Science Translations
Established 1990
PC410.COM™
PC Updater News

Digital Trails: Big Brother is Watching

You’re leaving digital breadcrumbs all over the place. It’s not that you’re messy; it’s that the software you use was designed by people who make money from your online activities. Mostly, that’s because when you browse a web page, you’re running scripts that do useful things like:

- If browsing on a small screen, show a single-column layout.
- If on a slow device, use smaller images.
- If browsing from the USA, show page in US English.
- If a repeat visitor, don’t re-download images.
- If it’s during business hours, show business ads.
- If in Towson, show an ad for a business in Towson.
- If a repeat visitor, show ads like the last items viewed.
- If user previously visited any site we share ads with, show product matching last visit elsewhere.
- If likely a member of political party ‘a’ show matching propaganda. (and so on....)

That list went from useful to potentially creepy pretty quick, but it's all the same technology. These things all work the same way. The web server asks your browser about the screen size you're using, the language, the country, and in many cases the location down to the zip code level, and much more. The tracking expands from that, plus the ability to see if you're visited the page before, using small text files known as cookies, just more breadcrumbs. And if cookies aren't available, there are a few dozen alternate ways to track you. The official word for that in the industry is 'signals' and you may hear it from vice presidents of large social media companies when they're testifying before Congress.

The tracking is the worst on social networking sites like Facebook and Twitter and hundreds of smaller sites, where you are offered ads and 'promoted content' based on any other page you've clicked. Business content is not immune; Microsoft bought LinkedIn, and the tracking continues. On the social sites, you are in a closed system to some extent, so if you don't like what they're showing you, there are options on the 'promoted content' to 'do not show me items like this' and there are some privacy settings in the account information that will reduce the tracking, but will never completely turn it off, because on a free web site, you are the product, not the customer, and you exist to provide ad viewer counts, and nothing else matters. Facebook's income is 2021 was around $117 billion, and you didn't pay for Facebook. The advertisers paid for that.

What are the results of all this tracking? Well, for years, Target has had a very odd knack of knowing when a customer is pregnant, and sending them maternity advertisements. They're apparently picking up that fact before family members and sometimes before the customer herself. Fast-forward to current times, where some no-abortion states want to know exactly that, and it suddenly is vitally important to keep private issues as private.

And the trackers are also looking for spear phishing targets, looking for email addresses and identifying business types so that they can send targeted (the 'spear') emails as bait for you to click on (the 'phish').

Target is not alone:
How it Feels When Bed Bath & Beyond Thinks You're Pregnant
https://gizmodo.com/bed-bath-beyond-buy-buy-baby-pregnancy-data-1849356818

And it's big business now:
These Companies Know When You're Pregnant—And They're Not Keeping It Secret
https://gizmodo.com/data-brokers-selling-pregnancy-roe-v-wade-abortion-1849148426

Much of what is being discussed as new just isn't new. The existing laws, and the regulations surrounding HIPAA, already provide partial protection from such things. But that's theoretical enforcement where new technology is always decades ahead of legal restraints. The data brokers generallcan't be physically traced, so what remains is preventing app companies, internet providers, and malware artists from mining your data to sell it.

What To Do About It

It's difficult to allow web developers to get the information needed to show a web page nicely on any size screen (called 'responsive' design), while at the same time completely blocking that same technology from showing you ads based on where you've surfed, what you've bought, and what your politics are, or your biology might be.

And the web browsers you use, especially Microsoft Edge and Google Chrome, are part of the system that makes you the product on the internet. Google Chrome, of course, is the free browser provided by the top digital advertising company on the planet, Alphabet. And Microsoft Edge is based on Google source code, called 'Chromium,' and comes from Microsoft, who's no slouch in advertising. In the first quarter of 2022, Google reported ad revenue of $68 billion. Microsoft reported $49 billion for search and news advertising. It is not in the best interests of these companies to provide software that blocks targeted advertising, because they make their money directing 'relevant' advertising to you.

Blocking the Invasion

There are two ways to block the tracking and collection gathering. The traditional advice of 'turn off third-party cookies in the browser' is not remotely adequate. What that does is not allow files created on one web site, containing things like the contents of a shopping cart or your email address, to be read by any other site. But again, the advertising networks that are tracking you don't rely on just cookies, so it takes software running to block the many, many background attempts to identify you and yours. That software can be either running a browser plugin that identifies and reduces tracking, or a browser designed to do that, and not one created by an advertising firm (Google and Microsoft, in particular).

There are a lot of ad-blocking plugins. The best-known and reliable ones are Ghostery (paid and free versions) and Adblock Plus (free). The paid version of Malwarebytes includes a browser extension that blocks trackers. Many other products also block trackers, but don't stack these products; use only one at a time.

The browsers have been ranked by how well they block tracking. Microsoft Edge is the worst, and then there's Chrome. Firefox is a little better, and that's almost certainly because they're not run by an advertising company. https://arstechnica.com/information-technology/2020/03/study-ranks-edges-default-privacy-settings-the-lowest-of-all-major-browsers/

The standout in that article is the Brave browser, which is designed specifically to block trackers, and starts out with default settings that block far more than other browsers. It's a good product, and there are plenty of good reasons to use it as your main browser.

Brave, by default, uses DuckDuckGo.com for searches, which is a web search engine that doesn't track users. DuckDuckGo can also set as your default search engine in any other browser. DuckDuckGo has their own browser in the Android Play Store and in the Apple App Store:

Google Play:
https://play.google.com/store/apps/details?id=com.duckduckgo.mobile.android&gl=US

Apple App Store:
https://apps.apple.com/us/app/duckduckgo-privacy-browser/id663592361

At this time, the best option for private browsing in Windows is Brave. DuckDuckGo is working on a Windows browser as well. I will announce it here once it's available.

Reminder: You can switch browsers all day long. And some web pages just don't work with every browser, or break after an update. So you need more than one. There are dozens, not just those I've mentioned. At the moment, Brave is very good. Firefox is OK. Chrome is what I'll use if a web site won't load properly on another browser. I try to avoid Edge. In all of them, always, look at the security and privacy settings. If in doubt as to what they mean, change only one at a time, or call me for help. Or just use Brave to surf and the DuckDuckGo web site to search. Remember, Big Brother is watching, and unlike in the book 1984, it's not just our governments who are paying attention.

For computer help, call 410-871-2877
Missed a newsletter? Back Issues

Mailing address:
Science Translations
PO Box 1735
Westminster, MD 21158-5735