Primer

Heligan
Strategic Insights

Do you know who's following your Digital Exhaust?

The nature of identity is changing. As our digital lives expand so do our digital indicators. These indicators are trackable and increasingly being used as a proxy to identify individuals.

How much do you think about the digital footprints you leave behind as you wander through the shops, buy goods online, browse the internet and generally go about your everyday lives?

If, like us, the answer is 'not much', then you are not alone…but there are some things you might want to be aware of, or at least to consider.

Most of you will have heard of cookies; the little bits of code attached to nearly all online activity that act like a breadcrumb trail allowing advertisers and data gathers to track your activity, collate your habits and preferences and then sell that information or use it to sell things to you more effectively. Collectively, this information is referred to as a 'Digital Exhaust' and you would be staggered at how much your exhaust is worth online!

However, cookies are but one (really obvious) way to track you. In fact, many companies are actually reducing reliance on them in favour of other methods to suck up your user data and movements whilst on their sites.

Browser fingerprinting

Wired recently ran an article on browser fingerprinting – this takes information about your browser, your network, your device and combines it together to create a set of characteristics that is mostly unique to you – your online fingerprint. The data that makes up your fingerprint can include the language you use, keyboard layout, your time-zone, whether you have cookies turned on, the version of the operating system your device runs on, and much more. Creating massive databases of profiles has gotten easier in recent years because of advances in artificial intelligence technology that allow for better cross-referencing and correcting of data. By fusing all this information, it's possible for advertisers (and adversaries) to recognise you as you move around the web…and a study from the Electronic Freedom Foundation found that they can be as accurate as 80%-90% in some cases.

Unlike cookies, it's hard to stop fingerprinting. Cookies are stored in your browser, and it's possible to delete your cookie history, block them, or turn them off entirely. With fingerprinting, it's all invisible.

So, what can you do to stop it…well the answer is not much! The biggest thing you can do to stop or disrupt folks following your digital exhaust is to use a browser that limits tracking and increases privacy such as FireFox, Brave, Safari and Tor. Search Engines like DuckDuckGo (a search engine that doesn't track your searches) have also branched out to develop a user browser.

It's important to remember this isn't life and death…it's just a bit of your privacy that you may be happy to trade for a big chunk of convenience…at the end of the day you just need to make an informed decision about who has access to some of that stuff you might consider private.