Internet privacy tools are confusing, ineffective for most people: report

October 31 2011

Internet users who want to protect their privacy by stopping advertisers and other companies from tracking their online behavior will have great difficulty doing so with commonly available "opt-out" tools, researchers at Carnegie Mellon University report.

User testing found that privacy options in popular browsers, as well as online tools or plug-ins for blocking access by certain websites or otherwise opting out of tracking, were hard for the typical user to understand or to configure successfully.

"All nine of the tools we tested have serious usability flaws," said Lorrie Cranor, director of the CyLab Usable Privacy and Security Laboratory (CUPS). "We found that most people were confused by the instructions and had trouble installing or configuring the tools correctly," Cranor said. "Often, the settings they chose failed to protect their privacy as much as they expected, or to do anything at all."

The CUPS technical report, "Why Johnny Can't Opt Out," is available online at http://www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html.

The growth of online behavioral advertising (OBA), which targets individuals with advertising based on their online activity, has caused some privacy advocates to press for regulations limiting the information companies can gather, or providing a dependable Do-Not-Track

mechanism. For now, individuals concerned about their privacy must take steps on their own.

To assess the ability of non-technical individuals to protect themselves, the Carnegie Mellon researchers evaluated the privacy settings on two popular browsers, Mozilla Firefox 5 and Internet Explorer 9. They also tested three tools that set opt-out cookies that are supposed to prevent particular advertising networks from displaying ads to users: DAA Consumer Choice, Evidon Global Opt-Out and PrivacyMark. And they tested four tools that are supposed to block certain sites from tracking the user at all: Ghostery 2.5.3, TACO 4.0, Adblock Plus 1.3.9 and IE9 Tracking Protection.

The researchers recruited 45 people without technical training who use the Internet frequently. Each person was interviewed and assigned tools to test based on their browser and operating system preferences.

The major findings:

- Users can't distinguish between trackers. Users are unfamiliar with companies that track their behavior, so tools such as Ghostery and TACO that ask them to set opt-out or blocking preferences on a per-company basis are ineffective. Most users just set the same preferences for every company on a list.
- Inappropriate defaults. One might assume that a user who downloads a privacy tool or visits an opt-out site intends to block tracking. But the default settings of these tools generally do not block tracking.
- Communication problems. Information tends to be presented at levels that are either too simplistic to inform a user's decision, or too technical to be understood.
- Need for feedback. Ghostery and TACO users received

notifications on every website visited about what companies were attempting to track them and whether the trackers had been blocked. But most other tools provided little, if any, feedback, so users couldn't tell whether the opt-out was working or even what it meant to be opted out.

- Users want protections that don't break things. Users weren't sure when the tools had caused parts of a website to stop working. Subscribing to a Tracking Protection List (TPL) that blocks most trackers except those necessary for sites to function can solve this problem. But participants were unaware of the need to select a TPL or didn't know how to choose one.
- Unusable interfaces. Most tools suffered from major usability flaws. Several participants opted out of only one company on the DAA website, despite intending to opt out of all of them. Users did not understand AdBlock Plus' filtering rules. And none of the participants who tested IE Tracking Protection realized they needed to subscribe to TPLs until prompted later in the task.

"The status quo clearly is insufficient to empower people to protect their privacy from OBA companies," Cranor said. "A lot of effort is being put into creating these tools to help consumers, but it will all be wasted — and people will be left vulnerable — unless a greater emphasis is placed on usability."

In addition to Cranor, an associate professor of computer science and engineering and public policy, the authors include CyLab research scientist Yang Wang and Ph.D. students Pedro G. Leon, Blase Ur, Rebecca Balebako and Richard Shay. This research was supported by The Privacy Projects and the National Science Foundation.

Provided by Carnegie Mellon University