NEW YORK POST

iSpy: Online companies spy on you more than you think — even reading your e-mail

by LARRY GETLEN

Posted: January 7, 2012

I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy
by Lori Andrews
Free Press

If you post a photo online from your iPhone, tech-savvy stalkers can tell exactly where you are. Researchers can predict the first five digits of your Social Security number from just your webcam photo. And if you type your name in the search box at Spokeo.com, you could wind up staring at a picture of your own front door.

While most people are aware that some amount of privacy has been lost due to the Internet and social media, "I Know Who You Are and I Saw What You Did" documents exactly how much we've lost and what dangers we face as a result.

"If someone broke into my home and copied my documents, he'd be guilty of trespass and invasion of privacy. If the cops wanted to wiretap my conversation, they'd need a warrant," writes Lori Andrews, a law professor and an expert on the integration of law and technology.

GETTY IMAGES

"But without our knowledge or consent, virtually every entry we make on a social network or other website is surreptitiously bring tracked and assessed."

Companies have contracted with Internet service providers to access everything we do on the web — even the contents of our e-mail messages — without our knowledge or consent.

These abuses are everywhere, as our information is collected and/or sold by our Internet service provider, the websites we visit, and even websites and companies we've never heard of (such as Spokeo, one of several websites that makes comprehensive information on people available for just a few dollars a month).

As early as 2001, the data aggregator DoubleClick was leaving tracking tools on the computers of visitors to 11,000 websites, including the 1,500 most-visited sites on the Internet.

In the course of researching this book, the author discovered that Comcast, her own ISP, had installed more than 100 tracking tools on her computer. More surprisingly, a site as seemingly innocuous as Dictionary.com left an incredible "234 tracking tools on a user's computer without permission — only 11 from Dictionary.com, and 223 from companies that track Internet users."

Andrews lays the blame on the industry known as behavioral advertising, which uses the web to collect as much information on individual consumers as possible.

Behavioral advertisers have struck deals with ISPs and websites to gain access to our data using a variety of online tools, and the level of intrusion is shocking.

If you use a free e-mail service such as Gmail for instance, you see targeted banner ads — because your messages have been "scraped" by companies. E-mail someone that you're pregnant? Expect diaper ads on your screen.

As one might assume, Facebook is a major offender, using the personal information of over 750,000,000 people — information people initially thought would remain private — to accommodate advertisers. Perhaps more frightening is that Acxiom — a data-aggregating company most people have never heard of — "has data on half a billion people from around the world, including 96% of Americans," with "an average of 1,500 pieces of data on each person [including] everything from their credit scores to whether they've bought medication for incontinence."

As much as our information is taken without our knowledge, the information we voluntarily place online — often believing it private — is used against us as well.

The book is rife with examples of people who lost their jobs for seemingly innocent and protected social-network postings — such as the teacher left unemployed for a photo of herself drinking a Guinness and a posting that she was playing "Crazy Bitch Bingo" — and mothers who've lost custody of their children for putting photos online with even a hint of sexuality.

Another of the book's stunning revelations, in fact, is the attitude of the courts toward the online world. Judges in divorce proceedings routinely allow one spouse access to the other's private social network accounts (and even, at times, their entire hard drive) as a matter of course. In one case, a disabled woman was denied spousal support in her divorce just because on her Match.com page, she stated that she led "an active lifestyle."

And where courts wouldn't allow references to a victim's past sexual history in a rape case, that has been shockingly reversed as it pertains to online activity. One father convicted of raping his 13-year-old daughter appealed, stating that the court should have allowed the inclusion of sexy photos and quizzes from the girl's MySpace page as evidence. While the appeal was denied for other reasons, the court did hold that the page should have been admitted as evidence that spoke to the girl's credibility.

"I Know Who You Are and I Saw What You Did" shows how the way society deals with the online world needs to be rethought, as the current methods make every one of us a potential victim.

At one point, the author recounts how, when her son was a month old, a friend placed "an Elvis-style gold chain around his neck . . . put a sealed bottle of Jack Daniel's in the stroller next to him," and then took a photo.

"What if she'd posted it on a social network," Andrews asks. "The Department of Children and Family Services might have tried to take my baby from me."

Larry Getlen, "iSpy: Online companies spy on you more than you think — even reading your e-mail," *New York Post*, Jan. 7, 2012, http://www.nypost.com/p/news/opinion/books/ispy_7LFM3AWIGs2bcs5yNraoIJ#ixzz1izJtNwxb.