**Findings And Discussions**

A study was conducted including 77 surveys and 21 in-depth interviews. The results suggest that, in addition to using the default privacy settings, students have developed a number of strategies to address their privacy needs. These strategies are used primarily to guard against social privacy threats and consist of excluding contact information, using fixed profile selection, untaging any information attached onto and removing tagged photos. These strategies are used primarily against social privacy threats and consist of cutting out any contact information.  It concludes as there is a tilt toward social privacy concerns. Little concern was raised about institutional privacy and no strategies were in place to protect against threats from the use of personal data by institutions. This is relevant for policy discussions, because it suggests that the collection, aggregation, and utilization of personal data for targeted advertisement have become an accepted social norm.

Another study was done on the internet users of the United States. With more and more people using the internet everyday, rates of internet penetration have risen exponentially. In this data-driven era, some people depend on the internet to store their information. The study shows that the number of data breaches that occurred in 2019 rise by 216 than the number of breaches that occurred during 2018.  While some see the loss of privacy as a necessary evil, almost 50 percent of U.S. internet users were more concerned about online privacy in 2019 than they were in 2018. With the rise of concern for the breach of internet privacy, new methods to prevent data breaches have been implemented. These new measures have reduced the number of breaches recently. Data breaches have been reduced by 400 from 2019 to 2020.

In any case, stolen personal information is always considered as loss, however sometimes consumers can benefit from revealing personal information, there are many situations in which they would rather remain anonymous. Several tools are available to help people browse the Web anonymously. Perhaps the best-known Web anonymity tool is the Anonymizer (http://www.anonymizer.com), a service that submits requests to Web sites on behalf of its users. Because the request is submitted by the Anonymizer rather than the user, information about that person is not revealed to the Web site. The Anonymizer is easy to use and provides both free and paid-subscription services. Users must trust the Anonymizer to protect their privacy, however, and this tool does not prevent users' Internet service providers from logging their Web activities. Other anonymity tools do not require users to trust a third party to maintain anonymity. Most of these tools, however, are still research prototypes. Crowds is an anonymity system developed by my colleagues at AT&T Labs-Research. With the slogan "Anonymity loves company," Crowds is based on the idea that people can be anonymous when they blend into a crowd. Large numbers of geographically distributed Web surfers can join a group called a crowd and forward all of their HTTP requests through the crowd. Each request is randomly forwarded to another member of the crowd, who can either submit it directly to the end server or forward it to another randomly selected member of the crowd. Neither the end Web server nor any of the crowd members can determine where the request originated. Users participate in a crowd by running a proxy server on their local computers and configuring their browsers to use the local computer as a proxy. Another anonymity tool developed at Lucent's Bell Labs is useful for people who want persistent but anonymous relationships with Web sites. The Lucent Personalized Web Assistant (LPWA) inserts pseudonyms into Web forms that request a user's name. LPWA is designed to consistently use the same pseudonyms every time a particular user returns to the same site, but use a different pseudonym at each Web site. This tool works in conjunction with an anonymizing proxy server; it could also be used with a system like Crowds. LPWA users allow Web sites to accumulate a profile of their preferences over time that may be useful for tailoring content and advertisements to their interests. However, LPWA prevents profile information from being linked to a user's name or combined with information revealed to other sites. P3P also contains a feature that allows for pseudonymous relationships and can be used in place of cookies. Users may choose to send the same unique identifier each time they return to a Web site with which they have reached an agreement. A P3P-compliant browser keeps track of the identifiers and sends a different one to each site. The goal is that once P3P implementations are readily available, Web sites will use this feature when they wish to develop persistent relationships with consumers but do not need personally identifiable information to provide their services. A P3P-compliant browser should also give users complete control over when to take advantage of this feature.