Sample T.W.

**"The Already Big Thing on the Internet: Spying on Users"**
**By Adam Cohen**

In 1993, the dawn of the Internet age, the liberating anonymity of the online world was captured in a well-known New Yorker cartoon. One dog, sitting at a computer, tells another: "On the Internet, nobody knows you're a dog." Fifteen years later, that anonymity is gone.

Anonymity on the Internet is gone

It's not paranoia: they really are spying on you.

active surveillance of users

Technology companies have long used "cookies," little bits of tracking software slipped onto your computer, and other means, to record the Web sites you visit, the ads you click on, even the words you enter in search engines — information that some hold onto forever. They're not telling you they're doing it, and they're not asking permission. Internet service providers are now getting into the act. Because they control your connection, they can keep track of everything you do online, and there have been reports that I.S.P.'s may have started to sell the information they collect.

Commercial uses of spying on consumers

The driving force behind this prying is commerce. The big growth area in online advertising right now is "behavioral targeting." Web sites can charge a premium if they are able to tell the maker of an expensive sports car that its ads will appear on Web pages clicked on by upper-income, middle-aged men.

Commercial motivation

The information, however, gets a lot more specific than age and gender — and more sensitive. Tech companies can keep track of when a particular Internet user looks up Alcoholics Anonymous meetings, visits adult Web sites, buys cancer drugs online or participates in anti-government discussion groups.

personal information & histories aren't protected

Serving up ads based on behavioral targeting can itself be an invasion of privacy, especially when the information used is personal. ("Hmm ... I wonder why I always get those drug-rehab ads when I surf the Internet on Jane's laptop?")

electronic invasion of privacy

The bigger issue is the digital dossiers that tech companies can compile. Some companies have promised to keep data confidential, or to obscure it so it cannot be traced back to individuals. But it's hard to know what a particular company's policy is, and there are too many to keep track of. And privacy policies can be changed at any time.

companies compiling files on private user data

There is also no guarantee that the information will stay with the company that collected it. It can be sold to employers or insurance companies, which have financial motives for wanting to know if their workers and policyholders are alcoholics or have AIDS.

Financial motivations to sell the info

It could also end up with the government, which needs only to serve a subpoena to get it (and these days that formality might be ignored).

info available for govt monitoring

If George Orwell had lived in the Internet age, he could have painted a grim picture of how Web monitoring could be used to promote authoritarianism. There is no need for neighborhood informants and paper dossiers if the government can see citizens' every Web site visit, e-mail and text message.

The public has been slow to express outrage — not, as tech companies like to claim, because they don't care about privacy, but simply because few people know all that is going on. That is changing. "A lot of people are creeped-out by this," says Ari Schwartz, a vice president of the Center for Democracy and Technology. He says the government is under increasing pressure to act.

The Federal Trade Commission has proposed self-regulatory guidelines for companies that do behavioral targeting. Anything that highlights the problem is good, but self-regulation is not enough. One idea starting to gain traction in Congress is a do-not-track list, similar to the federal do-not-call list, which would allow Internet users to opt out of being spied on. That would be a clear improvement over the status quo, but the operating principle should be "opt in" — companies should not be allowed to track Internet activities unless they get the user's expressed consent.

The founders wrote the Fourth Amendment — guaranteeing protection against illegal search and seizure — at a time when people were most concerned about protecting the privacy of their homes and bodies. The amendment, and more recent federal laws, have been extended to cover telephone communications. Now work has to be done to give Internet activities the same level of privacy protection.

*The New York Times* | Editorial Observer, April 5, 2008