Monitor

Anonymous no more

The internet: It is becoming ever more difficult to browse the internet without leaving behind digital footprints that reveal your identity

Mar 10th 2011 | from the print edition

WAY back in the early days of the web, in 1993, the *New Yorker* ran a cartoon featuring two dogs sitting in front of a computer. The internet-savvy canine is saying to its friend: "On the internet, nobody knows you're a dog." This joke captured the freewheeling anonymity of the early stages of internet adoption, but it doesn't work now. Today websites often know a great deal about their visitors, including their names and interests.

The ability to use the internet anonymously is being eroded on several fronts. Some popular websites, including Facebook, the leading social network, and Quora, a popular question-and-answer site, require users to give their real names, and block people who are suspected of using pseudonyms. Other sites ask that users provide their real names in order to be able to leave comments, in the hope that discussions will be more civil if people have to reveal their identities.

In recent months security researchers have shown that if you use your real identity on some sites, you can be identified when you visit others. One way this can happen involves "cookies", the snippets of data that websites deposit on visitors' computers, so that returning visitors can be recognised. It sounds creepy, but cookies are generally anonymised. Cookies can reveal things about your browsing habits—they are used to target advertising, for example, based on other sites you have visited—but they do not usually know who you are.

In 2010, however, privacy experts twice pointed out that Facebook was sending information about its users to the same advertisers that track browsing using cookies. It is not known what, if anything, the advertisers did with this information. The potential, however, is clear: the Facebook data could have been used to deanonymise the browsing histories associated with the cookies. Facebook plugged this leak of personal information, but only after the problem was given prominent coverage in the *Wall Street Journal*. When the leak was highlighted by computer scientists in August 2009, nine months earlier, Facebook took no action.

Another anonymity-eroding technique was recently flagged by computer scientists. It relies on "history stealing", in which a security flaw in a user's web browser allows rogue websites to

retrieve fragments of his browsing history. This may not directly reveal his identity, but can be very revealing. For example, if a user has joined three groups on a social network, there is a limited overlap between the groups' membership lists, and those lists are public, it may simply be a matter of working out who belongs to all three groups.

This sounds rather contrived, but it works in practice. Gilbert Wondracek at the Vienna University of Technology in Austria and his colleagues built a history-stealing website aimed at groups on Xing, a business-orientated social network. Mr Wondracek's analysis of over 6,500 Xing groups, containing a total of more than 1.8m users, suggested that his rogue site would be able to determine the identity of around four in ten visitors. A trial run, in which Mr Wondracek invited colleagues who use Xing to visit his history-stealing site, showed this estimate to be about right. The vulnerability he exploited has since been addressed by the engineers behind several browsers, including Firefox and Safari, but has so far not been fixed in Microsoft's Internet Explorer.

Meanwhile, Facebook has quietly gained the ability to monitor its users' wanderings elsewhere on the web. Many sites now include Facebook "Like" buttons. Click one, and your Facebook profile will be updated with a message linking to the page in question. This feature helps people share content with friends, but it also allows Facebook to track its users' browsing. In fact, merely going to a page containing a "Like" button while logged into Facebook is enough to notify the social network of your visit, whether or not you click the button.

Where is all this heading? It is clear that many firms can now track people as they move around the web, and can sometimes link these browsing histories to specific individuals and their personal information. If the days of anonymous browsing are not over yet, some observers think they soon will be. As Julie Cohen, a legal scholar at Georgetown University, put it in a prescient paper published 15 years ago, the internet era is "as much an age of information about readers as it is an age of information for readers". Speaking at the Techonomy conference last year, Eric Schmidt of Google distinguished between privacy, which he said should be respected, and anonymity. "Absolute anonymity could lead to some very difficult decisions for our governments and our society as a whole," he said.

But anonymity is freeing. It lets people go online and read about fringe political viewpoints, look up words they are embarrassed not to know the meaning of, or search for a new job without being thought extremist, stupid or disloyal. In America some judges have recognised that browsing habits will change if people feel that they are being watched. In rejecting a government demand for book-purchase data from Amazon, an online retailer, a judge wrote that the release of the information would create a chilling effect that would "frost keyboards across America". Librarians have long understood this, which is why they keep readers' files confidential. But many of the new custodians of people's reading records do not seem inclined to do the same.

from the print edition | Technology Quarterly