INSIGHT ON SOCIETY

EVERY MOVE YOU TAKE, EVERY CLICK YOU MAKE, WE'LL BE TRACKING YOU

Advertising-supported Web sites depend on knowing as much personal information as possible about you. One of the main ways ad firms discover your personal information is by placing so-called "tracking files" on your computer's browser. There are several kinds of third-party tracking files on Web pages. Cookies are the best known. These simple text files are placed in your browser and assign a unique number to your computer, which is then used by advertisers to track you across the Web as you move from one site to another (without telling you). Web beacons (sometimes also referred to as Web bugs) are a little more pernicious. Beacons are small software files that track your clicks, choices, and purchases, and even location data from mobile devices, and then send that information, often in real time, to advertisers tracking you. Beacons can also assign your computer a unique number and track you across the Web. A Flash cookie is a third kind of tracking file. Installed by Adobe Flash as you watch movies, these files can be used to install regular cookies on your computer and even restore cookies you have deleted. Recently, the use of Flash cookies has declined, replaced in part by Web sites using HTML5 local storage, which can be used for tracking the same way as Flash and regular cookies. Tracking can also be performed by apps on cell phones as well as Facebook. Most Facebook apps, for instance, all send personal information, including names, to dozens of advertising and Internet tracking companies.

So how common is Web tracking? In a trailblazing series of articles in the *Wall Street Journal*, researchers examined the tracking files on 50 of the most popular U.S Web sites. What they found revealed a very widespread surveillance system. Only one site, Wikipedia, had no tracking files. Two-thirds of the tracking files came from companies whose primary business is identifying and tracking Internet users to create consumer profiles that can be sold to advertising firms looking for specific types of customers. The other third came from database firms that gather and bundle the information and then sell it to marketers. Many of the tracking tools gather incredibly personal information such as age, gender, race, income, marital status, health concerns, TV shows and movies viewed, magazines and newspapers read, and books purchased. While tracking firms claim the information they gather is anonymous, this is true in name only. Scholars have shown that with just a few pieces of information, such as age, gender, zip code, and marital status, specific individuals can be easily identified. In October 2012, a Web Privacy Census conducted by the University of California Berkeley Center for Law and Technology found that the total number of cookies on the top 100 Web sites had increased by 80%, from 3,600 when first measured in 2009 to over 6,400. The vast majority of these cookies (about 85%) were third-party tracking cookies, from over 450 different third-party hosts. Google's DoubleClick was the top tracker, and the most frequently appearing cookie keys were those associated with Google Analytics. Similar results were observed when looking at the top 1,000 and top 25,000 Web sites. One cause: growth of online ad auctions where advertisers buy data about users' Web browsing behavior. When you visit a site, your visit is auctioned and the winner gets to show you some ads. All this takes place in a few milliseconds so you don't know its happening. Welcome to the brave new world of Internet marketing!

The Privacy Foundation has issued guidelines for Web beacon usage. The guidelines suggest that

(continued)

Web beacons should be visible as an icon on the screen, the icon should be labeled to indicate its function, and it should identify the name of the company that placed the Web beacon on the page. In addition, if a user clicks on the Web beacon, it should display a disclosure statement indicating what data is being collected, how the data is used after it is collected, what companies receive the data, what other data the Web beacon is combined with, and whether or not a cookie is associated with the Web beacon. Users should be able to opt out of any data collection done by the Web beacon, and the Web beacon should not be used to collect information from Web pages of a sensitive nature, such as medical, financial, job-related, or sexual matters. None of these ideas are found in current law.

In an effort to address growing congressional concerns about privacy, and build consumer trust online, an industry advertising group, the Network Advertising Initiative (NAI), released self-regulatory guidelines for the industry. Major advertising industry groups have adopted guidelines that emphasize transparency (tell consumers how you use their information) and choice (opt-in and opt-out). The NAI requires online firms to notify customers of Web beacon usage, state the purpose of their use, and disclose any data that could be released to third parties. The NAI also called for users to be given a choice (whether opt-in or opt-out) of any release of personally identifiable information (PII) to third parties, and to provide an opt-in choice for any release of information related to PII. In addition, the NAI provides a capability open to all Web users to opt out of online advertising networks collecting nonpersonal information on them. However, for this to work, users need to have a cookie downloaded to their browser that will inform the networks not to collect information on this user.

Currently, there are no laws or regulations in the United States that prevent firms from installing tracking files or using that information in any way they please. Although there has been considerable interest in protecting the privacy of consumers, thus far efforts to enact federal Do Not Track legislation have failed.

One roadblock involves the meaning of Do Not Track. Industry wants an opt-in, default Track Me feature on all Web sites, while the government and privacy groups are pushing for an opt-out Do Not Track feature in which the default is Do Not Track. In July 2013, a working group commissioned by the W3C proposed that Web users should be able to tell advertising networks not to show them targeted advertisements. Still unresolved, however, is whether those networks and data brokers should be allowed to collect the data in the first place.

Nearly all browsers now offer users the option of using a Do Not Track feature. But users have to remember to turn it on. A March 2013 survey by Forrester Research found that less than 20% of users used the Do Not Track setting on their browsers. In addition, not all Web sites honor the Do Not Track request, since they are not legally obligated to do so. Major Web sites and the online advertising industry insist their industry can self-regulate itself and preserve individual privacy. However, this solution has not worked in the past.

SOURCES: " 'Do Not Track' Rules Come a Step Closer to an Agreement," by Somini Sengupta and Natasha Singer, *New York Times*, July 15, 2013; "What Firefox's New Privacy Settings Mean for You," by Sarah A. Downey, Abine.com, March 29, 2013; "The Web Privacy Census," by Chris Jay Hoofnagle and Nathan Good, law.berkeley.edu/privacycensus.htm, October 2012; "Online Data Collection Explodes Year Over Year in US," eMarketer, Inc., July 19, 2012; "Online Tracking Ramps Up," by Julia Angwin, *Wall Street Journal*, June 17, 2012; "Microsoft's "Do Not Track" Move Angers Advertising Industry," by Julia Angwin, *Wall Street Journal*, May 31, 2012; "Opt-Out Provision Would Halt Some, but Not All, Web Tracking," by Tanzina Vega, *New York Times*, February 28, 2012; "How Companies Learn Your Secrets," by Charles Duhigg, *New York Times Magazine*, February 16, 2012; "Latest in Web Tracking: Stealthy 'Supercookies,'" by Julia Angwin, *Wall Street Journal,* August 18, 2011; "WPP Ad Unit Has Your Profile," by Emily Steel, *Wall Street Journal,* June 27, 2011; "Not Me Dot Com," by Luke O'Neil, *Wall Street Journal,* June 18, 2011; "Show Us the Data. (It's Ours, After All)," by Richard Thaler, *New York Times,* April 23, 2011; "What They Know About You," by Jennfier Valentino-Devries, *Wall Street Journal,* July 31, 2010; "Sites Feed Personal Details to New Tracking Industry," Julia Angwin and Tom McGinty, *Wall Street Journal,* July 30, 2010; "Study Finds Behaviorally-Targeted Ads More Than Twice As Valuable, Twice as Effective As Non-targeted Online Ads," Network Advertising Initiative, March 24, 2010.