**Problem**

Internet Privacy issue is an important topic on the internet. Much of the discussion is characterized by hype and preys on fear. This is obvious from looking at the wide range of “spyware protection” products available on the internet and the language used to promote these products. Without knowing the realities of how their surfing patterns are tracked and what they do with that information.

At the moment, technology is changing rapidly, so it is difficult for rules and procedures to be established and enforced as change is the only thing that is constant. Perhaps the greatest cause for concern is the unknown. Surfers do not know when and if they are being tracked, who collects that information, how it is done and for what purposes. Most internet users or surfers are least bothered about their online privacy and are unaware of the possible risks associated with it. Not only is their privacy endangered, but their safety too, especially when they are using the internet to carry out important and secretive tasks like online banking and sharing crucial business files.

Online users are incredibly vulnerable to security threats and there is a long list of issues associated with their safety. When we are online, we are spied on by a number of trackers for various purposes. Trackers keep a record of our search history and track all of our online activities through various means. This provides them with a clear picture of who we are and our interests, which is a breach of internet privacy policy and makes us a public property. Most of the time, this tracking is for advertisement purposes only and it allows advertisers to show ads according to our tastes and interests. But sometimes, this information is used by cybercriminals to carry out unauthorized and illegal activities risking our online existence.

There are various sites on the internet that need our personal information to get access to their services. These sites often store cookies and save your personal information and later use it for various purposes. Most of the time, this information is not encrypted and can be accessed by anyone. This mishandling of personal information may lead to serious consequences. The modern trend of e-banking portals have multiplied the risks associated with our internet privacy. By sharing our bank details and crucial files on the internet, we are paving ways for cyber burglars and making ourselves vulnerable to cybercriminals.

Most internet users proudly upload their social media posts highlighting their current location along with tagging friends and family members. It’s fun and exciting to share your life events with friends and family, but this data does not remain restricted to our expected audience only. This same data is stored on the social media site we are using and stays there forever, often without us knowing (though we might have been given our consent through a terms and services agreement). Along with social media apps, Google Maps and other apps also ask for our location and by turning on our location, we are providing first-hand information to the world about where exactly we are and what our next move is which is certainly risky and insecure.