Lab 1

a) Some applications we can use to see who is tracking us and encrypt your activity are as followed. Ghostery is a browser extension, what this extension does is it monitors the different web servers that are being called from a web page. It then matches them with a library of trackers. If Ghostery finds a match in the list of trackers it will show the tracker in the pop-up bubble or control panel. You can configure Ghostery to block communication with one or more of these trackers. Ghostery will interrupt the call form leaving the web browser. Another application to use is EasyPrivacy.

   EasyPrivacy is an optional filter list for your computer that completely removes all forms of tracking from the internet. This includes web bugs and tracking scripts this will protect your personal data. Probably the most common way to stop tracking is to use HTTPS. HTTPS is a communications protocol for secure communication over computer network. An asymmetric system uses two keys to encrypt communications a public key and a private key. Anything encrypted with the public key can only be decrypted with the private key and vis versa. These trackers track you to find information about you. This will lead to them suggesting ads for you to look at. Other things they can learn are what videos you might be interested in and web sites to visit. Some of these may be harmful to your computer. We can prevent this by using the applications mentioned above. These applications all proved us with a means to stop tracking and make our time on the internet safer.

b) The deep web gets its name because you will not find what you are looking for with a simple google search. Th deep web is comprised of sites that aren’t indexed. All the deep web websites are encrypted. The deep web can also go by names such as the Invisible web or the Hidden web. No one knows how big the deep web is. It could be hundreds or even thousands of times bigger the surface web. How we can reach the deep web is through the tor browser. Tor stands for the onion router and is an open source application available to the public. Tor is a network of volunteer relays where the user’s internet connection is routed. When this connection is established it is then encrypted and the incoming traffic bounces off the relays located all around the globe making the user anonymous. Tor protects a user's privacy, but does not hide the fact that Tor is being used. This way not only that your IP Address is kept safe but the entire message as well.

Some websites restrict what is allowed when using Tor. An example is Wikipedia limits the edits that can be made through Tor. When accessing the deep web, you must be careful of some of the following dangers. Many websites also operate in the dark, this is where criminal and hackers harbour and have plans to carry out malicious activity’s such as illegal drug trafficking, human trafficking and much more. Some links on the deep web can be deceptive to users. Avoid all suspicious links and any advertisements that you see as they could contain illegal or disturbing images. Another danger is not to confuse the deep web with the dark web. The deep web uses parts of the dark so you must browse with caution. It is not illegal to use the deep web. The deep web is just recourse that aren’t listed by popular search engines. However, as the deep web uses parts of the dark web some of the activity’s there are very illegals such as child pornography and human trafficking. These activities are obviously illegal so extra caution should be taken when browsing the deep web. The deep web houses 90% of the surface web. While 10% is accessible by everyday users just using search engines like Google, Yahoo or Bing.