Code That Tracks Users’ Browsing Prompts Lawsuits

By TANZINA VEGA

Sandra Person Burns used to love browsing and shopping online. Until she realized she was being tracked by software on her computer that she thought she had erased.

Ms. Person Burns, 67, a retired health care executive who lives in Jackson, Miss., said she is wary of online shopping: “Instead of going to Amazon, I’m going to the local bookstore.”

Ms. Person Burns is one of a growing number of consumers who are taking legal action against companies that track computer users’ activity on the Internet. At issue is a little-known piece of computer code placed on hard drives by the Flash program from Adobe when users watch videos on popular Web sites like YouTube and Hulu.

The technology, so-called Flash cookies, is bringing an increasing number of federal lawsuits against media and technology companies and growing criticism from some privacy advocates who say the software may also allow the companies to create detailed profiles of consumers without their knowledge.

Unlike other so-called HTML cookies, which store Web site preferences and can be managed by changing privacy settings in a Web browser, Flash cookies are stored in a separate directory that many users are unaware of and may not know how to control.

Ms. Person Burns, a claimant who is to be represented by KamberLaw, said she knew cookies existed but did not know about Flash cookies.

“I thought that in all the instructions that I followed to purge my system of cookies, I thought I had done that, and I discovered I had not,” she said. “My information is now being bartered like a product without my knowledge or understanding.”

Since July, at least five class-action lawsuits filed in California have accused media companies like the Fox Entertainment Group and NBC Universal, and technology companies...
like Specific Media and Quantcast of surreptitiously using Flash cookies. More filings are expected as early as this week.

The suits contend that the companies collected information on the Web sites that users visited and from the videos they watched, even though the users had set their Web browser privacy settings to reject cookies that could track them.

“What these cases are about is the right of a computer user to dictate the terms by which their personal information is harvested and shared. This is all about user control,” said Scott A. Kamber, 44, a privacy and technology lawyer with KamberLaw who is involved with some of the cases. The suits have been filed by firms including Parisi & Havens and the law office of Joseph H. Malley.

One lawsuit contends that Clearspring Technologies and media companies including the Walt Disney Internet Group “knowingly authorized” the use of online tracking devices that would “allow access to and disclosure of Internet users’ online activities as well as personal information.” Others say that the information was gathered to sell to online advertisers.

In August, Clearspring and Quantcast issued statements on their company blogs addressing the suits. Clearspring clarified its use of Flash cookies and said the legal filings were “factually inaccurate.” The company said it used Flash cookies, also known as Flash local storage, “to deliver standard Web analytics to publishers.” The post also stated that data was collected at the aggregate level including unique users and interaction time, but did not include personally identifiable information.

Quantcast’s blog post said that the company “uses Flash cookies for measurement purposes only and not for any form of targeted content delivery.”

Specific Media did not respond to requests for comment. Counsel for the media companies in the cases declined to comment; representatives of companies that had not yet been served with the suits also declined to comment.

Some privacy advocates said that despite the companies’ claims, if enough data is collected over time, advertisers can create detailed profiles of users including personally identifiable data like race and age in addition to data about what Web sites a user visits. They also take issue with the fact that Flash cookies can be used to restore HTML cookies that have been deleted from a user’s computer, circumventing a user’s privacy settings.
“The core function of the cookie is to link what you do on Web site A to what you do on Web site B,” said Peter Eckersley, a technologist at the Electronic Frontier Foundation. “The Flash cookie makes it harder for people to stop that from happening.”

According to Adobe, more than 75 percent of online videos are delivered using Flash technology, with media companies also using it to serve games and animation to users. The company says that Flash cookies are intended to be used for basic Web functions like saving a user’s volume and language preferences or remembering where a user left off on a video game.

In a public letter to the Federal Trade Commission in January, Adobe condemned the practice of restoring cookies after they had been deleted by a user. The company provides an online tool on its Web site to erase Flash cookies and manage Flash player settings. At least one suit, however, claims that the controls are not easy to reach and are not obvious to most Web users.

Chris Jay Hoofnagle, 36, one of the authors of a University of California, Berkeley, study about Internet privacy and Flash cookies that has been used in several of the legal filings, said the recent spate of suits pointed to a weakness in federal rules governing online privacy.

“Consumer privacy actions have largely failed,” Mr. Hoofnagle said. The lawsuits, he added, “actually are moving the policy ball forward in the ways that activists are not.”

Complaints about online privacy are now migrating to mobile technology. Last week, a lawsuit was filed by three California residents against a technology company called Ringleader Digital saying that the company used a product called Media Stamp that “acquired information from plaintiff’s phone and assigned a unique ID to their mobile device.”

The suit says that the information collected by the unique ID, using a technology called HTML 5, allowed Web site operators “to track the mobile devices’ Internet activities over multiple Web sites.”

In a statement, Bob Walczak Jr., Ringleader’s chief executive, said, “Our intent since the inception of the company has been to build a mobile advertising platform that users can control.” He added that Ringleader was working on “new ways for consumers to be able to verify for themselves that their opt-outs have taken effect.”
John Verdi, senior counsel at the Electronic Privacy Information Center, faulted the Federal Trade Commission for not being more aggressive on privacy issues, focusing largely, instead, on self-regulation.

“The F.T.C. has been inactive on this front and has failed to present meaningful regulation on this,” he said. “There’s wide evidence that online tracking is not being controlled by self-regulation.”

Christopher Olsen, an assistant director in the division of privacy and identity protection at the agency, said it had hosted a series of roundtable discussions about online and offline privacy challenges from December to March and planned to issue a report in the next few months to address those issues.

The agency is investigating several companies, but Mr. Olson declined to comment on the specifics.

Other efforts to address online privacy are taking place at the Congressional level. In July, Representative Bobby L. Rush, Democrat of Illinois, introduced an online privacy bill that would, among other things, require companies to disclose how they collect, use and maintain the personal information on users and to make those disclosures easy for users to understand.