

# [New functions of social networking sites](https://assignbuster.com/new-functions-of-social-networking-sites/)

[Technology](https://assignbuster.com/essay-subjects/technology/)

Facial recognition technology A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the previous images and setting up a facial database.

Recently, the famous social networking website, Facebook, announced that they would be implementing facial recognition technology in the tagging function of photos. With this technology applied, the Facebook system could recognize a person’s facial features and save all the data they have collected into a database. The Facebook system can identify the person in any photo with help from information saved in the database and tag the person immediately.

Doubtlessly, the new function can make the tagging process of photos a lot easier. With this new function, Facebook will suggest the person’s name for the human faces it has identified. Users don’t need to spend time on tagging every single photo that he has uploaded, so they might upload more photos as tagging is more convenient now, which might increase the connection between friends.

It seems like this technology is beneficial for everyone. However, we should look deeper and look at its effect on our privacy. As soon as this technology is applied in Facebook, some privacy issues are raised. Every time a user tags a photo, Facebook will automatically remember the facial feature of the person and save it in its system. Once it has collected an accurate database of every user (several hundred million users), it is not merely a social website, but a searching engine also!

Imagine, anybody on the street could take a picture of a person at anytime, and discover everything about that person just by posting the photo on Facebook and clicking the name that is suggested in order to read his profile. If the database fall into any government, the result may be disastrous. Even if the user have opted out the function, Facebook still gets their facial features from their previous tagged photo, and even photos that they have untagged! This is obvious a horrible consequence that such a “ convenient” function may lead to.

Some people may argue that the function actually give users more privacy, more chances of being tagged and discover what photos with their faces shown is posted on Facebook. However, compared to giving your facial features and information to the Facebook system, the latter is more destructive.

Facebook seems to be a safe and personal social platform for users to get connected with friends. But users should be aware of the fact that strangers on the web may gain access to their personal data and misuse it if they don’t handle their personal data carefully. Therefore, users should always pay attention to their privacy setting. First, they should not upload some of their sensitive information to the website, e. g. ID card number, address, daily routine (check-ins), telephone number etc., as these may allow strangers to keep track on their activities with the help of your photos. Secondly, they should be aware of their privacy setting. Users should avoid showing all their posts and photos to the public unless it’s necessary. These two basic measures against privacy infringement could help users to protect their own information from access by strangers.

Facial technology surely does bring us more freedom and convenience in connecting with friends. On the other hand, it infringes our privacy. Therefore, we should always use social networking sites carefully. Tracking cookies in browsers Apart from the new functions in social networking sites, tracking cookies also cause public concern on privacy issues.

Tracking cookies are basically used in an exchanging process, for an origin website to send state information (anything that can be accomplished through storing text data on the user's computer) to a user's browser and for the browser to return the state information to the origin site. However, some websites or hackers will use it as spyware in order to track the user’s browsing habits and history, get their account information or even password! All social networking sites contain cookies for its functions, making sure that you can log in at any time to the social networking site and to sites and services that connect with it and share what you're doing. Without the cookies, you cannot share Youtube links on your Facebook wall!

However, it was found that the cookies are only altered, but not deleted after you logged out. That means even when users are not on the site, the cookies are still tracking your browsing habits, and sometimes sending the information you browse to your Facebook account and posted on your wall. For example, when you are browsing the websites/ using the applications which are connected to the social networking site, it may send the link to your homepage and display it on your homepage without getting your permission.

Also, those websites might get our email and information from the social networking site and send advertising email, to the users. Even worse, sometimes cookies may mistakably send your account information and passwords to the social networking system, which infringe our privacy on browsing websites. To avoid this happening, we should log off every time and delete the cookies. Once again, the tracking cookies of social networking sites show us that how Internet technology could infringe our privacy while giving us the freedom and convenience to be “ connected” with friends faraway.