348-7900

infutor

The Consumer Identity Management Experts