

Privacy in virtual world

Have you ever visited any website? Have you ever sent an e-mail?

Have you ever used any application cooperating with the Internet?

If yes, do you know what data or information can be shared, published or provided to companies and what can other people know about you? Not only hackers' attacks, viruses, worms and Trojans are dangerous and can collect your private information. However, data collected and saved by companies providing services you use every day are also more public than you would like to even if you maybe do not know about it or just do not pay attention to it.

Most of applications, websites and web services collect some data about your activities, which can be later used to enhance functionality of the application, to provide search results faster or show more relevant information. On one hand it sounds great because it saves your time with providing better results. On the other hand it could be also dangerous and harmful because our personal data are saved somewhere and other companies or persons can potentially work with it or easily sell it. These data can carry different information. From information about your activity during browsing an Internet such as visited webpages, searches you made, goods you ordered to your personal profiles from social networks and mail clients. Simply said a website activity is tracked all the time.

Nowadays a lot of webpages use some kinds of analysis, which allow them to analyse what visitors do there. These tools can check what they click on, what they interact with, what they search for, if they scrolled enough to see the advertisement and so on. However, some tools just measure number of persons visiting the page and their activities in anonymous form, there are some other which allow to tailor the page for specific visitor. The above mentioned measurements are possible to be done also for a specific person. This data are saved either on sever site or client site and there is created a profile connected with user's web-browser, and used next time when visiting the page.

This is possible mainly due to lovely named tool cookie. Webpages you visit save your personal settings and some information which are connected with you and your profile on the page to small text files which are sent via network and saved on your PC. When you visit the same page again your personal settings are restored from this file. Of course these files are being sent encrypted but still there is a chance that some intruder can catch them and decrypt. Moreover in many cases are cookies used to improve and aim advertisements appearing on websites you are visiting. Such kind of utilization is for users not just useless but in many cases also unwanted.

Aimed advertisement is recently a big business and many companies have a huge profit from it. They collect, save the data and sell to third parties later on. Some of them are even companies we would not expect so. They collect our personal data which we give them by using applications or other services. Of course it has to be written in a user license agreement but sometime they just write uncertain information not describing exactly how are data collected and to whom distributed. Moreover if you install some application the agreement usually appears and you have to check a checkbox or click on button that you agree with it, but a lot of web services do not show you the agreement before using them and you agree with it by just using them even if you do not know about it.