TARGETED ADVERTISING OR HOW ADVERTISING COMPANIES COLLECT DATA ABOUT INTERNET USERS

Olenich D.I., *olenichvovk@gmail.com*
Dmytro Motornyi Tavria State Agrotechnological University

Before the advent of the Internet, advertisers and marketers aimed at their target audience, showing their ads on TV at certain times of the day, publishing their ads in newspapers and placing billboards in places where they would be seen clearly. Advertisers and marketers can now connect to the online world and receive massive amounts of user data to help get their message across to the right person at the right time.

Most of Internet users know that their online activity is tracked, usually via cookies, and is used for advertising and marketing purposes – but that is all they know. Most of these people do not know how much of their online data is collected and flows through the online advertising ecosystem [1]. Most of users have probably heard of cookies too – they are small text files that remain on the computer after visiting sites. Using a cookie, a website can track user activity online to know how much time you spent on the website, remember which language you chose and which other individual settings applied when visiting it. The web server of this site generates a cookie called ‘the main cookie’ – it mostly serves for analytics and other functional purposes. This cookie is often important for the site to function properly.

On the other hand, there are cookies generated by companies whose sites you have not visited, and they are a threat to privacy. One of the most aggressive ways to monitor user activity is the so-called digital fingerprint method. It is much more complicated than using cookies, but avoiding such surveillance is much more difficult. This method uses a script to collect information about the type of device, operating system (PC, iPhone, iPad, Android and so on), installed browser extensions, text encoding, time zone, screen resolution, installed fonts and more. Besides, advertising companies collect data about users on social networks. The easiest way to find out about user preferences is to analyze likes and emoji’s. For example, if you shared an article about tours to Brazil and put a smiley on it, then this act defines you as a lover of exotic trips. By gathering all this data together, marketers can create the perfect portrait of the consumer and to some extent understand you even better than your friends [2].

According to Dr. Peter Hannai, senior security consultant at *Asterisk*, a cyber security firm, smartphones are eavesdropping on us, albeit not in the sinister sense. In order for your smartphone to record your conversation, it needs a trigger – as when you say ‘hey Siri’ or ‘ok Google’. Without such triggers, any data you provide is processed only by the phone itself [2].

Here are some important tips for those who want to protect themselves from online surveillance. Change the default cookie settings in the browser and disable third-party cookies so that your data is not saved locally or as third-party cookies. The same settings should be applied to sessions and local storage. Learn about managing cookie settings in Chrome, Firefox and Opera. Configure your browser so that it automatically clears the local storage when it closes. For example, in Google Chrome, you can do this like this: go to ‘Settings’, choose ‘Show advanced settings’, click on the ‘Content Settings’ button in the ‘Personal Data’ section. In the ‘Cookies section’, check the box next to ‘Delete data when closing the browser’. Being careful while using online recourses safeguards users’ information from targeted advertising best of all.

References

1. Facebook and others are tracking you. *Globalnews*: website. URL: https://globalnews.ca (Last accessed 12.10.2019).
2. The Truth about Online Privacy. *Clearcode*: website. URL: https://clearcode.cc (Last accessed 12.10.2019).

Language adviser: Zaitseva N.V, Senior Teacher of the Department of Foreign languages