

Social Media Notebook: Will Privacy Be the Achilles' Heel of the Healthcare Social Media Revolution?

By Fard Johnmar

<http://www.mdnglive.com/articles/notebook-achilles>

Earlier this year, the popular social network Facebook introduced a new initiative designed to help corporations advertise to its users. Facebook's "Beacon" allowed members to "share information [about their actions on]... other websites for distribution to their friends." Facebook allowed advertisers to select the type of content that would be shared via the social network, including purchase information.



Facebook promised its users they would be able to “decide whether to distribute specific actions from participating sites with their friends.” Unfortunately, reality did not match Facebook’s promises. A few weeks after Beacon launched, influential Forrester analyst and blogger Charlene Li wrote a post, “[Close Encounter with Facebook Beacon](#),” in which she related her disturbing experience with the new advertising service. She said: Earlier this week, I bought a coffee table on [Overstock.com](#). When I next logged into Facebook... [I] saw [information about my purchase on my newsfeed]. I was pretty surprised to see this, because I received no notification while I was on Overstock.com that they had the Facebook Beacon installed on the site. If they had, I would have turned it off.

I used my personal e-mail address to buy the coffee table, so I was puzzled why and how this ‘personal’ activity was being associated with my ‘public’ Facebook profile. Li went on to note that her biggest problem with Facebook Beacon was that she didn’t have control over the information that would be shared with her network. She said “I need to be in control and not get blindsided... I was seriously wiggged out, but wouldn’t have been if Overstock had simply told me that they were inserting a Facebook Beacon and given me the opportunity at that time to opt-in to Beacon.”

Although purchasing a coffee table is an innocent activity, in a healthcare context, the situation could potentially carry serious repercussions. For example, what if a Facebook member with bipolar disorder

purchases a book about this condition on Amazon.com? Here's the catch: no one in their immediate network knows that they have this condition and the user does not want to share this information. All of a sudden, because of Beacon, everyone knows. This potentially serious privacy breach could have serious personal and professional repercussions.

Facebook Quenches Beacon Firestorm, but Privacy Concerns Remain

After weeks of user protest and negative press, [Facebook decided to modify Beacon](#). The company promised that "users will have clear options... to either delete or publish [information about their purchases]."

Facebook's move is welcome; however, the Beacon flap indicates that user privacy can sometimes take a back seat when Web 2.0 companies are racing to maximize their advertising revenue. This should be a major concern for healthcare social media advocates. Many companies are taking privacy concerns very seriously; however, there is a real possibility a company will someday inadvertently release or share private medical information. After all, it has happened before.

In 2002, Eli Lilly and Company agreed to settle Federal Trade Commission (FTC) charges that it had failed to protect information patients submitted on its Prozac.com website. According to the FTC, "A Lilly employee created a new computer program to access Medi-messenger subscribers' e-mail addresses and sent them an e-mail message announcing the termination of the Medi-messenger service. The [June 27 e-mail message](#) included all of the recipients' e-mail addresses within the 'To:' line of the message, thereby unintentionally disclosing to each individual subscriber the e-mail addresses of all 669 Medi-messenger subscribers." The FTC argued that Lilly violated its own privacy policies and failed to take appropriate steps to protect users' sensitive information.

Another concern is that many Internet users are not worried that their personal information is floating around in cyberspace. According to a report released in December 2007 by the Pew Internet & American Life Project, 60% of Internet users are "unconcerned about the extent of data available about them online." However, there are signs this blasé attitude may be partly fueled by ignorance. Privacy advocates say that information Internet users do not believe is online (such as their e-mail addresses, phone numbers, and names of employers) can be found via a simple search engine query.

As social media applications become more ubiquitous and powerful, it is very likely that Americans will continue to use them for health-related purposes. However, a major privacy breach could significantly set back efforts to empower patients, providers, and others using Web 2.0 technologies.

Fard Johnmar is the founder of Envision Solutions, LLC, a full-service healthcare marketing communications consulting firm. Visit www.envisionsolutionsnow.com to learn more about the company and the services it offers.