

AdvertisingAge[®]

Want to Target Online? You Better Build Trust

Behavioral Information Makes for More Effective Ads, but Amid Facebook Glitches and FTC Guidelines, Even Google Is Calling for Privacy Legislation

By [Erik Sherman](#)

Published: April 14, 2008

Facebook user Sean Lane last fall bought a diamond ring from Overstock.com as a Christmas present for his wife, and Beacon, the site's automated word-of-mouth system, told everyone in his online network -- including his wife.

Goodbye, surprise. Hello, mass protest! More than 50,000 users signed a MoveOn petition to make the feature opt-in only, and Facebook had a new screen name: Mud.

In December, the Federal Trade Commission issued a set of proposed guidelines for online-advertising self-regulation, something the agency had previously left to the sensibilities of website owners, ad networks and advertisers.

Then Facebook had a high-profile photo-privacy glitch in March. Now even Google is lobbying for national privacy legislation, though critics say it's not going far enough.

Prepare for backlash

Privacy issues aren't new. Marketers, retailers and agencies have encountered privacy concerns for decades by analyzing oceans of consumer data. But moment-by-moment tracking of web surfers garners attention and opposition no ordinary database ever did. As behavioral targeting touches more and more online marketing campaigns, marketers had best find ways to secure consumer privacy or face the

possibilities of irate shoppers, adverse press and government regulation.

The online-privacy issue has grown slowly, from pop-up ads to banner ads to cookie tracking, web beacons and tracking across broad ad networks. Consumers have put their trust in a nonexistent level of control.

"Individuals see the term 'privacy policy,' and they then assume that the website cannot sell their information," said Chris Hoofnagle, a senior staff attorney of the Samuelson Law, Technology & Public Policy Clinic at the University of California-Berkeley Law School. When asked whether a privacy policy meant a website couldn't sell information to other companies, 55.4% of California adults polled by the group said it was true and 9% said they didn't know.

If consumers ever thought otherwise, that would be a marketing nightmare.

Consumers "are afraid fundamentally of a giant database in the sky that is collecting information from different sources and has an aggregated file ... that can be linked back to you, and the information in that file could be used to discriminate against you or harass you with unwanted solicitation in the future," said Sarah Welch, chief operating officer of ad network Mindset Media.

'For the benefit of consumer'

Many ad networks using behavioral targeting say the concern is unrealistic and unreasonable. "We would never combine it with [personally identifiable information]," said Roy Shkedi, CEO of AlmondNet. "If the data does have commercial value, we do not store it. We don't take any personally identifying information. The companies that will win are the companies that recognize that everything we're doing should be for the benefit of the consumer. If you combine PII with web-based activities, then you need to ask the consumers to opt in."

But what is personally identifiable? Latanya Sweeney, an associate professor of computer science and public policy at Carnegie Mellon University, has shown a combination of gender, birth date and ZIP code is enough, when combined with readily available data, to uniquely identify 80% of people in the U.S.

Mr. Shkedi said his company hasn't tested to see whether the data it collects could

identify specific people.

Alan Chapell, president of consultancy Chapell & Associates, said the worry is overblown. "The big dirty secret is that most big companies that get this information can't get out of their own way to find somebody," he said.

Unfortunately, consumer problems can come from perception of a small sample of businesses. "We're at a turning point where the advertising that folks can see is all of a sudden going to escalate in terms of spook factor," said Colin O'Malley, VP-strategic partnerships and programs of TRUSTe, which certifies websites' privacy standards. "If the market as a whole doesn't take steps to get proactive with their notices to consumers and to minimize the invasiveness, then the market will be stuck before it gets out of the gate."

Last fall, AOL introduced a program to let consumers opt out of cookie collection, but most privacy experts seemed to think opt-in was a better option. Privacy advocates also introduced the concept of a do-not-track list, which would work similarly to the telemarketing industry's do-not-call list.

"I know AOL had a recent campaign to educate consumers on cookies," Mr. Chapell said. "It's tough, because most consumers don't care. It's about sending out several messages of education."

Problem brands

The problem isn't major brands, said Douglas Wood, partner at Reed Smith and an expert in advertising and media law. Instead, "edgier" brands in areas such as nonprescription medicine, credit and weight loss will sometimes push too far.

"There's clearly the risk of class actions there, of litigation," Mr. Wood said. "With the typical cavalier of marketers, they keep increasing their risks when there's no resistance until there's an explosion and someone gets burned." Add the concern of the European Union over data privacy, and the possibility of regulation having an impact on a global consumer company increases.

Targeting won't leave. Consumers generally aren't willing to pay for content, so websites need ad revenue and behavioral targeting.

"Marketers have really limited interest in buying undistinguished mass audiences," said Jim Meyer, CEO of Mindset Media.

Because the marketing dynamic has changed, companies will need to build and keep trust to avoid consumer backlash. "Your average user [has] control over media that they didn't have formerly," said Tim Davis, a principal with Deloitte. "The one thing they don't control is their private information and what is done with that."

Only trust makes opt-in possible

If targeting technology is to improve, and companies get sufficient return on their online investments, users must willingly give up private information. Only trust will make that possible, and marketing departments need to consider privacy.

To start, companies should decide whether they really need behavioral marketing.

"I think from an effectiveness standpoint, from what I've seen, [behaviorally targeted advertising is] up to three to four times more effective in terms of getting a click-through rate or other response vs. regular display advertising," said Christopher Vollmer, a Booz Allen Hamilton VP and author of "Always On: Advertising, Marketing and Media in an Era of Consumer Control."

That's a number that can vary: AlmondNet's Mr. Shkedi said behaviorally targeted ads can convert prospects to customers five to 10 times better than nontargeted ads. Tracy Ryan, associate professor of advertising research at Virginia Commonwealth University and author of "Advertising 2.0: Social Media Marketing in a Web 2.0 World," quoted a rough rule of thumb of doubled effectiveness.

Behaviorally targeted ads can cost far more than untargeted ads. "You might pay \$120 cost per thousand for a behaviorally targeted ad, but \$10 a thousand for nonbehaviorally targeted ad," Ms. Ryan said. Only careful analysis shows if behaviorally targeted ads get the return on investment they need to more than make up for potential privacy concerns.

Some ad networks don't require targeting. Search-based ads, for example, work with the context of information. "We don't do behavioral targeting within our network,"

said Adam Wicks Walker, chief strategy officer of Hydra Network. "We're really only interested in two data points: Did the user click on the ad and did the user subsequently land on the company's website?"

If behavioral targeting is a must, then a company needs an expansive view of privacy, starting with clear explanations of policies, not complex documents needing the training and patience of a lawyer on the clock.

Next, policies must be carried out. "Oftentimes the corporate intent reflected in the privacy policy is not what is being done in the organization," Mr. Davis said. Even a company with proper procedures loses control when passing information to a business partner. The more widely that information gets spread about, the more likely it is that one link in the marketing chain will fail.

Companies have their online marketing -- and protection of privacy -- work cut out for them. Do it right, and they get a business edge. Do it wrong, and the edge goes to their competitors.