

knowing it—see box) so they can deliver more effective ads. Web entrepreneurs are counting on advertisers paying a higher CPM (cost per thousand) for this rifle-shot data than they do for the old shotgun approach. “We charge more than average because each advertiser can see how their ad is performing with each demographic and can then focus their campaign,” says Steve Chadima, founder of Free-PC. Forrester

Research estimates that Internet advertising will grow from \$2.8 billion in 1999 to \$22 billion in 2004. But with click-through rates hovering at under 1%, those ad dollars will support only a handful of the many businesses that are making a go of the giveaway. “It’ll be a dogfight,” says Chan Suh, CEO of Net advertising operation Agency.com. “People who think that advertising makes up for the lack of a biz model and execu-

tion are going to fall by the wayside.” The Goody guys have no doubts about their model. But neither does their competitor, Third Voice, another free client that allows users to post on websites. These two Internet software firms will be battling it out for eyeballs, advertisers and traffic. One thing you can bet on, however: no price wars. —*With reporting by Susan Kuchinskas/San Francisco and Julie Rawe/New York City*

Click and Dagger: Is the Web Spying on You?

JEFF BEZOS, CEO of Amazon.com, describes the perfect online shopping experience as launching your browser and finding on the screen the exact item you want—which you may not have even known you wanted until that very moment. “One product,” he says, “with one button. And you click on it, and it is sent to you and improves the quality of your life.”

Retailers aren’t there yet. That perfect calibration of consumer desire and selling proficiency will require more information—privacy advocates say too much information—about you.

Marketers know plenty right now. Advertising networks like DoubleClick and MatchLogic, content sites like *Time.com* (TIME’s online affiliate), and even retailers like Amazon.com are able to gather information by depositing numerical files called cookies into your Web browser. Embedded in the cookie is an identifying number, like a cyber fingerprint, that alerts a server to your presence. Whoever sent the cookie can monitor where you go on the Web, what you click on, what you read, what you buy and what you don’t buy. Some sites, including Amazon, maintain strict privacy policies that promise to guard the data being gathered. But advertising networks like DoubleClick have

openly built a business around finding out what they can about you and passing it on to advertisers.

Most of us are unaware of being watched. But if you surf the net half an hour a day, chances are there’s an online profile of you—not the you who has a name, Social Security number and address but a cyber you who reflects your online behaviors and can help marketers target ads especially for you. Already, some of the ads you see when you hit sites like Yahoo or Lycos are there because you are. Other visitors

are getting different ads that cater to their online profiles.

The implications of this technology—and the potential threat to your right to privacy—are only now becoming understood. “A tremendous amount of personal-data collection is going on. Millions of people’s preferences, behaviors and desires are being profiled,” says Jeffrey Chester of the Center for Media Education.

Online ad agencies say they only want to improve the consumer experience, not gather dirt on webbies. “The point is to receive information that you are interested in as opposed to what you are not,” says

Lyn Chitow
Oakes, COO of ad

agency FlyCast. “It doesn’t seem like advertising if you’re interested in it.” For example, DoubleClick has 50 million active cookies, which means that 50 million people see at least one targeted ad a month. This prolific snooping is nothing new. Credit-card companies have been building databases for years and offering deals based on your spending habits.

But tailing someone through cyberspace may be far more revealing of personal details. “If you go to sites about mental health or pornography, that information could be subpoenaed in a civil suit or custody battle and used against you,” warns Jason Catlett, president of Junkbusters, a privacy advocacy group. That’s why the Federal Trade Commission convened a workshop last week to explore the privacy implications of Web profiling. “Not only are privacy policies difficult to locate online,” says FTC chairman Robert Pitofsky, “in almost all cases users don’t even know this is happening.”

The industry has vowed to self-regulate, hoping to ward off FTC oversight. If the feds do get involved, many Net businesses built around giving away products in exchange for consumer data may be on a collision course with your right to privacy.

—K.T.G.

With reporting by Adam Zagorin/Washington

