Google Is Watching You

Digital privacy advocate and secret smoker Kevin Bankston was outed on Google's Street View. So, what else does the Internet know about us?

Kevin Bankston didn't think anyone would notice his little cigarette break. His family didn't know he sometimes snuck a smoke. So Bankston was surprised when a photo of him smoking outside his San Francisco office appeared online several years ago on Amazon.com's (AMZN) now-defunct A9.com map service. He was even more shocked when, in May, he found out he was caught again on candid camera—possibly smoking—this time by Google's (GOOG) new "Street View" map service.

Bloggers began buzzing about Bankston's double-lightning-strike luck, and the two photos now appear all over the Internet. A Web search for "Kevin Bankston smokes" reveals more than 20,000 links. "I felt somewhat embarrassed and a bit spied upon," says Bankston. "I am now thoroughly outed as a cigarette smoker."

PRIVACY ADVOCATES SEEK PROTECTIONS

Coincidentally, Bankston also happens to be one of the leading advocates for digital privacy. An attorney for the Electronic Frontier Foundation, he's trying to turn his personal problem into a larger point: In the quest to fill the Web with information, online companies are often trampling on individuals' right to privacy, says Bankston.

Of course, the trade-off between privacy and Web innovation is nothing new. The Internet's most popular services enable people to do everything from research ailments to virtually tour Times Square—for free. But when you type in a Web search, your words are stored by Google and other search providers, along with information tying those words to your personal computer. If you surf the Web, the pages you visit and what you do on them are tracked with "cookies," tiny text files that download to your computer so they can report back to their ad network owners.

But while Web services have long made their money tailoring advertisements to individuals based on their online doings, more users are paying attention, and some are starting to balk. Consumer advocates and privacy experts have renewed cries for stricter guidelines—even new laws—that would change the way many Web companies do business.

CURBING DATA RETENTION

Government agencies in the U.S. and overseas are taking notice. The European Union's Data Protection Working Party has heavily criticized Google's retention of search data. In the U.S., the Federal Trade Commission is reviewing whether to allow a string of proposed acquisitions of ad networks by major search companies. Those deals—Google's $3.1 billion takeover of DoubleClick (DCLK), Microsoft's (MSFT) $6 billion buyout of aQuantive (AQNT), and Yahoo!'s (YHOO) $720 million purchase of Right Media—would enable the big search providers to start tracking which Web sites individuals visit outside their own networks (see BusinessWeek.com, 5/21/07, "Behind Those Web Mergers").

Already, some of the pushback has resulted in change. In June, Google said it would scale back how long it retains search data from 24 months to 18 months and would consider letting its cookies expire earlier. In response to complaints, Google also made it easier to have an image removed from its map services, which have captured people in compromising positions such as sunbathing and flashing underwear. Bankston's photo is no longer on the site.

Many privacy advocates want more concessions. Bankston would like Google to blur the faces of everyone in its map pictures. Others would like to see search words and data stored only for as long as it takes to deliver the immediate search results and related ads. Still others would like all companies that use cookies to alert users regularly and proactively give them the option not to be tracked.

TARGETED ADS RELY ON USER DATA

If the most stringent calls are heeded, more than mergers would be at risk. Over the next four years, $9.6 billion is expected to be spent on ads triggered by a user's online surfing activity, according to a June eMarketer report. While sites that feature auto reviews and fashion news would continue to attract ads, Web sites without such obvious draws would be hard hit by the loss of ads placed as a result of surfing behavior.

Many Web companies say the privacy concerns are, in many respects, overblown. After all, the information collected online is tied to a number representing a particular computer, not to a person's name or Social Security number. And the companies say they're only collecting the information to show say, a car ad, to someone who might be in the market for a car. They don't want to know someone's address, political views, or any other information that isn't tied to a potential purchase. They just want to deliver fewer untargeted ads.

There's reason for marketers to believe that people respond well to targeting. In his June report, eMarketer senior analyst David Hallerman found that users are more willing to receive ads related to things they like. "Although they are generally unaware that behavioral targeting is the cause, many consumers find ads that are systematically more relevant to their interests, preferences, or intentions to be more palatable or even welcomed," wrote Hallerman. That's not to say privacy is not a concern, he says. But it's not enough of a worry to give up free services and content. "People are used to the fact that, in order to get something for free, they will see ads," says Hallerman.

TRADING PRIVACY FOR FREE SERVICE

Web companies say they are not running afoul of any privacy laws. Google, for example, says the photos for Street View don't capture anything that passersby couldn't see as well. "All the imagery is being collected on public streets…It is just like what we are seeing walking down a street," says Stephen Chau, product manager of Google Maps.

More important, many Web companies argue that consumers are not willing to sacrifice the availability of free access to services in exchange for more privacy. This year, Amobee, a Redwood City (Calif.) company that delivers ads to cell phones ran a series of trials offering consumers the option to choose between a paid download service and a free ad-supported service that would track some of their mobile Web-surfing behavior. For every consumer who paid for the content, 50 more took the free version with targeted ads.

Roger Wood, senior vice-president for Amobee's Americas region, says people born after 1975 have

completely different attitudes about privacy and are more receptive to the Web's trade-offs. "Where you live, how many times a day you shop, how many girlfriends you have—they don't care about that level of privacy," says Wood.

But do younger generations care about privacy at all? Wood thinks today's teens and twentysomethings do jealously guard their thoughts and feelings. However, a scan of the Internet shows evidence to the contrary. After all, people share everything from what they ate for dinner to their political views on publicly searchable blogs. "Lifecasters" like Justin.tv's Justin Kan, who videotapes every moment of his day to stream live on the Web for public consumption, share their intimate conversations and moments. Likewise, millions have uploaded videos of themselves to Web sites such as YouTube and Metacafe.

LIMITS TO SHARING

Despite all the sharing—or perhaps oversharing—privacy advocates maintain that many people do care. In her upcoming book, Privacy in Context, New York University professor Helen Nissenbaum argues that people expect varying amounts of privacy depending on where they are, even when online or in public. Nissenbaum points to the anger Facebook users showed when the social network installed a feature automatically updating all their approved "friends" to new posts. Clearly, she says, users expected that certain people would see the things they wrote, but that it would fly under the radar for most users (see BusinessWeek.com, 9/8/06, "Facebook Learns from Its Fumble").

Similarly, many AOL (TWX) users were outraged after the company posted search records, identifiable only by a number assigned to individual computers, on the Internet. Online publications identified several users from the data and The New York Times came knocking on one user's door, showing her searches about her family and friends' health problems. Several people sued AOL (see BusinessWeek.com, 8/23/06, "Fallout from AOL's Flub").

Whether it's a topless sunbather tanning on her roof in the Netherlands or just a guy on his cigarette break, most people don't expect millions of Internet voyeurs to catch them in the act. Perhaps they'll need to get used to it.

Holahan is a writer for BusinessWeek.com in New York.

Catherine Holahan