Online tracking more common than most realize, new study finds

November 10 2015

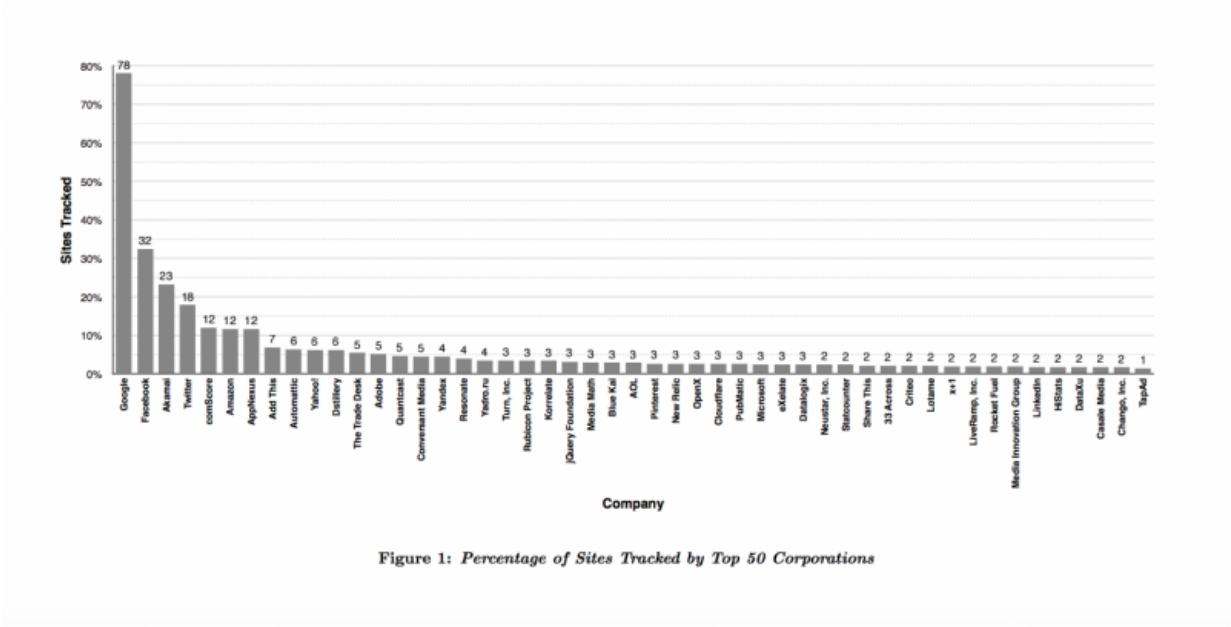

Figure 1: *Percentage of Sites Tracked by Top 50 Corporations*

These 50 corporations were monitoring the greatest percentage of third party data from the Alexa top one million sites studied. Credit: Courtesy of Tim Libert

Think of how often sit with your phone, tablet, or computer, quietly shopping or reading the latest headlines. Browsing the internet certainly feels like a solitary activity, but as a new study in the *International Journal of Communication* reveals, you may be surprised by just how many companies are observing.

Tim Libert, a doctoral student at the Annenberg School for Communication at the University of Pennsylvania analyzed the Alexa top one million websites, finding that 88 percent leak user data to third parties—sites that would be unfamiliar to most users.

"There's some suggestion that it's anonymous data," says Libert, "but when you have big data sets that can be combined with other big data sets, you can be identified pretty easily."

Sites that leak user data contact an average of nine external domains, indicating that the activity of a single person visiting a single site may be tracked my multiple entities.

By tracing the unintended disclosure of personal browsing histories on the web, Libert discovered that a handful of U.S. companies receive the vast bulk of user data worldwide, led by Google, which tracked users on nearly 80% of the websites studied. Other top followers on the sites studied include Facebook (32%), Twitter (18%), ComScore (12%), Amazon (12%), and AppNexus (12%).

While this monitoring of your behavior doesn't signal nefarious activity or a security breach, it does increase the risk of one taking place. "If your data is being sent to several companies," says Libert, "that creates new potential points of failure where your data could be hacked or leaked."

Using the contents of NSA documents leaked by Edward Snowden, Libert also determined that roughly 20% of websites are potentially vulnerable to known National Security Agency spying techniques. And by a number of large companies aggregating user data from countless smaller sites, this also makes it easier for government agencies to gather data.

This information may be used to serve you more relevant advertising or to deliver content more quickly, but the ways in which your data is used is not always transparent. And efforts to opt out of that data collection can prove frustrating.

Ostensibly there should be a solution: the browser's "Do Not Track" (DNT) setting. However Libert's study found that with the notable exception of Twitter, DNT requests are totally ignored.

"It's up to regulators to work with companies to comply, because they're not doing it on their own," says Libert. "The infrastructure to respect people's privacy preferences exists, and it works. But unless there are real financial consequences for corporations, they're just going to ignore DNT. Self-regulation to date has been a big failure."

Provided by University of Pennsylvania

Citation: Online tracking more common than most realize, new study finds (2015, November 10) retrieved 24 April 2024 from https://phys.org/news/2015-11-online-tracking-common.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.