Are you unique

Karnav Popat

You know how data privacy is so important these days? You have all that uproar over Facebook and Google and Cambridge Analytica and Zynga, and you have people using VPNs and IP spoofers and the bells and whistles. Turns out, none of that stuff works and everyone, not just the big companies but everyone who’s interested, can know exactly what you (specifically you, singled out from the billions of devices) are doing at any given moment. Fun, right?

Browser fingerprinting turned up as a tracking method sometime in the early 2010s. It started out, as so many of these things do, as a research project, where Californian data scientists tried to use canvas fingerprinting to identify and block botnets. By 2014 however, a shady company named AddThis had quietly added fingerprinting to their customer tracking features and was leveraging it to create customer profiles on the individual level.

The way browser fingerprinting works is quite similar to how regular fingerprinting works: the patterns of data and metadata that our browser sends out are so large that the probability of them being unique, even among the billions of browses out there, is incredibly high. You can try it out for yourself at amiunique.org, or uniquemachine.org; if, like me, it turns out that you’re unique, there’s probably already a profile of your shopping preferences on some Chinese sweatshop bot’s marketing list.

The prospect of someone being able to monitor you on the internet is quite naturally, terrifying. The net gives us a sense of security in anonymity, a feeling that we’re going to go unnoticed among the masses. Being stripped away of that comfort and realizing that Amazon probably knows your real feelings about Taylor Swift can be severely unnerving.

In situations like that, there’s two kinds of people: first, there’s the paranoid r/conspiracy lurkers. A friend of mine, for example, when confronted with the fact that his incognito-mode activities probably aren’t hidden, decided that throwing 5000 bucks a month on the first fingerprint spoofer he’d ever heard of, without confirmation or even knowing if it worked, was a good idea. That same friend had previously been under the impression that VPNs, incognito mode (hahaha) and adblockers formed a viable privacy screen. The fact that a tool as powerful and as 1984-esque is virtually unknown, is as unnerving as the tool itself.

The second kind of person are those who simply don’t care. You see, in early 2001, Microsoft got sued for antitrust violations when they packaged Internet Explorer with the dominant Windows. Ah, the good ol’ days, when monopolies were dangerous and privacy still existed. Today, Google does literally the exact same thing by packaging Chrome with all sorts of devices, and still manages to get away with it. The only thing that’s changed in these 20 years is that we’ve happily traded our safety and privacy for convenience. To paraphrase another friend on the same topic (realize where I got the idea for this article yet?), we know that Google is spying on us, but just their brand name is enough to let us accept it anyway.

Here’s a little thought experiment to help you understand why browser fingerprinting is the new drone surveillance: Run down a list of the sites you remember having gone on in the last week. Instagram, Facebook, Google, and the usual suspects, yes, but also probably convertio.co and duplichecker and all sorts of sites that you wouldn’t trust with your credit card. What happens when every visit to all those sites gets cobbled together and neatly filed under your name, accounts and address? What happens is targeted advertisement on steroids. That’s when you enter the world of psychoanalysis from LinkedIn profiles, probably a little thoughtpolice on the side, too.

Fortunately, the answer lies, as always, with the extremely generous open-source community. Fingerprinting blockers are becoming increasingly available, either as paid applications, or as integrated plugins on open source browsers (such as Tor, itself the last bastion of free speech that reddit is perceived as). Without that sort of privacy software, for all you know, Chinese gestapo are looking through your webcam this very moment. But hey, that auto-login feature is sweet, huh?