# Trackers, what are they?

Created on 8 February 2023

Everytime you go online, you leave behind a series of **digital footprints**, which record information such as the videos you watched or liked on YouTube, or stuff you purchased on websites like Amazon.

## Where do these footprints go?

The footprints you left online can be collected by something called **TRACKERS**. You can imagine trackers as little elves that pick up your data.



TRACKER elves collect information about the websites and apps you visit, and send them to other companies.

Multiple TRACKER elves can be found on every website you visit, and every app you have on your phone. In some cases, there can be as many as 20+ TRACKER elves for one app.

# What do TRACKERS do?

There are different types of TRACKERS

**FUNCTIONAL TRACKERS**

Provide services you request, such as remembering your username, region, and language.

**ADVERTISING TRACKERS**

Monitor your behaviour online and display ads according to your interests

**SOCIAL TRACKERS**

Used by social media apps to collect your likes, follows, comments and sharings.

Some of these TRACKER elves are essential for apps to function, while others help app companies to avoid creating their own tracker elves all the time.



However, because tracker elves collect lots of data about your online digital footprints, they can know a lot of you, and they can start to make assumptions about you, such as assuming what kind of videos you like to watch, or how old you may be.

These elves can also *share* their assumptions about you with other tracker elves from other websites or apps you use. They are kind of gossiping about what you do on different websites and apps without you knowing it, so that they create what they think a more precise `profile' about you,

Because trackers now know so much about everyone online, many companies are paying lots of money to have this data. This is how tracker companies make money, even though you don't have to pay to use any website or apps.

# What does this mean for you?

Trackers can appear harmless, because they are largely invisible, and nobody seems to know how much data they collect about us.

Finding out more about what trackers do is an important task for many computer scientists in Oxford.

Our research has shown that trackers are found in many of the apps out there. We also found that trackers are quite **commonly found on apps appearing child-friendly, or commonly used by many children**. For example, we found 30+ trackers associated with the app Duolingo, 20+ associated with YouTube and Instagram (see figure below).
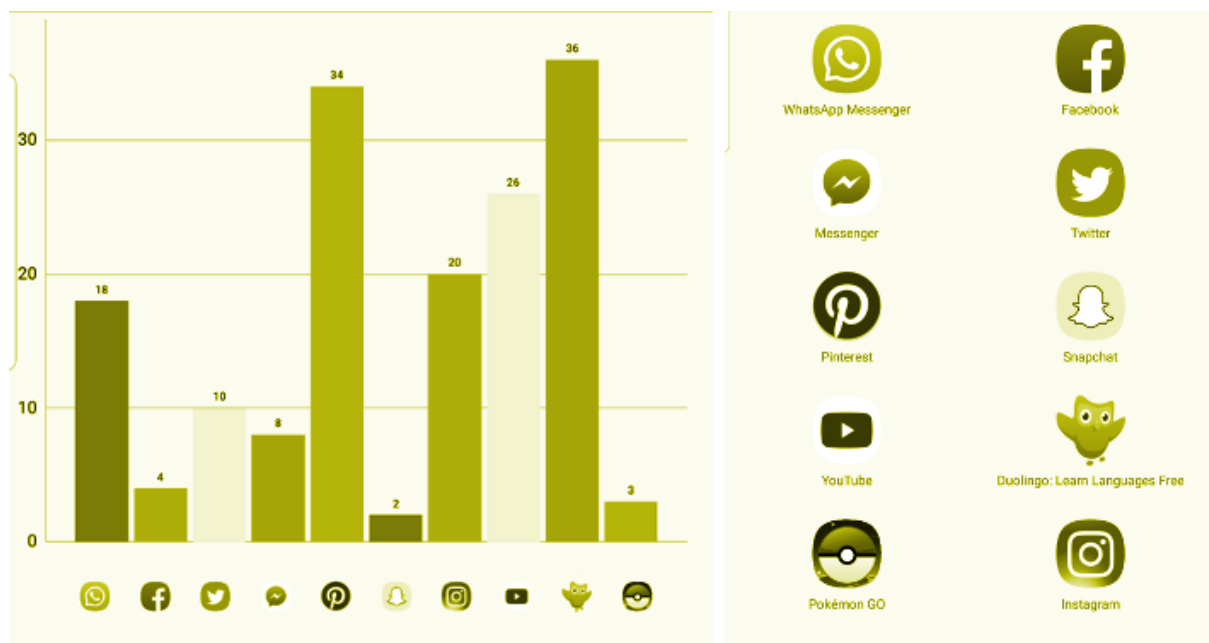


Analysis performed in 2019

We also noticed that from the moment a user opened an app, lots of *footprints* were sent over to many trackers. The footprints could include information about your location (although rarely your postcode or precise location), your device ID, the model of your device (being an Android or iOS), as well as other information such as when you used an app, for how long, and other apps you are using.

One *visible* consequence of trackers is users receiving lots of (often tailored) advertisements. The tracker industry is estimated to be worth several billions American dollars, and they largely make money by online marketing -- sending targeted advertisements to users.

Tech companies use lots of techniques to persuade users to stay longer on the apps, so that users can buy more stuff or they could collect more data about the users. Such techniques are what we call **'profiling'** -- users' actions online are extensively analysed by computer code in order to decide what type of users you may be, and repeatedly put `interesting' content in front of you. Without you realising it, you may start to develop a new habit or interest, such as an addiction to a new type of energy drink, or constantly checking your social media accounts in fear of missing out. This is the magic of tracking, profiling and advertising!
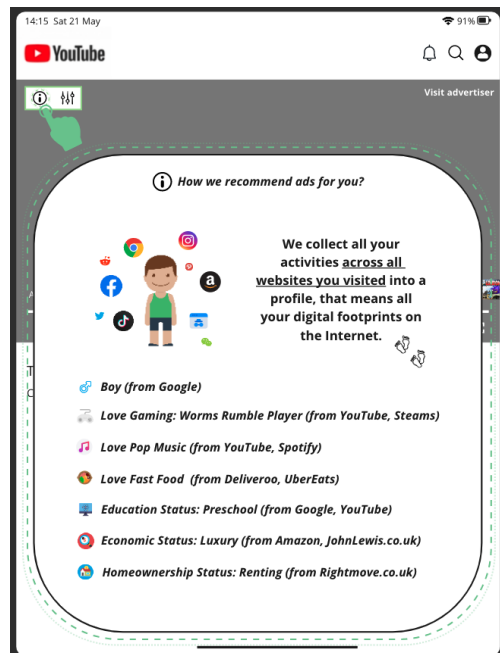


Apart from these less direct harms, there have also been lots of serious consequences when tracking and profiling are used by tech companies to control what a user sees online. For example, influence users' opinions about a country or their leaders, or having children or teenagers repeatedly exposed to harmful content online.

## What can we do?

First of all, by reading this short article, we hope many of you will become more aware of what trackers are and what they do.

We created the KOALA Hero app to help you reveal the trackers behind the apps. You can also block some of the trackers you don't like, although this function is not quite perfect yet.

We are working very hard to reduce the use of trackers in tech or even remove them completely. However, it can be challenging to bring changes. We would love to hear your thoughts and hope this article can help you think more about what you see and do online.

**You can learn more about trackers with our short video and comic book. You can also write to us via oxfordccai@cs.ox.ac.uk.**

# Glossary

Digital footprints: Everytime you go online, you leave behind a series of **digital footprints**, which record information such as the videos you watched or liked on YouTube, or stuff you purchased on websites like Amazon.

**Trackers**: **Trackers** collect digital footprints you left online, and use this information to make assumptions about you, such as assuming what kind of videos you like to watch, or how old you may be. They also often share this information with trackers of different websites and apps to make a more precise guess about you and your interests.

**Profiling**: **Profiling** is a computing technique that collects and analyses users' actions online in order to decide what type of users you may be, and repeatedly puts 'interesting' content in front of you. Without you realising it, you may start to develop a new habit or interest, such as addiction to a new type of energy drink, or constantly checking your social media accounts in fear of missing out.