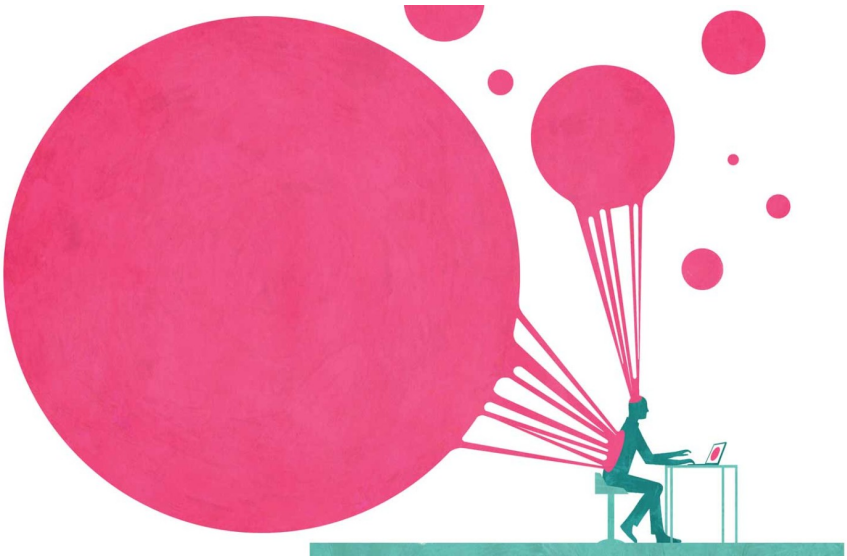
Harvard
Business
Review



MARKETING

Ads That Don’t Overstep

by Leslie K. John, Tami Kim, and Kate Barasz

FROM THE JANUARY–FEBRUARY 2018 ISSUE

The internet has dramatically expanded the modern marketer’s tool kit, in large part because of one simple but transformative development: digital data. With users regularly sharing personal data online and web cookies tracking every click, marketers have been able to gain unprecedented insight into consumers and serve up solutions tailored to their individual needs. The results have been impressive. Research has shown that digital targeting meaningfully improves the response to advertisements and that ad performance declines when marketers’ access to consumer data is reduced. But there is also evidence that using online “surveillance” to sell products can lead to a consumer backlash. The research supporting ad personalization has tended to study consumers who were largely unaware that their data dictated which ads they saw. Today such naïveté is increasingly rare. Public outcry over company data breaches and the use of targeting to spread fake news and inflame political partisanship have, understandably, put consumers on alert. And personal experiences with highly specific ads (such as one for pet food that begins, “As a dog owner, you

might like…") or ads that follow users across websites have made it clear that marketers often know exactly who is on the receiving end of their digital messages. Now regulators in some countries are starting to mandate that firms disclose how they gather and use consumers' personal information.

This throws a whole new dynamic into the mix: How will targeted ads fare in the face of increased consumer awareness? On one hand, awareness could increase ad performance if it makes customers feel that the products they see are personally relevant. Supporters of cookies and other surveillance tools say that more-relevant advertising leads to a more valuable, enjoyable internet experience. On the other hand, awareness could decrease ad performance if it activates concerns about privacy and provokes consumer opposition.

The latter outcome seems more likely if marketers continue with a business-as-usual approach. One study revealed that when a law that required websites to inform visitors of covert tracking started to be enforced in the Netherlands, in 2013, advertisement click-through rates dropped. Controlled experiments have found similar results.

Some firms have done better than others in anticipating how customers will react to personalization. Amazon features shopping ads throughout its site, making product recommendations based explicitly—and often conspicuously—on individual users' search data, without seeming to draw any consumer ire whatsoever. However, in a now-infamous example, when Target followed a similar practice by creating promotions that were based on individual shoppers' consumption data, the response was not so benign. The retailer sent coupons for maternity-related products to women it inferred were pregnant. They included a teenager whose father was incensed—and then abashed to discover that his daughter was, in fact, expecting. When the *New York Times* reported the incident, many consumers were outraged, and the chain had a PR problem on its hands. Similarly, Urban Outfitters walked back the gender-based personalization of its home page after customers complained. "We saw customer frustration at being targeted outweigh any benefit," Dmitri Siegel, the marketing executive in charge of the initiative, concluded in an interview with the *Times*.

For the consumer who prefers relevant ads over irrelevant ones (an ad-free experience is not realistic in today's ad-supported web landscape), it's important that marketers get the balance right. Digital marketers need to understand when the use of consumer data to personalize ads will be met with acceptance or annoyance so that they can honor consumers' expectations about how their

information should be used. The good news is that social scientists already know a lot about what triggers privacy concerns off-line, and new research that we and others have performed demonstrates that these norms can inform marketers' actions in the digital sphere. Through a series of experiments, we have begun to understand what causes consumers to object to targeting and how marketers can use personalization while respecting people's privacy.

The Privacy Paradox

People don't always behave logically when it comes to privacy. For example, we often share intimate details with total strangers while we keep secrets from loved ones. Nevertheless, social scientists have identified several factors that predict whether people will be comfortable with the use of their personal information. One of these factors is fairly straightforward—the nature of the information. Common sense holds that the more intimate it is (data on sex, health, and finances is especially sensitive), the less comfortable people are with others knowing it.

A second, more nuanced factor involves the manner in which consumers' personal information changes hands—what social scientists call "information flows." One such norm is, to put it colloquially, "Don't talk about people behind their backs." While people may be comfortable disclosing personal information directly (what scientists call "first-person sharing"), they may become uneasy when that information is passed along without their knowledge (what we term "third-party sharing"). If you learned that a friend had revealed something personal about you to another, mutual friend, you'd probably be upset—even though you might have no problem with both parties knowing the information. It can also be taboo to openly infer information about someone, even if those inferences are accurate. For example, a woman may inform a close colleague of her early-term pregnancy, but she'd likely find it unacceptable if that coworker told her he thought she was pregnant before she'd disclosed anything.

In our recent studies we learned that those norms about information also apply in the digital space. In our first study, we collected a list of common ways in which Google and Facebook use consumers' personal data to generate ads. We then asked consumers to rate how acceptable they found each method to be, and—employing a statistical technique called factor analysis—identified clusters of practices that consumers tended to dislike, which mirrored practices that made people uncomfortable off-line:

- obtaining information outside the website on which an ad appears, which is akin to talking behind someone's back
- deducing information about someone from analytics, which is akin to inferring information.

Next, we wanted to see what effect adherence to—or violation of—privacy norms would have on ad performance. So we divided participants in our study into three groups. In a simulation of acceptable, first-person sharing, one group first browsed a website; on that same site we later displayed an ad accompanied by the disclosure "You are seeing this ad based on the products you clicked on while browsing our website." In a simulation of unacceptable, third-party sharing, another group browsed a website and then visited a second site, where we displayed an ad accompanied by the disclosure "You are seeing this ad based on the products you clicked on while browsing a third-party website." The final group served as a control; like the other groups, these participants engaged in a browsing task and were then shown a targeted ad, but without a message. In all groups, we measured interest in purchasing the advertised product as well as the likelihood that participants would visit the advertiser's website. Additionally, to understand how these three ad scenarios affected consumers' attitudes, we asked all participants which they valued more: the personalization of ads or the privacy of their data.

> If people dislike the way their information is shared, purchase interest drops.

We found that when unacceptable, third-party sharing had occurred, concerns about privacy outweighed people's appreciation for ad personalization. Those attitudes in turn predicted interest in purchasing, which was approximately 24% lower in the group exposed to unacceptable sharing than in both the first-party sharing and the control groups—a clear indication of backlash.

We then conducted a similar test using declared (acceptable) versus inferred (unacceptable) information. After completing an online shopper profile, one group saw an ad that was accompanied by the disclosure "You are seeing this ad based on information that you provided about yourself." After filling out the same form, a second group of subjects saw an ad but were told, "You are seeing this ad based on information that we inferred about you." A final control group saw the ad without any disclosure. The group that viewed the ad generated through inferences showed 17% less

interest in purchasing than the other groups did—even though the ads were exactly the same across groups. In sum, these experiments offer evidence that when consumers realize that their personal information is flowing in ways they dislike, purchase interest declines.

Mitigating Backlash

But it's not all bad news. Three factors can increase the upside of targeted ads for both marketers and consumers. Taking them into account will help marketers provide personalized ads that inform consumers of products they want and need but in a way that feels acceptable.

Trust.

A common practice that advertisers currently use to preempt targeting backlash is to offer voluntary ad transparency. Many now display an AdChoices icon, a blue symbol indicating that the accompanying ad has been tailored to the individual recipient's characteristics. In some cases, consumers can click on the icon to find out why the ad has been displayed to them. In 2014, Facebook introduced a similar "Why am I seeing this ad?" feature on its site.

Such disclosure can be beneficial when targeting is performed in an acceptable manner—especially if the platform delivering the ad is otherwise trusted by its customers. In one experiment conducted with Facebook users, we first asked participants how much they trusted the social media company. Next, we directed them to find the first advertisement in their Facebook news feed and read its accompanying transparency message. We asked them to indicate whether the message conveyed that the ad had been generated using first- or third-party information and using declared or inferred information. Then we inquired about how interested they were in purchasing the advertised product and engaging with the advertiser in general (by, say, visiting its website or liking its Facebook page). Overall, ads from unacceptable flows performed worse than those from acceptable flows. However, trust enhanced consumers' receptiveness: People who trusted Facebook and saw ads based on acceptable flows expressed the highest interest in purchasing the product and engaging with the advertiser.

We also found that when trust was high, disclosing acceptable flows actually boosted click-through rates. In a set of field experiments, we partnered with Maritz Motivation Solutions, which runs redemption websites for loyalty programs such as airline frequent-flier programs, a context in which consumer trust tends to be high. These sites use the same technology as the large e-commerce sites,

except that the currency is points instead of money. In one experiment, when we revealed first-party sharing by telling shoppers that an advertisement was based on their activity on the site, click-through rates increased by 11%, the time spent viewing the advertised product rose by 34%, and revenue from the product grew by 38%.

Control.

Central to many privacy concerns is the loss of control. Consumers may not object to information being used in a particular context, but they worry about their inability to dictate who else might get access to it and how it will be used down the line.

In a novel experiment, MIT's Catherine Tucker partnered with a nonprofit that advertised on Facebook. The nonprofit targeted 1.2 million Facebook users with calls to action such as "Help girls in East Africa change their lives through education." For half those users, the ad was also personalized, openly invoking an attribute that a user had revealed on Facebook. For example, an ad might read, "As a fan of Beyoncé, you know that strong women matter," if a user had liked the popular singer on Facebook. Midway through this experiment, Facebook instated new privacy features that gave users more control over their personal information (without changing the attributes that advertisers could use to target people). The social media platform allowed people to keep their connections private and to manage their privacy settings more easily. Before this policy change, the personalized ads did not perform particularly well; if anything, users were slightly less likely to click on them than on generic ads. After the change, however, the personalized ads were almost twice as effective as the generic ones. In other words, when consumers are given greater say over what happens with the information they've consciously shared, transparently incorporating it can actually increase ad performance.

> With personalized ads, there's a fine line between creepy and delightful.

In another experiment we showed participants a targeted advertisement, systematically varying the disclosures appearing alongside it. With one group of participants, the ad was accompanied by a message saying that (unacceptable) third-party information had been used to generate it. A second group of participants saw the same transparency message—plus a prompt reminding them that they could set their ad preferences. A third group simply saw the ad. Purchase interest was lower in the

first group than in the last group. However, in the second group—consumers who were reminded that they could dictate their ad preferences—purchase interest was just as high as in the group that had seen no message. In other words, reminding consumers that they can meaningfully control their privacy settings buffered any backlash to unacceptable data collection. However, there was also a fourth group in this experiment—whose reactions unfortunately highlight the potential for consumers to be misled. This group's members also received the ad transparency message and a prompt about managing their information. This time, however, participants were merely reminded that they could choose their profile picture. Purchase interest in this group, too, was just as high as in the group that had seen no message.

Control over personal data is becoming increasingly important in today's online world, where protracted, multilayered data collection is now common. For instance, data brokers aggregate all kinds of personal information—from platforms like Facebook as well as internet shopping sites, store loyalty programs, and even credit card companies. Therefore, as targeted advertising becomes more sophisticated and specific—and consumers' awareness of the ways in which their privacy may be compromised grows—offering people meaningful control over their information will likely improve ad performance.

Justification.

Revealing why personal data has been used to generate ads can help consumers realize the upside of targeted ads. In one experiment by Tiffany Barnett White of the University of Illinois and her colleagues, a personalized ad by a movie rental company that invoked users' physical locations backfired, but its performance improved when the copy explained why the physical location was important: The consumer was eligible for a service not available in all places. A commitment to provide justification can also foster appropriate use of data. If you have difficulty coming up with a good reason for the way you use consumers' data, it should give you pause.

Guidelines for Digital Marketers

When it comes to ad personalization, there's a fine line between creepy and delightful, so it could be tempting to conclude that the safest approach is to keep people in the dark—to obscure the fact that personal information is being used to target consumers, especially when advertising products of a more sensitive nature. Indeed, that's what Target reportedly tried after its pregnancy promotion scandal: It started arbitrarily inserting coupons for random items in its mailings to expecting

mothers, so the baby-products ads would look incidental and less conspicuous. It might also be tempting to manipulate consumers by giving them meaningless opportunities to feel in control that create a false sense of empowerment.

While such tactics may work in the short term, we believe they are ultimately misguided. Even setting aside the potential ethical issues, deceit erodes trust if it is discovered. And as our experiments show, trust enhances the positive effects of using personal information in ways consumers deem acceptable. Research into other areas also suggests that trust has spillover benefits. For example, with Bhavya Mohan and Ryan Buell, one of us (Leslie) has done research on pricing—another area where concealment and manipulation can boost profits in the short term—showing that when firms are transparent about the variable costs involved in producing a good, their consumers' trust grows and sales rise. Finally, it's doubtful that concealment will remain a viable tactic; consumers are becoming savvier, and regulators are pressuring companies to reveal their data-collection practices. An off-line analogue may be useful here as a guide: You might gain temporary advantage by deceiving a friend, but the damage if the deception is discovered is deep and lasting. Relationships are stronger if they are honest.

So what suggestions would we make to digital marketers looking to maximize the potential of ad targeting? We offer five:

1. Stay away from sensitive information.

In particular, try to avoid using anything about health conditions, sexual orientation, and so on. Google, for example, doesn't allow advertisers to target on the basis of sexual interests or "personal hardships." Similarly, Facebook recently updated its policies, preventing advertisers from basing their targeting on personal attributes such as race, sexual orientation, and medical conditions. This move presents challenges to companies that sell sensitive goods—which may want to avoid targeting altogether. Rather, such firms should consider finding their customers in ways that don't involve using personal data—by advertising on websites those customers are likely to visit, for example.

2. Commit to at least a minimum amount of transparency.

There is a wide spectrum between concealment and full disclosure, with many acceptable points between the two. As a general rule of thumb, we suggest that marketers at least be willing to provide information about data-use practices upon request. Such disclosures should be clear and

easily accessible. This is one of the purposes of the AdChoices icon; interested consumers can click on it to learn why they are seeing an ad (or to opt out of targeted advertising), but the icon isn't disruptive to consumers who are less privacy-sensitive. Simply having it on a website can be beneficial and in and of itself can foster trust. However, if a transparency initiative fails to deliver on its promise—by, for example, offering confusing or opaque explanations for why an ad is being shown—its value to the consumer will erode. A genuine commitment to disclosure may also serve as a kind of organizational prophylactic against abuse, by ensuring that employees understand that data practices must always be customer-centric and ethical. As the saying goes, sunlight is the best disinfectant.

3. Use data judiciously.

Data collection opens up all sorts of innovative and clever insights into customers, but again we counsel restraint. Consumers react poorly when personal information is used to generate a recommendation or an advertisement that feels intrusive or inappropriate. Conversely, they will give advertisers more leeway if they are delighted by recommendations. For example, Stitch Fix, the subscription-service clothing retailer, knows a lot about its customers, including information people typically prefer to keep private, such as their weight and bra size. But this information is extremely useful to the site's service of curating a package of clothing pieces that suit the customer, delivered to her doorstep. Because Stitch Fix's use of personal information is appropriate and helpful, it doesn't feel invasive.

Consumers may even be willing to forgive unacceptable data collection if they benefit from it in a compelling way. For example, the dating app Tinder tells a user how many Facebook friends he has in common with a given prospect, making it clear that third-party sharing is occurring, which would usually result in a backlash. However, in this case the sharing is clearly valued by users, so they seem to accept the practice.

4. Justify your data collection.

We also suggest that marketers explain why they are collecting personal information—and how it will generate more appropriate and useful ads. This is especially true when it might not be obvious to consumers why a given piece of information is necessary. LinkedIn justifies its data usage policy as follows: "We use the data that we have about you to provide, support, personalize and make our services (including ads) more relevant and useful to you and others." Such disclosures can also act as a mission statement of sorts for employees—again helping to prevent abuse.

5. Try traditional data collection first.

Marketers should not forget that they can (and should) still gather information from customers the old-fashioned way—without digital surveillance. While Stitch Fix draws a great deal of inferences about consumers' preferences from their online behavior, it also makes extensive use of surveys in which consumers can reveal at will their tastes and physical attributes. Other firms that rely heavily on making accurate recommendations to customers—such as Amazon and Netflix—also give consumers an opportunity to directly state their preferences. Supplementing less-transparent ways of using consumers' information with more-open ones can decrease feelings of invasiveness. More important, it can also provide a richer picture of the customer, facilitating even better recommendations. Of course, gathering data directly from consumers is costly and may sometimes be impractical (for one, response rates to consumer surveys are notoriously low). But if they have to resort to third-party information, marketers can give consumers meaningful control over how it will be used. For example, both Google and Facebook let users have considerable say about the ways they can be targeted.

CONCLUSION

There's still a lot we don't know about how people respond to online data collection and ad targeting, and norms around privacy may change over time as young digital natives become consumers and technology further penetrates our lives. For the time being, applying norms from the off-line world can help companies predict what practices consumers will accept. In the end, all ad targeting should be customer-centric—in the service of creating value for consumers.

A version of this article appeared in the January–February 2018 issue (pp.62–69) of *Harvard Business Review*.

Leslie K. John is an associate professor of business administration at Harvard Business School. Twitter: @lesliekjohn.

Tami Kim is an assistant professor of marketing at Darden School of Business, University of Virginia. Her research focuses on implicit social contracts in the digital age.

Kate Barasz is an assistant professor of marketing at IESE Business School in Barcelona.

This article is about MARKETING

⊕ **FOLLOW** THIS TOPIC

Related Topics: DATA | SECURITY & PRIVACY

Comments

Leave a Comment

POST

3 COMMENTS

pablo samano 5 months ago

Very clear article, the good sequence of messages as factor to motive the positive response of customer, as the activity perssuasion dictates: the information what we used how marketer tell us the step with the customer roll in the sales funnel, y think what we aproach this thinks for display best ads at the right time. I do not think it´s a matter of quantity of information only, rather of relevancy of the message

REPLY 0 0

JOIN THE CONVERSATION