Facebook Is Using You

By LORI ANDREWS

LAST week, Facebook filed documents with the government that will allow it to sell shares of stock to the public. It is estimated to be worth at least $75 billion. But unlike other big-ticket corporations, it doesn't have an inventory of widgets or gadgets, cars or phones. Facebook's inventory consists of personal data — yours and mine.

Facebook makes money by selling ad space to companies that want to reach us. Advertisers choose key words or details — like relationship status, location, activities, favorite books and employment — and then Facebook runs the ads for the targeted subset of its 845 million users. If you indicate that you like cupcakes, live in a certain neighborhood and have invited friends over, expect an ad from a nearby bakery to appear on your page. The magnitude of online information Facebook has available about each of us for targeted marketing is stunning. In Europe, laws give people the right to know what data companies have about them, but that is not the case in the United States.

Facebook made $3.2 billion in advertising revenue last year, 85 percent of its total revenue. Yet Facebook's inventory of data and its revenue from advertising are small potatoes compared to some others. Google took in more than 10 times as much, with an estimated $36.5 billion in advertising revenue in 2011, by analyzing what people sent over Gmail and what they searched on the Web, and then using that data to sell ads. Hundreds of other companies have also staked claims on people's online data by depositing software called cookies or other tracking mechanisms on people's computers and in their browsers. If you've mentioned anxiety in an e-mail, done a Google search for "stress" or started using an online medical diary that lets you monitor your mood, expect ads for medications and services to treat your anxiety.

Ads that pop up on your screen might seem useful, or at worst, a nuisance. But they are much more than that. The bits and bytes about your life can easily be used against you. Whether you can obtain a job, credit or insurance can be based on your digital doppelgänger — and you may never know why you've been turned down.

Material mined online has been used against people battling for child custody or defending themselves in criminal cases. LexisNexis has a product called Accurint for Law Enforcement, which gives government agents information about what people do on social networks. The Internal Revenue Service searches Facebook and MySpace for evidence of tax evaders' income and whereabouts, and United States Citizenship and Immigration Services has been known to scrutinize photos and posts to confirm family relationships or weed out sham marriages. Employers sometimes decide whether to hire people based on their online profiles, with one study indicating that 70 percent of recruiters and human resource professionals in the United States have rejected candidates based on data found online. A company called Spokeo gathers online data for employers, the public and anyone else who wants it. The company even posts ads urging "HR Recruiters — Click Here Now!" and asking women to submit their boyfriends' e-mail addresses for an analysis of their online photos and activities to learn "Is He Cheating on You?"

Stereotyping is alive and well in data aggregation. Your application for credit could be declined not on the basis of your own finances or credit history, but on the basis of aggregate data what other people whose likes and dislikes are similar to yours have done. If guitar players or divorcing couples are more likely to renege on their credit-card bills, then the fact that you've looked at guitar ads or sent an e-mail to a divorce lawyer might cause a data aggregator to classify you as less credit-worthy. When an Atlanta man returned from his honeymoon, he found that his credit limit had been lowered to $3,800 from $10,800. The switch was not based on anything he had done but on aggregate data. A letter from the company told him, "Other customers who have used their card at establishments where you recently shopped have a poor repayment history with American Express."

Even though laws allow people to challenge false information in credit reports, there are no laws that require data aggregators to reveal what they know about you. If I've Googled "diabetes" for a friend or "date rape drugs" for a mystery I'm writing, data aggregators assume those searches reflect my own health and proclivities. Because no laws regulate what types of data these aggregators can collect, they make their own rules.

In 2007 and 2008, the online advertising company NebuAd contracted with six Internet service providers to install hardware on their networks that monitored users' Internet activities and transmitted that data to NebuAd's servers for analysis and use in marketing. For an average of six months, NebuAd copied every e-mail, Web search or purchase that some 400,000 people sent over the Internet. Other companies, like Healthline Networks Inc., have in-house limits on which private information they will collect. Healthline does not use information about people's searches related to H.I.V., impotence or eating disorders to target ads to people, but it will use information about bipolar disorder, overactive bladder and anxiety, which can be as stigmatizing as the topics on its privacy-protected list.

In the 1970s, a professor of communication studies at Northwestern University named John McKnight popularized the term "redlining" to describe the failure of banks, insurers and other institutions to offer their services to inner city neighborhoods. The term came from the practice of bank officials who drew a red line on a map to indicate where they wouldn't invest. But use of the term expanded to cover a wide array of racially discriminatory practices, such as not offering home loans to African-Americans, even those who were wealthy or middle class.

Now the map used in redlining is not a geographic map, but the map of your travels across the Web. The term Weblining describes the practice of denying people opportunities based on their digital selves. You might be refused health insurance based on a Google search you did about a medical condition. You might be shown a credit card with a lower credit limit, not because of your credit history, but because of your race, sex or ZIP code or the types of Web sites you visit.

Data aggregation has social implications as well. When young people in poor neighborhoods are bombarded with advertisements for trade schools, will they be more likely than others their age to forgo college? And when women are shown articles about celebrities rather than stock market trends, will they be less likely to develop financial savvy? Advertisers are drawing new redlines, limiting people to the roles society expects them to play.

Data aggregators' practices conflict with what people say they want. A 2008 Consumer Reports poll of 2,000 people found that 93 percent thought Internet companies should always ask for permission before using personal information, and 72 percent wanted the right to opt out of online tracking. A study by Princeton Survey Research Associates in 2009 using a random sample of 1,000 people found that 69 percent thought that the United States should adopt a law giving people the right to learn everything a Web site knows about them. We need a do-not-track law, similar to the do-not-call one. Now it's not just about whether my dinner will be interrupted by a telemarketer. It's about whether my dreams will be dashed by the collection of bits and bytes over which I have no control and for which companies are currently unaccountable.