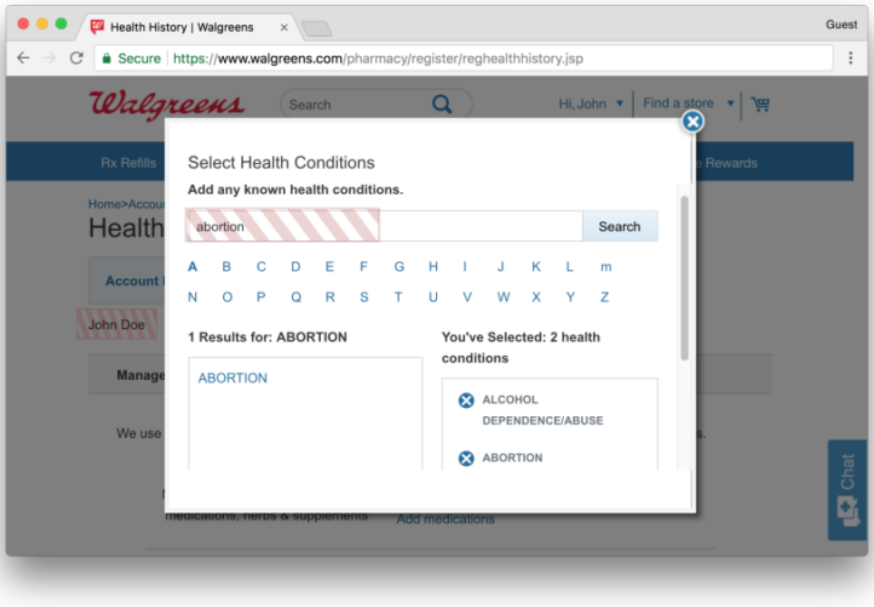
ALL SEEING EYE —

No, you're not being paranoid. Sites really *are* watching your every move

Sites log your keystrokes and mouse movements in real time, before you click submit.

DAN GOODIN - 11/20/2017, 1:38 PM



Steven Englehardt

Enlarge

199

If you have the uncomfortable sense someone is looking over your shoulder as you surf the Web, you're not being paranoid. A new study finds hundreds of sites—including microsoft.com, adobe.com, and godaddy.com—employ scripts that record visitors' keystrokes, mouse movements, and scrolling behavior in real time, even before the input is submitted or is later deleted.

Session replay scripts are provided by third-party analytics services that are designed to help site operators better understand how visitors interact with their Web properties and identify specific pages that are confusing or broken. As their name implies, the scripts allow the operators to re-enact individual browsing sessions. Each click, input, and scroll can be recorded and later played back.

A study published last week reported that 482 of the 50,000 most trafficked websites employ such scripts, usually with no clear disclosure. It's not always easy to detect sites that employ such scripts. The actual number is

almost certainly much higher, particularly among sites outside the top 50,000 that were studied.

"Collection of page content by third-party replay scripts may cause sensitive information, such as medical conditions, credit card details, and other personal information displayed on a page, to leak to the third-party as part of the recording," Steven Englehardt, a PhD candidate at Princeton University, wrote. "This may expose users to identity theft, online scams, and other unwanted behavior. The same is true for the collection of user inputs during checkout and registration processes."

Englehardt installed replay scripts from six of the most widely used services and found they all exposed visitors' private moments to varying degrees. During the process of creating an account, for instance, the scripts logged at least partial input typed into various fields. Scripts from FullStory, Hotjar, Yandex, and Smartlook were the most intrusive because, by default, they recorded all input typed into fields for names, e-mail addresses, phone numbers, addresses, Social Security numbers, and dates of birth.

The following video captured data as it was transmitted in real time to FullStory:

User replay fullstory demo.

Even when services took steps to mask some of the data, they often did so in ways that continued to jeopardize visitor privacy. Smartlook and UserReplay, for instance, collected the number of characters typed into password fields. UserReplay also logged the last four digits of visitors' credit card numbers.

Englehardt said the services provide manual and automatic tools website operators can use to redact information that is collected on their properties. But the tools in many cases require large amounts of developer time and skill. And even then, sites with strong legal incentives not to leak sensitive data were found doing just that. Walgreens.com, for instance, sent medical conditions and prescriptions alongside user names to FullStory despite the extensive use of manual redactions on the pharmacy site.

Another example: the account page for clothing store Bonobos leaked full credit card details—character by character as they were typed—to FullStory. Adding insult to injury, Yandex, Hotjar, and Smartlook all offer dashboards that use unencrypted HTTP when subscribing publishers replay visitor sessions, even when the original sessions were protected by HTTPS.

Representatives for both Walgreens and Bonobos have said the sites have stopped sharing information with FullStory, according to reports from Motherboard and *Wired*.

It's not clear what meaningful recourses Internet users have for preventing the data collection. The researcher said that ad-blockers can filter out some, but not all, of the replay scripts. Checking the "do not track" option built into some browsers also failed to stop the logging. That means every keystroke typed into a Web field may be logged, character by character, even if the visitor later deletes the field and never presses a submit button.

Until more robust protections are available, people should remember that just about anything they do while visiting a website can be logged.

DAN GOODIN
Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

READER COMMENTS 199 SHARE THIS STORY

← PREVIOUS STORY NEXT STORY →

Related Stories

British water utilities admit they use divining rods to find leaks

DOJ names Iranian as hacker that stole unaired episodes from HBO

Drugs that switch your brain into squirrel-mode may save you from a stroke

FCC will also order states to scrap plans for their own net neutrality laws

Today on Ars

British water utilities admit they use divining rods to find leaks

DOJ names Iranian as hacker who stole unaired episodes from HBO

Drugs that switch your brain into squirrel-mode may save you from a stroke

FCC will *also* order states to scrap plans for their own net neutrality laws

Chinese students claim they worked illegal overtime making the iPhone X

Dealmaster: Get a PlayStation 4 for $200 and other early Black Friday deals

With today's launch of the OnePlus 5T, the OnePlus 5 is dead

Colorado fines Uber $8.9M for allowing dozens of unauthorized drivers

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US
CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS