Online, your private life is searchable

Photos, addresses, family ties, court documents, details from MySpace profiles -- the moment information is published online, it can be copied and re-posted, and often is.

By David Sarno

August 16, 2009

When Maya Rupert wrote an article frowning at several Southern states for officially celebrating Confederate History Month, Internet critics lined up to fire back.

But this time, they arrived with more than harsh words.

The 28-year-old Los Angeles attorney's detractors dug up a photo of her and posted it, along with details of political contributions she'd made, in an online discussion of the article she wrote for the L.A. Watts Times. They called their finds evidence of her bias on the emotionally charged subject.

"It really surprised me when I found out that people could see how much I donated to Obama," Rupert said, referring to the $400 she gave to the candidate last year, the record of which is available through several online watchdog sites.

After that, Rupert said, "they pulled a picture off my firm's website and said, 'Of course she's black.' "

Until recently, personal information has been scattered across cyberspace, to be found or not depending on the luck and sophistication of the searcher. But a new crop of "snooper" sites is making it easier than ever for anyone with Internet access to assemble the information into a digital portrait.

"It's amazing what you can Google," one of the people who criticized Rupert wrote in an online forum.

Rupert has since learned that the photo and campaign contributions were just a small part of her online "footprint" -- an expansive dossier that she did not realize was available to anyone searching her name.

On Snitch.name, users can enter a name -- their own or someone else's -- and watch as the site culls information from dozens of search engines, social networks and directories.

Rupert entered her name into Snitch last week, and within a minute she was presented with photos of herself, details of her California Bar membership and the names and addresses of her sister and parents.

"I'm a fan of open records and a fan of a lot of information being public," she said. "But there's public," and then there's the unfettered Web where "at the touch of a button, I can find out private information about you and use that for other purposes."

"It's really creepy," she said.

Looking in the digital mirror

Online information about consumers comes from several sources. Public records such as campaign contributions, property sales and court cases are increasingly posted on the Internet. At the same time, marketers are collecting information about consumers' Web browsing and buying habits. And then there are the thousands of online communities such as Facebook and Twitter, where users supply the personal information themselves.

In general, people have felt that their information is better protected within the walls of social networks, where they can control what is posted and approve who can view it. But privacy experts warn against being lulled into a false sense of security.

"The rule of thumb for Internet privacy is that you don't let it get out there in the first place," said Pam Dixon, founder of the World Privacy Forum. The moment information is openly accessible online, it can be -- and often is -- copied from one site to another, making it extremely onerous to stamp out even if it's deleted from the original site.

"It's not like chasing Alice in Wonderland down a rabbit hole," Dixon said. "It's like chasing a hundred Alices down a hundred rabbit holes."

In the course of exploring her own digital footprint, Rupert saw photos and information from a social networking profile she'd started in 2003 on Friendster.com, thinking that only her friends would be able to see it. Little did she know that, years later, much of the material would end up exposed to the open Web. Details from her MySpace profile had also been copied to third-party sites she'd never heard of, where they remained accessible no matter whether she removed the material from MySpace.

Even if you don't post any information about yourself online, however, maintaining a low profile can be a challenge.

Sites such as Huffington Post's FundRace2008 can freely gather and post information about hundreds of thousands of campaign contributions, including the donor's name and address and the amount donated.

BlockShopper.com maps home sales -- including the property's sale price, its address, and the names of the buyer and seller. That data is publicly available, often from county assessor and recorder offices.

Many kinds of court documents, which can contain social security numbers and family details, are public records. And city governments can post building permit applications, complete with blueprints of private homes.

Vatche Yepremian, who runs a mortgage lending company in Glendale, said he was well acquainted with the array of public information available about him online. His footprint includes details about several properties he owns, a home remodel plan he submitted to Glendale in 2007 and various court proceedings in which he is named.

Rather than being disturbed by the availability of data, Yepremian said it has been a useful tool when deciding whether to grant applicants a loan.

"If I want to lend money to someone, I want to make sure that everything and anything they've told me is the truth," Yepremian said. Even a few years ago, verifying an applicant's claims might have required a call to a title company or a crosstown drive to inspect a property. Now the Web saves him the trouble. "It makes life much easier," he said.

Perhaps the least understood by consumers is the practice of behavioral tracking, where marketing companies log activities such as the Web pages users visit, the ads they click and the terms they search for.

Most companies say information about user activities is stored securely and anonymously.

Even so, Paul Stephens of the Privacy Rights Clearinghouse said, "an individual's patterns on the Internet can reveal a tremendous amount of information about them, and it can be a gold mine for companies that want to market to you."

Privacy advocates say many consumers are hardly aware that any of their online activities are being stored, much less analyzed for marketing purposes.

"The standard online right now is that your information is taken and used unless you opt out," Stephens said. But in order to do so, consumers must first realize there's something to opt out of. That will require greater transparency on the part of those collecting information, Stephens said.

Behavioral tracking has an Orwellian ring to it, but the ability to efficiently guess consumers' desires is fundamental to the fast-moving world of online marketing.

"Many of our favorite sites on the Web are supported by advertising," said Alissa Cooper of the Center for Democracy and Technology. "It's an incredibly important piece of the fabric of the Web."

That's why banning behavioral tracking is not the solution, Cooper said. "The real key is for consumers to know what is going on and to be able to make an informed choice about whether they want their data to be part of the process."

Limiting your personal exposure

With little federal regulation of the use of information that companies collect online, consumers are often left to their own devices to protect themselves.

Googling your own name has often been referred to as "vanity searching" -- but now it's better thought of as vigilance.

Use search engines to keep track of what's out there about you and to spot unwanted leaks early. "People search" sites such as Snitch.name,

Spock and PeekYou can also be useful when trying to clean up your digital breadcrumbs.

If you find information about you on a website you believe has no right to it, write to the site owner and request that it be removed. Getting a response may be difficult, however, as many of the sites that compile and store such details are automated. If the data is particularly sensitive, ask a lawyer for advice.

When signing up for a consumer or social site where you might share personal information, make sure to familiarize yourself with the privacy policy and learn how to work the site's privacy settings.

Social networks such as Facebook give users relatively high levels of control over who sees their data, but don't assume that your profile is private by default: Often you'll need to tighten the settings yourself to deny access to people you don't know.

Many government records are public by law, and preventing them from appearing online can be difficult, said Dixon of the World Privacy Forum. But consult a lawyer; judges are able to seal some documents and records, generally before they go online.

It's also possible to avoid certain types of behavioral tracking. One of the easiest ways is to restrict your Web browser's use of "cookies" -- the tiny data mechanism that helps sites keep track of your browser.

By regularly clearing your cookies, you can cut down on the number of clues you're offering to marketers regarding your browsing habits. Look for a privacy setting in your browser's "Options" area that allows you to limit which types of cookies your browser accepts and how quickly they expire.

The growth of the Internet may actually spur the evolution of digital privacy, said Cooper of the Center for Democracy and Technology.

"Consumers are becoming producers and putting their own content on the Web," she said. "With that comes the urge to be able to control who sees what."

david.sarno@latimes.com

http://www.latimes.com/business/la-fi-cover-privacy16-2009aug16,0,5238484,print.story