

NAME Heegan Greenman

PERIOD 1st

Article of the Week #1 (Sept. 1)

The Internet Is Spying on You

← This is what the entire article is about because it all is talked about

Every time you go online, sophisticated data miners are tracking your every move. What do they know about you?

How frequently am I followed online?
 Constantly. Your computer leaves a unique digital trail every time you visit a website, post a comment on a blog, or add a photo to your Facebook wall. A growing number of companies follow that trail to assemble a profile of you and your affinities. These profiles can contain shocking levels of detail—including your age, income, shopping habits, health problems, sexual proclivities, and ZIP code—right down to the number of rooms in your house and the number of people in your family. Although trackers don't identify their subjects by name, the data they compile is so extensive that "you can find out who an individual is without it," says Maneesha Mithal of the Federal Trade Commission.

How does the technology work?
 The moment you land on a website, it installs a unique electronic code on your hard drive. Owners of websites originally placed "cookies," the simplest such codes, on computers for users' convenience, in order to remember things like the contents of online shopping carts. But a cookie placed by one site can also serve as a tracking device that allows marketers to identify an individual computer and follow its path on every Web visit. It's like a clerk who sells you a pair of jeans at one store, then trails you around the mall, recording every store you visit and every item of clothing you try on. "Beacons" are super-cookies that record even computer keystrokes and mouse movements, providing another layer of detail. "Flash cookies" are installed when a computer user activates Flash technology, such as a YouTube video, embedded on a site. They can also reinstall cookies that have been removed. Such "persistent cookies," says Marc Rotenberg of the Electronic Privacy Information Center, make it "virtually impossible for users to go online without being tracked and profiled."

Who's doing the spying?
 Marketers, advertisers, and those whose businesses depend on them. Most websites install their own cookies and beacons, both to make site navigation easier and to gather user information. (Wikipedia is a rare exception.) But third parties—advertisers and the networks that place online ads, such as Google and iAds—frequently pay site hosts to install their own tracking technology. Beacons are even sometimes planted without the knowledge of the host site. Comcast, for example, installed Flash cookies on computers visiting its website after it accepted Clearspring Technologies' free software for displaying slide shows. Visitors who clicked on a slide show at Comcast.com wound up loading Clearspring's Flash cookies onto their hard drives, which Comcast said it had never authorized.

How is personal data used?
 It's collected and sold by companies like Clearspring. Such information can be sold in large chunks—for example, an advertiser might pay \$1 for 1,000 profiles of

Notes on my thoughts, reactions and questions as I read.

This sentence instantly caught my attention because it made me very nervous

Yes
Yes

What happened to my privacy?

Do they possibly know you better than yourself?

Can these "cookies" see emails, texts etc.

This entire process is incredibly efficient

How long do these stay on your computer

Why are these "cookies" legal?

How do they know

But not that it did not know about it, or take advantage of it

Who sell it

This article was a deeply disturbing piece of information to digest if it is true or an extremely ill humored prank. The article was most likely directed toward the general public, in order to inform them how little privacy they really have with their internet use and to also cause people to question if they want people to know what they do while connected to the internet. The author first tells exactly how much anyone can learn about you for a price... less than a candy bar. The author goes on to explain how and why marketers use codes known as "cookies" and "Beacons" to track what you do online. Then the author continues by giving examples of people who discovered what companies knew about millions of people. The author then describes that this practice is perfectly legal and how to avoid too much information from being gleaned from what you do on the net. In this rapidly developing world many have realized that knowledge is power.

For so little?