



## Who Owns You? Finding a Balance between Online Privacy and Targeted Advertising

Published : December 12, 2007 in [Knowledge@Wharton](#)

On November 6, Facebook outlined a strategy to integrate more targeted advertising into its popular social networking website. Facebook CEO Mark Zuckerberg saw the new initiative as an opportunity for users to refer products to each other and allow friends to share information as they shopped online and visited other websites. The system, called Beacon, was also intended to lead to more relevant -- and profitable -- advertising through precise targeting based on a user's buying habits, social circle and geography.



This is a single/personal use copy of Knowledge@Wharton. For multiple copies, custom reprints, e-prints, posters or plaques, please contact PARS International: [reprints@parsintl.com](mailto:reprints@parsintl.com) P. (212) 221-9595 x407.

But on December 5, after receiving numerous complaints from the high school kids, college students and young professionals who populate Facebook, Zuckerberg issued an apology for a program that, among other things, could track a user's web behavior and report it on a Facebook user's profile page. The problem: Facebook didn't initially ask its customers to opt in to the targeting program. As a result, some customers were caught off guard by Facebook's sudden use of detailed user tracking. In conjunction with the apology, Facebook introduced new privacy options to give users more control over how Beacon operates.

The incident raises many questions, according to experts at Wharton. For example, what is the balance between privacy and online ad targeting? Will marketers continue to experiment? Are these early efforts just a precursor of what's to come? Will consumers become more wary of sharing information? Does privacy really exist online?

Those questions don't have quick answers given that online advertising is entering an experimental age where marketers, Internet giants and consumers are fumbling to find the proper balance between more advanced ad targeting and privacy. Indeed, experts at Wharton say that companies aren't quite sure where the line between the two is until they trip over it.

"We are in a situation with the Internet where we are having an escalation of marketing activity to hyper-target consumers," says Joseph Turow, director of the Information and Society Program at the Annenberg Public Policy Center (APPC) at the University of Pennsylvania. "The Facebook incident is symptomatic of the direction we are headed. We will see more attempts to mine people's habits and relationships. We are in the post privacy era. It's not just that companies are using data: They are using statistics to figure out the probability of a person" making a purchase, for example, or visiting another site.

Facebook's broad ad strategy, which also lets partners such as Coca-Cola, Fandango and Overstock.com create pages and befriend users, is designed to allow marketers to target groups based on location, college and peer group. That strategy, however, was largely overshadowed by Beacon's tracking technology, which includes the ability to report back to Facebook when a user makes a purchase or similar transaction on a Facebook partner website. For example, if a person buys movie tickets, jewelry or a DVD on a partner site, Beacon can broadcast that fact to anyone who has access to the user's Facebook profile. As originally configured, Beacon was enabled by default, unless the user declined the action on each transaction or went through a series of steps to opt out of participation for each vendor.

Privacy worries arose almost immediately, and partners like Overstock.com stopped using Beacon after complaints started pouring in. One Overstock.com customer wrote on a blog post that he bought an engagement ring to surprise his girlfriend on New Year's Day, only to have the secret broadcast on

Facebook. Forrester Research analyst Charlene Li said in her blog that she was "blindsided" when she bought a coffee table from Overstock.com and saw it on her Facebook profile page. Her biggest complaint was that she didn't know Facebook was tracking her. Like every other Facebook user, Li was included in the Beacon program when it initially launched. Only after numerous complaints -- and advertiser angst -- did Facebook create a blanket opt-in policy for Beacon that requires the customer to give prior permission before being included in the program.

"We released a new feature, called Beacon, to try to help people share information with their friends about things they do on the web. We have made a lot of mistakes building this feature, but we have made even more with how we have handled them. We simply did a bad job with this release, and I apologize for it," wrote Zuckerberg in a blog post on December 5. "The problem with our initial approach of making it an opt-out system instead of opt-in was that if someone forgot to decline to share something, Beacon still went ahead and shared it with their friends."

At issue is the evolution of online advertising. Companies ranging from Coca-Cola and Land's End to Internet giants like Google and Amazon.com track customer behavior in an effort to better tailor products, advertising and services. For the customer, the payoff is more relevant advertising. For the web publisher, the return is better advertising revenue, given that a few extra pennies from advertisers spread over billions of page views can add up to a large payment. "Certainly, targeted marketing helps firms," says [Shawndra Hill](#), a professor of operations and information management at Wharton. "The more information you have on your consumers, the better. When marketing to millions, if not hundreds of millions, of customers, just a slight improvement in targeting translates into a lot of money."

[In her research](#), Hill has found that network-based marketing -- the type that Facebook is pursuing -- can be more effective because it finds customers who would otherwise be overlooked. The message: Social networks can be lucrative to advertisers. However, Hill suggests there is "a balance between targeted marketing and invading consumer privacy."

The big issue is finding that balance, preferably at a point that satisfies both consumers and marketers, says [Andrea Matwyshyn](#), professor of legal studies and business ethics. "There is a contradiction here. Users on one hand are willing to experiment with privacy-invasive technologies at websites like Facebook, but there's a tipping point in data sharing when users say 'this is enough.'" From an advertiser standpoint, "it becomes a delicate balance between targeting and providing services, and crossing a thin line in the sand" over privacy, says Matwyshyn, who adds that online advertising could be derailed if it is viewed as an intrusion.

One thing is certain: Internet giants and their advertising partners are working diligently to better target users even if this occasionally raises hackles. Google hopes to acquire DoubleClick, an Internet advertising firm, to offer more targeted keyword and display advertising. In September, Yahoo bought BlueLithium, a firm that specializes in behavioral ad targeting. Google scans email in its Gmail service to serve up targeted ads. [Microsoft's HealthVault service](#) will also rely on advertising tailored to customers who store medical records on its portal. Companies such as these are targeting users anonymously, but Turow notes that these efforts need more examination as well. "Anonymity is a red herring," says Turow. "Even if you are anonymous, you can be targeted. And that information can be combined with other data."

Meanwhile the companies that control big advertising budgets are willing to experiment. Coca-Cola North America spokeswoman Susan Stribling says that targeted advertising and privacy are an ongoing balancing act as marketing evolves. "It's not an 'either or' proposition," says Stribling. "In some cases, targeting leads to a better relationship and in other cases it may be viewed as an intrusion." For instance, Stribling says Coca-Cola's My Coke Rewards website absorbs customer information in exchange for points that can be cashed in for products. Users answer surveys and provide information to Coca-Cola, which uses the data to tailor content and prizes. "It's useful for us and a better experience for the customer."

Coca-Cola, a Facebook advertiser, is going to continue to experiment with social networks. The company was never a part of Facebook's Beacon program, Stribling notes, adding that Coca-Cola had all along planned to experiment with Facebook's ad program in phases. Today, the company is taking a wait-and-see approach with Beacon.

According to Jonathan Johnson, senior vice president of corporate affairs at Overstock.com, the company is evaluating its use of Beacon in the future. "We launched with Facebook Beacon, had some complaints and immediately turned it off," says Johnson. "We need to be sure that the Facebook community understands how it works."

### **No One Knows You're a Dog**

According to Wharton marketing professor [Z. John Zhang](#), the Facebook incident highlights the Internet's privacy conundrum. "With the Internet, you have unlimited potential for privacy: No one knows you're a dog," he says, referring to a famous *New Yorker* magazine cartoon. "On the other hand, a company can accumulate so much information about you, including how much time you spend on a website and [what sites] you visit. If [a company] pulls that information together with other data, [the user] loses privacy. If companies target too much, the entire online environment will change. It becomes big brother-ish."

Zhang says the biggest issue with Facebook's Beacon plan was that the change was too radical. Facebook users were accustomed to sharing information on the social networking site, but once tracking branched out to third party sites, users became concerned. "There is this adjustment people make over time," says Zhang. "If you lose a little privacy today and tomorrow, over time you don't notice it as much. Facebook's Beacon was too drastic."

Kendall Whitehouse, senior director of IT at Wharton, agrees. "What's troubling people with Facebook is the radical change," he says. "There's a strong backlash because Beacon was introduced after Facebook users had spent a great deal of time creating their profiles and networking with friends under certain assumptions of privacy and control. Many users have a strong attachment to the site and how it worked. Then Facebook suddenly changed the rules of the game."

What's unclear is whether Facebook's privacy fumble will have any lasting impact. Matwyshyn says that in the late 1990s, there were privacy concerns about so-called "cookies," small files that websites deposit on your PC to track usage and remember items like user preferences. Today, cookies are commonly used by numerous websites.

Whitehouse contrasts Facebook's multi-site tracking techniques with the way cookies were originally intended to be used. "By design, cookies are meant to be written and read by a single site and, as such, I see no problem with the technology. I would assume that any website I visit has the ability to know what I do while I'm on their site. But some ad systems now serve banner ads from a central server to multiple websites and, by doing so, can track a user's movement across different sites." And this, according to Whitehouse, raises larger concerns, as does Facebook's tracking system. "Facebook's Beacon system takes this to a new level by allowing cross-site actions to be recorded back to Facebook, which is particularly troublesome since, in the case of Facebook, the behavior can be linked to your individual user account -- and thus to your name and profile."

For Matwyshyn, the key to online ad targeting is transparency. Companies need to be clear about what they are doing with customer information and provide easy opt-out and opt-in procedures. "The same type of cross linking and tracking at Facebook may have been acceptable in a different presentation with a transparent process and an explanation of what was happening," says Matwyshyn. "Users didn't expect the type of connection that Beacon had."

Turow agrees that transparency would ease privacy concerns, but a clear-cut disclosure of motives is unlikely. "I would love transparency, but there's a real tension marketers feel between the desire to bond with customers and the incentive to undermine that trust. Any time you collect data to market to people, you are eroding trust.... If companies were completely transparent, everyone would opt out."

As a result of this transparency tug of war, Turow argues that consumers have no idea what targeting goes on "behind the screens." "People really don't know very much about marketing data on the web and off," says Turow. "They understand they are being tracked, but they don't understand privacy policies, which aren't designed to be read." Indeed, an Annenberg Public Policy Center survey found that 59% believe that if a company has a privacy policy, that it won't share information with third parties. That's not true, says Turow.

Facebook's response to the privacy concerns over Beacon was to switch to an opt-in policy. What remains

to be seen is how many people will allow Facebook to track their visits to third party websites. According to Turow, a straight opt-in policy is the gold standard when it comes to privacy. All consumers should have to opt in to share information with companies. The big issue with the 'opt-in only' approach is that few people would choose to share data, acknowledges Turow. "If everything was opt-in, no one would participate."

There is a hybrid approach where companies could have an 'opt-in only' policy and pay customers for information and insight, says Turow. As Zhang puts it: "There has to be some inducement."

## The Learning Curve

Finding the balance between better targeting and privacy is going to take time, says Hill. "We are all just learning on both the [company] side and user side."

Wharton experts generally agree, suggesting that the younger generation of web users -- those in high school and college -- will ultimately reveal the emerging attitudes about privacy. Why? This generation will be the first to have been exposed to social networks at an early age over a long period of time. They will also be the ones who have become accustomed to broadcasting their lives over MySpace and Facebook. The question is how attitudes change as these users grow up.

"Younger users use the Internet differently" than older ones, says Hill. "There may be a slower learning curve [about privacy], but when things go wrong, they will pull back. Consequences -- such as not getting a job because of something you posted on MySpace -- will change behavior quickly. Older users have learned that it's important not to put all of your information out there."

Matwyshyn suggests that "people will learn the hard way about privacy. Once privacy is challenged, there will be a greater sensitivity to information being provided involuntarily. If users feel they can't control information, they will use the medium less."

The current generation of web users will make for a revealing case study on privacy in another decade, Whitehouse adds. "We don't have a long history in this area. This is the first generation that has grown up with these social networking tools. It will be interesting to see where the world is in 10 years when these people have jobs and families. We may see the pendulum swing back a bit on privacy. A lot of us did some stupid things when we were younger, but they weren't broadcast worldwide. This generation is different, but is it different because something has fundamentally changed or simply because it's currently dominated by young people? Time will tell as today's youth grow into adulthood."

On the corporate side of the equation, marketers have to be sensitive to privacy issues and "do what users consider reasonable," says Matwyshyn. "Companies are trying to be sensitive, yet trying to know their customers."

Given the dollars at stake -- research firm ZenithOptimedia projects global Internet advertising to be \$60.88 billion in 2010, a sum that will top the amount spent on magazine advertising -- companies are racing to figure out the privacy vs. better targeting equation. Just don't expect a solution for that advertising equation overnight, says Turow. "There are complicated questions to be addressed. This data is really the story of you. Who owns your information? Why give up ownership of your story? Are you opening yourself up too much? These are deeply philosophical questions that don't get answered overnight."

---

This is a single/personal use copy of Knowledge@Wharton. For multiple copies, custom reprints, e-prints, posters or plaques, please contact PARS International: [reprints@parsintl.com](mailto:reprints@parsintl.com) P. (212) 221-9595 x407.