AOW 1:

THE INTERNET IS SPYING ON YOU

Margin Notes:_____/50

Questions:_____/50

Total Score:_____

Student _____
Class Period _____

Instructions: Read the following article carefully and **make notes in the margin** as you read. Your notes should include:

- Comments that show that you **understand** the article. (A summary or statement of the main idea of important sections may serve this purpose.)
- Questions you have that show what you are **wondering** about as you read.
- Notes that differentiate between **fact** and **opinion**.
- Observations about how the **writer's strategies** (organization, word choice, perspective, support) and choices affect the article.

Your **margin notes** are part of your score for this assignment.

THE INTERNET IS SPYING ON YOU
Every time you go online, sophisticated data miners are tracking your every move. What do they know about you?

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

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 movie lovers—or in customized segments. An apparel retailer might buy access to 18-year-old female fans of the *Twilight* movie series who reside in the Sunbelt. "We can segment it all the way down to one person," says Eric Porres of Lotame, which sells these profiles. Advertisers use the profiles to deliver individualized ads that follow users to every site they visit. Julia Preston, a 32-year-old software designer from Austin, recently saw how this works firsthand when she started seeing lots of Web ads for fertility treatments. She had recently researched uterine disorders online. "It's unnerving," she says.

Is all this snooping legal?
So far, yes. While an e-commerce site can't sell to third parties the credit card numbers it acquires in the course of its business, the legality of various tracking technologies—and the sale of the personal profiles that result—has never been tested in court. Privacy advocates say that's not because there aren't abundant abuses, but because the law hasn't kept pace with advancing technology. "The relevant laws," says Lauren Weinstein of People for Internet Responsibility, an advocacy group, "are generally so weak—if they exist at all—that it's difficult to file complaints."

Can you avoid revealing yourself online?
Aside from abandoning the Internet altogether, there's virtually no way to evade prying eyes. Take the case of Ashley Hayes-Beaty, who learned just how exposed she was when *The Wall Street Journal* shared what it had learned about her from a data miner. Hayes-Beaty's computer use identified her as a 26-year-old female Nashville resident who counts *The Princess Bride* and *50 First Dates* among her favorite movies, regularly watches *Sex and the City,* keeps current on entertainment news, and enjoys taking pop-culture quizzes. That litany, which advertisers can buy for about one-tenth of a cent, constitutes what Hayes-Beaty calls an "eerily precise" consumer profile. "I like to think I have some mystery left to me," says Hayes-Beaty, "but apparently not."

How to fight back against data miners
There are ways to minimize your exposure to data miners. One of the most effective is to disrupt profile-building by clearing your computer browser's cache and deleting all cookies at least once a week. In addition, turning on the "private browsing" feature included in most popular Web browsers will block tracking technologies from installing themselves on your machine. For fees ranging from $9.95 to $10,000, companies like ReputationDefender can remove your personal information from up to 90 percent of commercial websites. But it's basically impossible to eradicate personal information, such as property records and police files, from government databases. "There's really no solution now, except abstinence" from the Internet, says Lt. Col. Greg Conti, a computer science professor at West Point. "And if you choose not to use online tools, you're really not a member of the 21st century."

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

Answer questions ON NOTEBOOK PAPER, or type and print, and staple to the article. USE text evidence.

1. *Describe a danger associated with being spied upon via the internet.*
2. *In two sentences, summarize the message the author is trying to convey by writing this article.*
3. *Choose three vocabulary terms that you had not mastered prior to reading this article. Explain how you determined the meaning of these terms based on the selection rather than using a dictionary.*
4. *Does it disturb you that you being followed on the internet? Reflect.*
5. *Discuss what you might do to protect your privacy.*