How to reduce your digital spoor

by Andy Pepperdine

Introduction

Awareness of the way that many corporations are tracking us is becoming more and more widespread among the pundits, media and the general public. This paper is intended to give some hints as to how you can protect yourself, and what the future dangers might be.

Of particular notice is reference [1], which, although I have not read it (yet), I have seen an excerpt that makes it look worthwhile investigating for anyone who is concerned about these things. For example she considers the development of China's "Social Credit" score that it wants to introduce to include everyone in the country, by putting numbers on whatever you want to do and whether your political statements accord with the official lines. The better you score, the easier it will be to obtain jobs, loans and other things. This looks like exactly the sort thing that any tyrant would like to emulate, and so many people have already given so much to Facebook and the like, those scores could easily be created now.

First, I will indicate some of the tricks used to collect the data, and then perhaps how you can reduce their effect. It is now impossible to remain totally hidden, although you can make it difficult for them to associate actions wit a particular individual.

Tracking

Tracking is the name given to what companies do to collect data about you, individually. They rely on the ability to set cookies from social media and other sites which are linked as a third party to the pages you are actually looking at. These third parties then collect, collate and sell on any data they obtain to mostly advertisers, who then tailor what they can send to you. But there is every reason for them to sell to anyone who wants to buy, such as political organisations, credit agencies, insurers, etc.

The website at https://trackography.org/ [2] has information about the trackers on various media sites, like broadcasters, newspapers and other news sources you may frequent. Since this information is valuable, and journalism is struggling to make a profit, then selling access to your reading habits is something they can use to help their bottom line.

In the same way, government services could in theory use the same data brokers to obtain information about you.

Cookies

The principal and traditional method of keeping tabs on you is through cookies. If these persist from one session to the next, then you are leaving a history that is easy to follow, and also will enable correlations to be made across all the sites you visit. Even if they do not know your name and other details, they can get enough over time to aim advertisements spookily accurately.

Unfortunately, cookies are a necessary part of staying logged in to sites you are browsing – there really is no other way of doing it technically. One thing you can do is delete your history and cookies whenever you close your browser.

Another simple thing is always to explicitly log out after you have visited somewhere. That way the trackers cannot see your actions on that site, although they will know what handle you use on those other sites unless you clear the cookies as well.

Private browsing

If you are concerned about spilling data across the net, it is worth considering using Private Browsing mode. This is a way of compartmentalising your browsing so that you do only certain things from certain browser configurations. If you do that, then all the trackers will see is what you are doing in that window, and not any of the previous history in the session. It is a way of restricting the leakage, although not completely preventing it.

To start Private Browsing on Firefox, use File → New Private Window, or use the Menu → New Private Window, or from the keyboard Ctl+Shift+P.

In Chrome/Chromium, use Menu → New Incognito Window.

Browser Fingerprinting

Fingerprinting is the name of a technique used to try to identify and track you by examining the attributes of the browser you are using. So if those attributes are unique, then they will know that is always you when you use that browser.

If you want to determine what characteristics your browser has you can use the EFF tool Panopticlick [3] here: https://panopticlick.eff.org/ which will tell you just how unique it is. Mine always seem to turn out to be unique.

Different browsers will give different results. However, note that the EFF site can only report on how unique it is according to people who have actually used them to do the test. In practice, real trackers will have seen many more browsers than EFF have, and EFF will be biased towards the more technical aware and savvy.

It is very hard to prevent this type of identification as it does not depend on any type of cookie, and will give the same results whenever you use that browser on that machine.

Canvas hash

One of the things it tests is known as a canvas hash. This is relatively new technique, whereby a site can render some special text in a hidden part of the display, and then read it back to see the exact sequence of pixels it contained. This will identify not only the way the browser renders the text, but also the way the hardware and it’s drivers do so. Because this can identify more precisely than some other features, work is going on in browsers to see whether they can prevent the read back, but I do not know the present status of that work.

Secure sites

Apart from the commonly mentioned protection and selection of good passwords to sites, it is worth considering using an add-on to Firefox or Chrome that will ensure that the connection is via a

secure link wherever possible. This add-on is another EFF tool called HTTPS everywhere [4], and is available

A more extreme add-on is HTTPS by default [5].

Suppressing scripts

Scripts are things that interpret what you are doing on a form or page, and will adapt the page to what you are doing. For example, adjusting what you see according to what you select. This gives a tracker the ability to collect the data they want.

Some browsers have builtin features to mitigate this problem, and other use add-ons. Unfortunately the latest version of Firefox does not support the popular NoScript add-on. Instead the current recommendation is to use the add-on Privacy Badger [6], which will learn about what trackers are trying to get to you and suppress those it notices are tracking you. It also has the ability for you to adjust its settings by hand so it can be made as severe as you like.

Real world tracking

One of the displays I saw in London showed in real time all the devices that had left their wifi open and trying to connect for everyone in the room. It was fascinating how many were left open, especially Apple devices, both phones and iPads, and also how accurately they could be located. When you leave wifi enabled, the device will always be trying to connect to whatever networks it can find. This means that you may inadvertently connect to a tracking network, or illegal access point where all traffic is scanned.

Always turn off wifi when you are not using it, and only connect to networks that you know about.

How to see where the browser goes

Firefox has an add-on called Lightbeam [7] which collects the locations of all sites that are visited, either directly, or via third party links. If you leave it to collect this information over weeks, then you can get it to display all the connections graphically. It also has a mode where it will suppress tracking, but I know nothing about those capabilities.

References

[1] Botsman, Rachel., *Who Can You Trust? How Technology Brought Us Together – and Why It Could Drive Us Apart*, Penguin Portfolio, 2017, ISBN: 978-0241296172

[2] Trackography at https://trackography.org/ is run by the Electronic Frontier Foundation (EFF) and can tell you which sites are tracking your use of which media sites.

[3]Panopticlick at https://panopticlick.eff.org/ will compute the uniqueness of your browser among those that EFF have seen. There also helpful hints on what you might do in some cases.

[4]HTTPS everywhere at https://www.eff.org/https-everywhere will switch to HTTPS connections for those sites it knows will support it. Firefox has an add-on from its store.

[5]HTTPS by default at https://github.com/Rob--W/https-by-default will force everything to HTTPS unless you have made an explicit exception. Firefox has an add-on from its store.

[6] Privacy Badger at https://www.eff.org/privacybadger will learn and suppress tracking sites. Firefox has an add-on from its store.

[7] Lightbeam at https://addons.mozilla.org/en-US/firefox/addon/lightbeam/ enables you to see where the browser has been. It accumulates data over time and can display all the links graphically.