AN ARTICLE FROM Marketing DIVE

The blessing and curse of proximity marketing

Editor's Note: The following is a guest post from Paavana L. Kumar, associate, at the advertising, marketing and promotions practice group at Davis & Gilbert.

Whether you are a fashion retailer or a chain drugstore, proximity marketing should be on your radar. Proximity marketing is a sophisticated way to target consumers in their daily lives: marketers can send consumers personalized messages triggered by factors such as their geolocation, their purchasing and preference history and even the weather. According to recent studies, including **a report by Retail Touchpoints**, nearly half of retailers in the U.S. launched proximity marketing programs going into 2016, and the number has only skyrocketed this year.

The surge in campaigns harnessing this technology is not surprising. Over the last few years, retailers have increasingly seen consumers migrate away from brick-and-mortar retail stores in favor of convenient digital outlets. Many consumers feel that, with the ease of smartphone and "one-click" shopping, browsing for products in a physical store is almost obsolete. However, the very same digital technology that has caused such a crisis in the retail industry may now be poised to help retailers — that is, assuming they are able to understand and properly navigate the space's unique legal and regulatory hurdles:

Catching consumers in the moment

Today's consumers engage in a shorter purchasing process, but the essential principles that underlie business-to-consumer marketing have not changed — consumers still make emotional buying decisions, they still want to comparison shop to make the best choices and they still prefer to see content that is relevant and helpful to them. Proximity marketing is a way to appeal to these fundamental consumer desires without sacrificing a focus on the in-store experience.

Proximity marketing comes most commonly in the form of beacon-based campaigns. Department stores such as Macy’s, Nordstrom and Neiman Marcus, as well as major fashion retailers such as Urban Outfitters and American Eagle, are already using beacons to target consumers based on their physical location. At a basic level, beacons emit radio signals to connect with nearby consumers’ mobile devices, working in conjunction with a retailer-specific app in order to push certain notifications to consumers when they are in proximity to the beacon — for example, a special offer for a product in the aisle in which they are browsing. By targeting the consumer in the moment, the technology can capitalize on a buyer’s immediate reaction to a product, which can be even more effective than serving ads to them before they decide to go to the store.

Yet retailers and other marketers using this technology, and harnessing consumer data to tailor their advertising, should bear in mind that they are subject to a complex legal and regulatory framework which revolves around key principles of notice, choice and consent. From marketers’ perspective, navigating these requirements poses a unique dilemma: how can they create content compelling enough to convince the consumer to stay committed through the opt-in process to share their data? And perhaps more importantly, how can the marketer stay transparent and give consumers the choice to easily opt-out of data tracking, while still maximizing the chances that they will choose to stay loyal?

Driving mobile engagement

Even while grappling with these regulatory issues, from a business perspective the biggest challenge for retailers using traditional beacon technology is the necessity of utilizing a retailer-specific app. Since the consumer needs to have downloaded the retailer’s app to enable the digital engagement, these retailers are unlikely to attract new customers beyond the dedicated consumer base that they have already convinced to do so. A possible solution is to develop integration outlets with the Physical Web.

The Physical Web is a recent Google development utilizing beacons to broadcast a URL to nearby mobile devices. In the fashion retail context, a store location or a mannequin in the window could broadcast a URL which drives a consumer to a virtual fitting room or a special discounts page. This type of technology has potentially widespread applications for retailers and marketers working in partnership with each other and sharing data — for example, in airports or shopping malls where a specific marketer may not have a relationship with a particular consumer, but can provide a platform where other retailers can integrate their apps and reach out to that consumer.

However, these newer solutions to expand consumer reach also present business, legal and regulatory challenges. From a business standpoint, marketers need to be cognizant that targeting consumers who have not specifically downloaded a retailer app may annoy them or cause them to view the marketer's messaging as "spam" — even making them resort to ad blocking if the content seems depersonalized or otherwise uninteresting. And from a legal perspective, these campaigns need to be structured to stay in line with recent regulatory and self-regulatory guidance around the collection, use and maintenance of consumer data such as purchasing history, online activity, geolocation and demographic information — which in and of itself may pose logistical challenges when trying to win and keep consumers.

At a high level, consumers need to be notified that their data will be collected by virtue of interacting with a beacon or similar device, and they must be given the choice as to whether to proceed. If data is used to track consumers across devices, retailers must be transparent about their tracking choices and give consumers an easy way to opt-out of such tracking. Consider that for beacon marketing generally, consumers must not only download the retailer's app, but then must also separately opt-in to any location or other forms of tracking — and as such, it's especially important to develop compelling creative to sustain interest through that multi-step process.

Different codes of conduct, different strategies

The Federal Trade Commission (FTC) has brought several enforcement actions against both online and offline companies for failing to comply with their posted privacy policies, failing to adequately safeguard data, failing to honor consumer opt-out promises and for a general lack of transparency. Self-regulatory groups such as the Digital Advertising Alliance (the DAA) and the National Advertising Initiative (the NAI) have developed their own set of standards to promote transparency, consumer control, data security and accountability when tracking consumers and engaging in cross-app advertising.

For example, the Mobile Location Analytics Code of Conduct provides that retailers using in-store tracking technology must display conspicuous signage disclosing the presence of location-based data collection, which is connected to an opt-out mechanism alerting consumers of their right to opt-out and to decline participation in the retail analytics program. There has been an ensuing spate of enforcement actions in the mobile space which highlight these requirements and the importance of consumer choice.

So for the cutting-edge marketer engaging in proximity advertising, there are a host of issues to consider from both a creative and a compliance perspective, but there is also more to the story: proximity marketing is most effective when integrated into a broader campaign which uses big data across multiple devices and media to further succeed at personalizing advertising to the individual consumer (e.g. by tracking purchase preferences to variable factors such as the time of day) while also gathering data at the same time to improve future campaigns.

For example, this broader tracking may enable retailers to know which consumers are the most receptive and to amp up their targeting efforts with respect to those consumers and demographics to minimize the amount of “opt-outs” across the campaign overall. But these cross-device practices may also be caught in the cross-hairs of FTC regulations. In recent years, the FTC, in particular, has issued reports on the Internet of Things and a 2017 report on Cross-Device Tracking.

Keeping consumers informed and secure

These reports and guidelines highlight the need for consumers to be informed of any data or tracking that they may not expect — for example, interaction with a broad-spectrum beacon that reaches beyond the confines of an affirmatively-downloaded retailer app. Per such FTC recommendations, retailers should also build data security features into any of these tracking services, collect the minimum amount of consumer data necessary to serve the marketing purpose and be aware that if collecting sensitive information (such as health, financial, and children’s information), specific additional laws will likely apply.

Ultimately, while connected benefits may pique consumer interest, using connected technologies does not obviate the need for clearly communicated data practices, opt-out mechanisms and other elements that incorporate regulatory consumer protection requirements. While building in these notice and consent mechanisms may cause retailers to balk in the fear that consumers will not complete the opt-in process (or opt-out too quickly), there is a real potential for brand payoff: brands that are transparent with their consumers and let their consumers know that they are in control of their private information may win consumer loyalty while also mirroring key regulations on point. When developing these mechanisms, work closely with technology teams to enable a streamlined, creatively preferred process that won’t lose consumers, but that will still comply with regulatory guidance.

Remember that consumers will be most loyal to a brand that they trust, and that trust stems not from the individual messages they receive, but from the overall concept, messaging and authenticity of a brand.