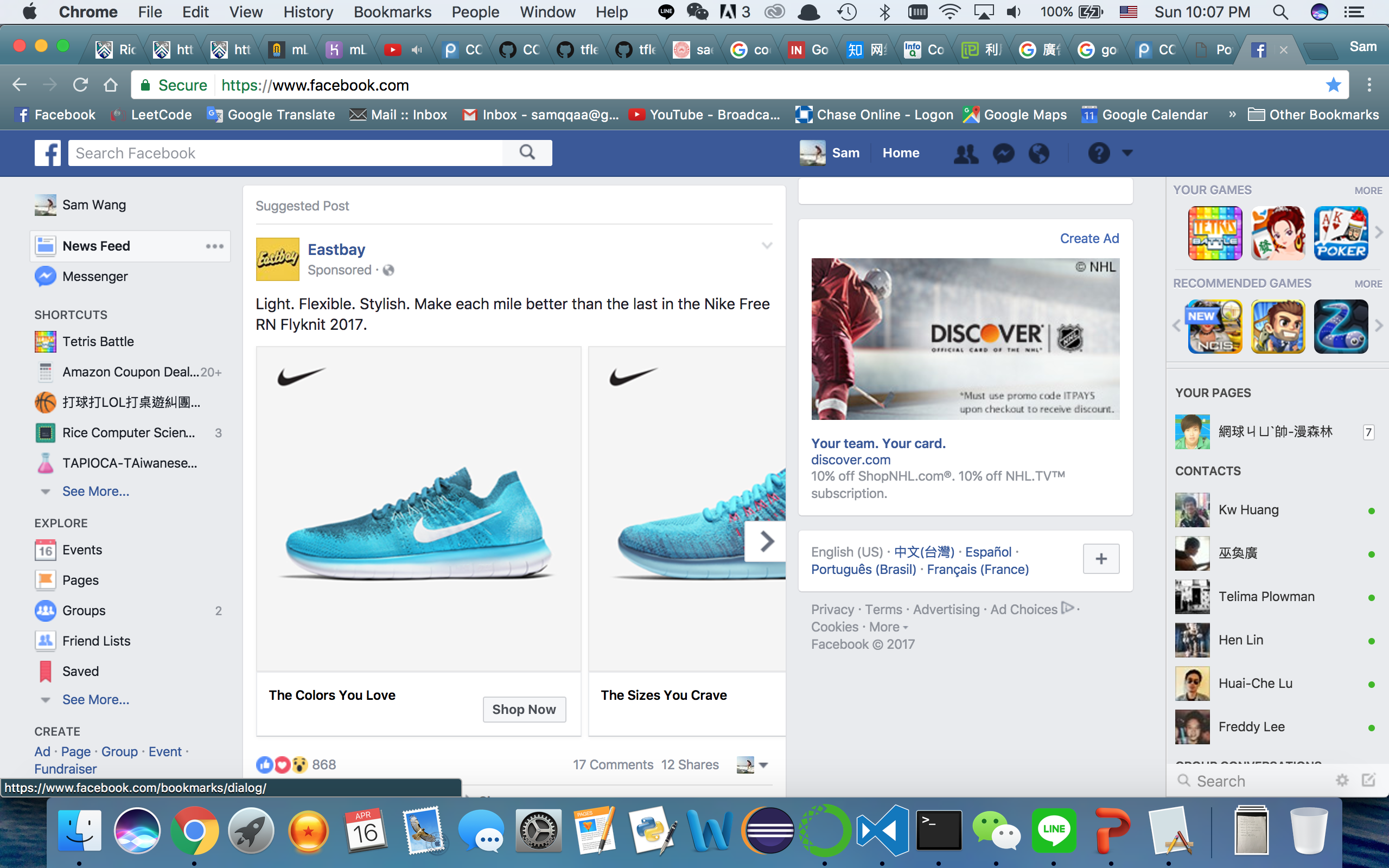
**Ads and Cookie Safety**

**Comp 531**

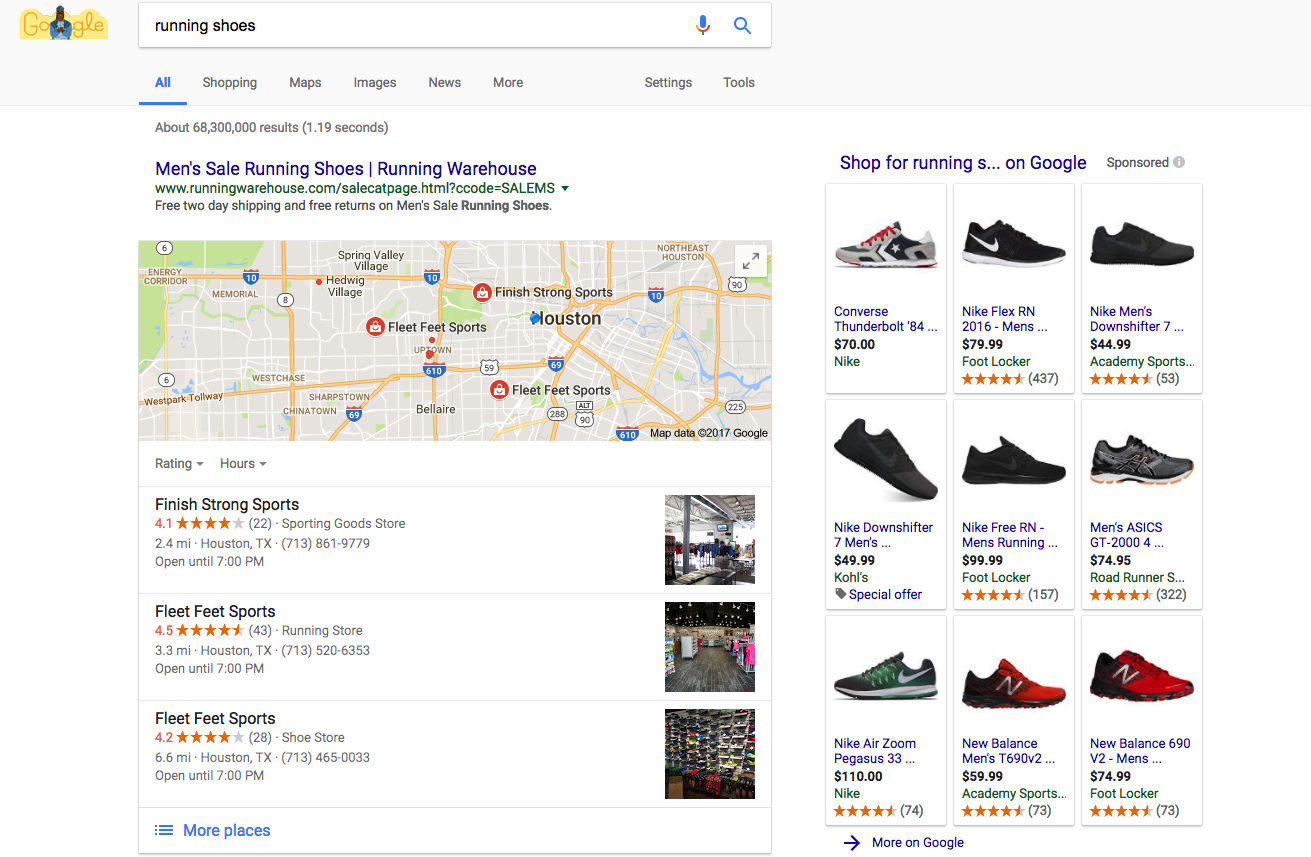
**Sam Wang**

We have seen online commercials everywhere, on webpages, search engine and even social networks. This blog is to break down how online advertisement works and how it is related to cookie safety.

First of all, let me remind you what cookies are. Cookies are a little piece of data given by a web server and store on the browser. It can be your personal information such as your username, preferred language, IP address, user habits and more. It is stored as a text file and will be sent back to the server every time the browser has a request from the server. It is extremely handy that it remembers your preference and you do not have to reset it every time you log back to the website.

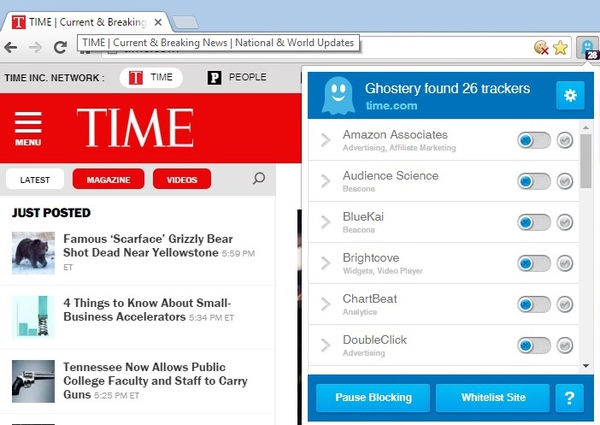


Now, how is it related to online advertisement? Have you ever had the experience that a piece of commercial follows you wherever you go, and the item of the commercial happened to be the one you recently viewed? Yes, they are using cookie. Let’s look at the picture above. When I went to Eastbay website to buy a pair of shoes, they had their cookie stored on my browser. Eastbay then buy the commercial service from Facebook. Facebook consequently have a frame/component of Eastbay embedded in the central column. Facebook might have sold the ad service to many customers but when it detects my cookie from Eastbay, it displays the commercial right into my newsfeed. The Discover commercial in the right column has the same logic as well. The usage of cookie is call third party cookie. Facebook does not own the cookie and neither does it have the access. It is also called cross-site cookie.



As for ads on Google, it works a bit differently. Presumably you are using Google Chrome as your main browser and you have linked your Google account with it, Google has had your cookie already. It is linked to your account and Google can therefore use it to detect your personal information. On the right side is the display ad, customers buy the commercial service and when Google will access user cookie and find appropriate blocks to display.

Even though there are accurate commercials that might meet your personal need, isn’t that a little scary? How the websites access your browsing history and use it for advertising. Do you feel your privacy is invaded? There are few things you can do. First of all, you can activate the Do Not Track (DNT) feature on your browser. Almost all the browsers have this feature and it poses DNT field on the http header. It therefore disallows the cross-site user tracking from the websites. Your cookies will not be access by any other website if it does not have the same domain name. Secondly, you can have some add-ons on you browsers such as Adblock. This kind of add-ons not only blocks the usage of cross-site cookies but further stops displaying the commercial components on the web applications. This method is very powerful and is very popular among all users. The last one to secure your privacy is the Ghostery add-on. It detects the components on the website that is accessing/tracking your data. If you see any suspicious components on the add-on, you can just disable its access. This method can effectively block some sketchy websites from stealing your personal information.



There are some malicious websites that sneakily put a one-pixel component onto popular websites such as Yahoo or Google. Since it is put onto the website, its component thus has the right to access to your cookie and send it back to the malicious server end. The component is usually invisible and is hard to detect if you do not have good web knowledge. They might be selling the information to other corporations and analyze personal habits. This kind of stealing components is called web beacons/bugs. Luckily once this web beacon was detected by Ghostery, it can be blocked once and for all.

Since the DNT field can effectively block the cross-site tracking and all the browsers have this feature, you might wonder why it is not set as default. The answer is simply: there are a lot of interests involved. Online advertising is a huge business and the net profit earn by popular commercial agency is measured in billions. No one wants to give up the benefits and it is therefore not used.



Traditional online advertising works well because it has the user cookie on the browser. It tracks the preference and interest of users and thus adjusts the corresponding commercial strategy. However, this type of cookie tracking ads has started to decline after 2007. The reason is the rise of smart phones/tablets. Apple Inc. revolutionarily banned the usage of third party cookie. The CEO back then was Eric Litman; he thought the commercial agency gained too much personal information through the visit of websites and thus disabled the functionality. After that, advertising agencies have to find another way to gain the information from users. It does not affect Apple much because apple has the user Apple account linked to the device. They have all the access to user information on users’ IPhone/IPad. However, this indeed impacted Google a lot, they only have Google Chrome app to gain the cookie and most of the users just used the default browser Safari instead of downloading a new one.

All the advertising agencies therefore have to adapt a new way to access users’ data. The Interactive Advertising Bureau has published a whitepaper to discuss some alternative technologies to replace the traditional cookie tracking. The one that is mostly likely to be the next major tracking method is the mobile ID. Since every smart device has a unique ID, it makes sense to track the ID and analyze the information of the users. All the online commercial corporations are working on innovative methods to analyze user data and there is a balance to be found between the profits commercials bring and the privacy of all users. We the users would not mind commercials on webpage as long as it is safe and acquires minimum personal information.

Reference:

Google policies

<https://www.google.com/policies/technologies/ads/>

Facebook policies

<https://www.facebook.com/policies/cookies/>

HTTP cookie Wikipedia

<https://en.wikipedia.org/wiki/HTTP_cookie>