MANAGING ANONYMOUS AND AUTHENTICATED EXPERIENCES

across the customer lifecycle.

2016

TABLE OF CONTENTS

INDIVIDUAL attention.

Identifying consumers as individuals is important because identity is the only constant carried across different interactions.

Before mobile, SEO, or Facebook ever existed, it didn't cost much to reach anonymous consumers through print, broadcast, and outdoor media. But audience segmentation was inaccurate and performance was hard to measure. On the other hand, identifying prospects through direct mail or phone was measurable, but more expensive and difficult to scale.

Digital marketing technologies have transformed both anonymous and authenticated interactions. Online ads, websites, and search reach more anonymous consumers for less, with much better segmentation and measurement. They've also added entirely new capabilities like behavioral monitoring and predictive analytics.

Today's digital campaigns build lasting relationships between brands and authenticated contacts, across channels and locations. As the customer journey becomes more complex, it's increasingly critical to identify consumers as individuals because identity is the only constant carried across every interaction.

In this paper, we'll explore five tips for managing anonymous and authenticated experiences:

- **Benefits of well-executed personalization**
- **Considering data as a continuum**
- **How to safely combine data**
- **Technology building blocks you'll need**
- **Ways to eliminate risk**

Personalization, identity, and privacy.

Personalization:

Relevance to the attributes, interests, and behaviors of the consumers of a group, such as the target group for a campaign. Individuals' interactions with a brand may be personalized even when no personally identifiable information about them is known or exchanged.

Identity:

The unique set of persistent characteristics that separate an individual from others—things that don't change as a consumer switches devices, locations, and platforms. Identity is closely associated with one piece of personally identifiable information, such as a physical or electronic address, credit card, phone number, and so on.

Privacy:

Information that may not be disclosed for legal, ethical, or cultural reasons. Information may be private (credit card number) or public (name and street address) and may also be private without identifying a person (medical conditions).

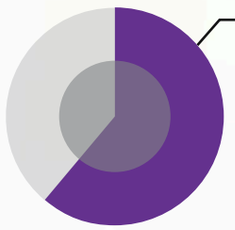
TIP #1

PERSONALIZATION works.

When marketers use the word personalization, they intend to adapt interactions based on what they know about a person, whether or not that person has shared information with them. Marketing techniques inherently create and manage interactions to personalize relationships with brands consumers can trust, delivering content that matches their preferences, attributes, and behaviors, and measuring marketing outcomes so marketers can focus and refine their efforts.

However, to realize these benefits, personalization must be done well. In fact, 63 percent of consumers are unresponsive to out-of-context messages.[1] In addition, data breaches and surveillance disclosures have raised public awareness of data privacy and resulting regulations and standards—so data used for personalization must be managed carefully.

"Customers respond to personalized, relevant experiences based on the data they feel comfortable sharing with your brand. But missteps are easy to make and could turn your customers away," says privacy expert Tim Sparapani, founder of legal strategy firm SPQR Strategies. "It's not about what we know we're sharing, it's about what we don't know is being collected and sold about us," he says.[2]



63%

of consumers are unresponsive to out-of-context messages. But with personalization, you see increases in sales, click-through rates, and conversion.

In days when marketing teams operated from separate silos, direct marketing specialists could control the use of data to comply with regulations, contracts, and industry standards. But the increasing use of cross-functional digital marketing platforms has created more complexity.

The undeniable value of personalization encourages marketers to find ways to get the most use of all their data, across the entire customer lifecycle. And the first step to using data well is understanding it thoroughly.

True Value, the world's largest retailer-owned hardware cooperative, struggled to personalize its cross-channel marketing to increase customer impressions. Although the Chicago-based company offers top-quality products and exceptional service, its marketing team knew it needed to get a more comprehensive view of its customers and tailor its messages across channels.

The marketing team overcame these challenges by first migrating data from several data sources—loyalty programs, historical responses, e-commerce system feeds, and others—to build the first email customer profile. With new technology, they were also able to manage other critical activities, such as setting up templates to reduce production time and improve targeting, establishing efficient campaign workflows, and training staff.[3]

By implementing a more advanced, multichannel campaign management solution, True Value can now execute campaigns independently, resulting in faster, more agile campaign management and increasing open rates by up to 163 percent. But Melva Godwin, manager of campaign management at True Value, says the company wants to do more than just increase sales.

"We want to be of service to our customers and communicate with them in ways that meet their specific needs. That requires relevant content across channels at just the right time."[4]

MELVA GODWIN
Manager of Campaign Management
True Value

TIP #2

DATA is a continuum.

Marketers can personalize interactions using information that spans complete anonymity to full authentication, with a middle range in which identified data may be used intermittently.

The distinction between anonymous and authenticated hinges on personally identifiable information (PII)—information that can be used alone, in combination, or in context to contact an individual. This information includes unique and partial identifiers such as name, address, phone number, and email address, as well as financial, employment, or other data associated with an individual.

Anonymous but not unknown.

Information is anonymous when it's not personally identifiable. But digital marketers can still know a lot about an anonymous consumer. Even first-time visitors to a website may reveal their IP address, browser, search history, computer configuration, and other personal information. With the right anonymous data, it's even possible to create a digital fingerprint unique to a single individual.[5]
Such information doesn't constitute personally identifiable information unless it can be used to identify, locate, or contact an identifiable consumer.

As visitors browse, they give a properly equipped website even more information—what kind of content makes them hover, click through, bounce out, abandon shopping carts, and hundreds of other behaviors, with associated and derived measures like latency and conversion.

Authenticated by permission.

At the other end of the spectrum is authenticated data—personally identifiable information that consumers allow brands to use. Authenticated data can be as simple as an email address or as comprehensive as an online loan application. The key is that the information uniquely identifies an individual and can be used only as that individual explicitly permits.

Just as marketers may know a lot about an anonymous visitor, they may know very little about authenticated users, who may use a made-up username and disposable email address. But registration or login creates a personal relationship between a brand and a consumer—one that can be very valuable if handled well.

Managing the gray area.

It may be easier to manage purely anonymous or authenticated relationships—don't use or reference personally identifiable information, and don't exceed the permissions the consumer agreed to. In all cases, follow the applicable regulations, contracts, and company policies.

But things get more complicated in the gray area, where permissions may be conditional, intermittent, or indirect. With an increased sensitivity to privacy, too much personalization can feel invasive.

In an Adobe survey on personalization, 71 percent of consumers reported that they like receiving personalized offers, but 20 percent said these offers aren't well done, and another 20 percent felt that today's personalization efforts are too intrusive.[6]

The following are some sample situations, with suggestions on how to manage them.

Managing permissions.

When customers authenticate by logging in to a site, they grant permission for the site to treat them like a known customer—"by name"—but the permissions aren't universal. Keep in mind that:

- Earlier unauthenticated sessions, even if they could be associated via IP address or browser history, aren't covered under the current permission.
- The current session prior to login can be treated as permitted. The defining case is a user who browses anonymously, then logs in to buy something, and doesn't want the shopping cart's contents to disappear.
- Email links followed to a site shouldn't be considered logins. They don't grant permissions to use personally identifiable information.
- Logins are per device—logged in on the desktop doesn't mean logged in on a mobile phone and vice versa.
- Logging out terminates permissions to link to any personally identifiable information. It's a deliberate return to anonymous status.

Using data from other providers.

Companies that deal in consumer data are typically very precise about the terms for using and sharing it.

- Second-party providers (for example, airlines partnered with credit card companies) may share data under the permissions granted by the application or other explicit consumer opt-in.
- Third-party providers "rent" consumer identities that might include data, such as investable assets, affluence, and credit worthiness. Providers who deliver anonymous data typically forbid combining it with personally identifiable information in marketing databases or using it in marketing channels that include personal information. The best way to use third-party anonymous data is to augment existing anonymous profiles with demographic or behavioral information.

Note that in late 2015, the European Court of Justice ruled that the transatlantic Safe Harbor ruling, which lets American companies use a single standard for consumer privacy and data storage in both the United States and Europe, is invalid. Since then, companies have been adjusting how they transfer personal data from Europe to non-European countries. To learn more about how the Safe Harbor ruling affects your company, read our privacy policy and responses to frequently asked questions.[7]

Combining authenticated and anonymized data.

Databases designed for different purposes make it easier to separate authenticated and anonymized first-, second-, and third-party data.

- Campaign management solutions record interactions with authenticated users and customers using first-party and personally identifiable information. The data shouldn't be enhanced with anonymous third-party cookie-based data, even when it's technically possible to link them.
- Data management platforms (DMPs) support first-, second-, and third-party data, combining anonymized data from multiple sources for segmentation, targeting, and audience management.
- Centralized marketing cloud platforms allow first-party data to be anonymized and shared across channels, including data management platforms or campaign management solutions, while managing login permissions. Anonymous first-party data can be used to enhance personally identifiable information and vice versa. Second-party data may be shared only with first-party data for targeting under express permission. Third-party data should never be combined with first-party personally identifiable information for marketing campaigns directed at identified individuals.

TIP #3

EFFECTIVE WAYS
to combine data.

Here are three of the most effective ways to combine anonymous and authenticated data without infringing regulatory rules or alienating audiences. Interactions like these provide more relevant experiences, convenience, and, in some cases, monetary value.

In each method, data originally collected under anonymous or authenticated conditions is used in the other domain, subject to aggregation, hashing, or other processes that preserve the protections and permissions under which the data was originally collected.

"By using cross-channel solutions, marketers can stitch together singular customer identities based on interactions across touchpoints to transform every customer interaction."[8]

MICHAEL KLEIN
Director of Retail Strategy
ADOBE

1 Display ad targeting (authenticated to anonymous). Display ads are most cost-effective when they're precisely targeted and when a brand's customers are among the best possible targets. Anonymizing (or "hashing") the identities of authenticated customers allows the sophisticated targeting of display ads, ensuring that the highest probability purchasers see the content most likely to lead them to purchase.

2 Remarketing (anonymous to authenticated). Customers abandon applications midway through the purchase process for a variety of reasons, including concerns about costs. Remarketing treats abandoned applications as opportunities to deliver more contextual information, more attractive terms, or other incentives to acquire the prospective customer. Behavioral data from anonymous visitors can be analyzed for patterns and sequences that predict high and low purchase likelihood.

Brands can apply rules from these anonymous visitors to predict which cash incentives, discounts, recommendations of related products, and other incentives will be most effective with high-value existing customers.

3 Look-alike audiences (authenticated to anonymous). To reach beyond a brand's customer base without sacrificing targeting precision, marketers can create look-alike audiences with hashed, or scrubbed, information from their marketing databases and then use audiences with similar characteristics from third-party vendors.

TIP #4

CONSIDER new technology.

Complex and often discontinuous customer journeys require sophisticated tools for managing anonymous and authenticated data. While the specifics of any solution should be worked out between the brand marketer and solution provider, the following table shows what fundamental elements are included.

REQUIREMENTS	TECHNOLOGY	BENEFITS
Manage the pre-purchase (anonymous) customer journey	Real-time analytics	Measure and monitor performance, and predict outcomes
	A/B testing	Optimize offers and experiences based on performance
	Data management platform	Manage data to enhance anonymous digital experiences, such as display ads
Manage the post-purchase (authenticated) customer journey	Cross-channel campaign management solutions	Deliver personalized experiences based on CRM, personally identifiable information, and first-party data
Combine insights from anonymous and authenticated sources across all marketing contacts while managing login permissions	Centralized marketing cloud technology	Use one hub to manage login permissions, contractual obligations, and consumer expectations for anonymous and authenticated data

TIP #5

ELIMINATE risks.

Discussions about rules and contracts make data-driven marketing sound risky and may tempt some marketers to avoid it entirely. But that's a mistake—one that puts brands at a competitive disadvantage and deprives consumers of personalized experiences. Of course, the details are important, but a few fundamental questions can help you put things in perspective and proceed with confidence.

1 What are you trying to accomplish? As we've seen, marketers can do a lot with a defined and segmented anonymous audience. If you need personal information, how much do you really need? A complete birth date or precise location? Does a planned cross-platform campaign justify its cost and complexity, or would more focused campaigns with built-in testing do the job?

2 What permissions are in effect for this particular interaction? Permission to use a consumer's name on a website doesn't imply consent to push location-dependent content to their mobile device, and permissions don't extend from one web session to the next if the user logs out. If permissions are ambiguous, redraft your opt-in language.

3 Do you tell consumers what you'll do with their data and then stick to your promises? Make sure you clearly communicate how you'll use the information you collect. Don't violate your customers' trust by crossing boundaries.

4 Will an interaction be intrusive, poorly timed, or out of context? This is the "creepy zone"—the gray area. Most marketers know it when they see it. By pinpointing the latency, frequency, and content that works best for a planned interaction, you'll discover what's too much, too often, and irrelevant.

As you continue to personalize data, find ways to safely combine anonymous and authenticated information, and reevaluate the technology you'll need to be successful, remember that we're here to help you along the way.

About Adobe Marketing Cloud

Adobe Marketing Cloud empowers companies to use big data to effectively reach and engage customers and prospects with highly personalized marketing content across devices and digital touchpoints. Eight tightly integrated solutions offer marketers a complete set of marketing technologies that focus on analytics, web and app experience management, testing and targeting, advertising, audience management, video, social engagement, and campaign orchestration. Learn more about creating personalized experiences with anonymous and authenticated audiences at www.adobe.com/marketing and www.adobe.com/campaign.

Adobe Privacy and Security Center

Learn more about privacy topics at the Adobe Privacy Center and how we're building continuous security into our Shared Cloud infrastructure.

[1] "Mind the Marketing Gap," The Economist Intelligence Unit, June 2013.

[2] "The Data Brokers: Selling Your Personal Information," 60 Minutes, March 9, 2014.

[3] Adobe Customer Story, True Value.

[4] Ibid.

[5] Panopticlick, Electronic Frontier Foundation.

[6] Adobe Digital Index, 2015 Online Shopping Predictions.

[7] Adobe Safe Harbor Privacy Policy.

[8] Personal interview with Michael Klein, director of retail strategy, Adobe, November 20, 2015.