April 30, 2010

Shoppers Who Can't Have Secrets

By NATASHA SINGER

IT'S called behavioral tracking:

•

Cameras that can follow you from the minute you enter a store to the moment you hit the checkout counter, recording every T-shirt you touch, every mannequin you ogle, every time you blow your nose or stop to tie your shoelaces.

•

Web coupons embedded with bar codes that can identify, and alert retailers to, the search terms you used to find them and, in some cases, even your Facebook information and your name.

•

Mobile marketers that can find you near a store clothing rack, and send ads to your cellphone based on your past preferences and behavior.

To be sure, such retail innovations help companies identify their most profitable client segments, better predict the deals shoppers will pursue, fine-tune customer service down to a person and foster brand loyalty. (My colleagues Stephanie Rosenbloom and Stephanie Clifford have written in detail about the tracking prowess of store cameras and Web coupons.)

But these and other surveillance techniques are also reminders that advances in data collection are far outpacing personal data protection.

Enter the post-privacy society, where we have lost track of how many entities are tracking us. Not to mention what they are doing with our personal information, how they are storing it, whom they might be selling our dossiers to and, yes, how much money they are making from them.

On the way out, consumer advocates say, is that quaint old notion of informed consent, in which

a company clearly notifies you of its policies and gives you the choice of whether to opt in (rather than having you opt out once you discover your behavior is being tracked).

“How does notice and choice work when you don’t even interface with the company that has your data?” says Jessica Rich, a deputy director of the bureau of consumer protection at the Federal Trade Commission.

The commission has brought several dozen complaints against companies about possibly deceptive or unfair data collection and nearly 30 complaints over data security issues. In 2009, the commission proposed new guidelines for Web advertising that is tailored to user behavior.

The problem is, the F.T.C.’s guidelines are merely recommendations. Corporations can choose to follow them — or not. And the online advertising standards don’t apply to off-line techniques like observation in stores.

Mike Zaneis, vice president for public policy at the Interactive Advertising Bureau, a trade association based in Manhattan, says the advertising industry is not generally collecting personally identifiable data.

His group has worked closely with the F.T.C. on industry self-regulation, he says, and is developing new industry standards to alert consumers as they encounter ads based on their online behavior.

In the meantime, Mr. Zaneis says, consumers can use an industry program if they want to opt out of some behavior-based ads. As for mobile marketing, he says, consumers are always asked if they want to opt in to ads related to their cellphone location.

The larger issue here is not the invasion of any one person’s privacy as much as the explosive growth of a collective industry in behavioral information, says Jeff Chester, the executive director of the Center for Digital Democracy, a nonprofit group that works to safeguard user privacy.

“The whole business model is unfettered data collection of all your activities online and off,” Mr. Chester says. For example, he says that when consumers opt into cellphone ads, they may not understand that marketers may link their locations with information from third-party databases. The result, he says, is mobile dossiers about individual consumers.

As contradictory as it might sound, we need new strategies for transparent consumer surveillance.

In a country where we have a comprehensive federal law — the Fair Credit Reporting Act —

giving us the right to obtain and correct financial data collected about us, no general federal statute requires behavioral data marketers to show us our files, says Ms. Rich of the F.T.C.

So, is the European model, involving independent government agencies called Data Protection Commissions that are charged with safeguarding people's personal information, better than ours?

Europe's privacy commissioners have generally been more forward-looking, examining potential privacy intrusions like biometric tracking, while the F.T.C. is still trying to understand the magnitude and the implications of the Web, says Marc Rotenberg, the executive director of the Electronic Privacy Information Center, a research group in Washington.

"The U.S. system with regard to privacy is not working," Mr. Rotenberg says.

By early fall, the F.T.C. plans to propose comprehensive new privacy guidelines intended to provide greater tools for transparency and better consumer control of personal information, Ms. Rich says.

In the meantime, what if consumers take a more active interest in who is collecting information about them?

In a recent documentary called "Erasing David," the London-based filmmaker David Bond attempts to disappear from Britain's surveillance grid, hiring experts from the security firm Cerberus to track him using all the information they can glean about him while he tries to outrun them. In the course of the film, the detectives even obtain a copy of the birth certificate of his daughter, then 18 months old.

But the real shocker is the information Mr. Bond is able to obtain about himself — by taking advantage of a data protection law in Britain that requires public agencies and private businesses to release a person's data file upon his or her written request.

In one scene, Mr. Bond receives a phonebook-thick printout from Amazon.com listing everything he ever bought on the site; the addresses of every person to whom he ever sent a gift; and even the products he perused but did not ultimately buy.

He also receives a file from his bank, including a transcript of an irate phone call he once made after the bank lost one of his checks. The transcript noted that he seemed angry and raised his voice.

"It read like a mini-Stasi file," Mr. Bond said when I called him last week. When recorded messages inform us that we may be taped "for training or quality assurance purposes," he

reminded me, we should remember that our conversation may end up in our dossiers.

INSPIRED by Mr. Bond's odyssey, I called some companies with whom I do business.

A customer service representative at a bookstore chain where I have a discount card told me that the company maintains a list of the amount each member spends on each transaction so that the store can tell people how much money they saved at the end of the year. But a loyalty cardholder is not permitted to obtain his or her own purchase history.

Then I called an online travel agency and asked if I could get copies of my flight history and phone transcripts. I was regretting a disgruntled call I made to the agency a few months ago after being stranded at an airport in a blizzard. The customer care rep said clients couldn't obtain their own transcripts unless it was for legal purposes.

Was I being taped this time, too? They always tape, he said.