The Importance of Internet Privacy and Net Neutrality to Internet Users in the Modern Era

As electronic commerce gains traction in our modern world, internet privacy and anonymity are essential to internet users. The contemporary society is full of free internet services because of the belief that the internet is the solution for the future. We all own cell phones, shop online and use credit cards. However, the corporations and governments controlling the online surveillance do more than storing the information. Whenever we use the internet we expect net neutrality; not to be interfered with when carrying out our online activities on the internet. Net neutrality safeguards our right to communicate on the internet freely. Therefore, internet privacy is paramount, and access rights of internet users must be respected by the government and the corporate sector.

According to Techopedia, internet privacy is protection provided for the data published online by individuals through the internet. Net neutrality, on the other hand, is an internet principle that prevents internet service providers from influencing communication through the internet. The internet service providers are mandated to provide smooth and unrestricted communication for internet users under the net neutrality principle. However, last week the FCC voted on net neutrality, a move seen as a plan to kill net neutrality. The move has, however, received significant criticism with the majority of those against the move call for preservation of the existing net neutrality laws.

Internet users have resentfully admitted to the fact that online surveillance by the governments and companies is part of normal life. Internet users in the United States have less protection than other countries (Mineo, N.p). The Congress recently voted to allow for collection and selling of customers' browsing data. According to a security expert, Schneier (2017), the U.S.A Freedom Act had little impact in changing the way the government collected data. "The NSA's data collection has not changed; the laws limiting what the NSA can do have not changed; the technology that permits them to do it has not changed" (Mineo, N.p). According to Schneier, Edward Snowden's revelations about the government's surveillance plan informed the people of what was happening, but it never changed what was happening.

The National Security Agency (NSA) is a United States intelligence unit charged with the collection, translation and analysis of data and information for the sake of monitoring and counter intelligence. As a security agency, privacy of data and information is necessary. Therefore, tight security measures are essential in protecting the privacy of the data and information under the custody of the NSA. The case of Edward Snowden is a case of insider

threat which was not anticipated when designing the security policy for the NSA. Therefore, some of the security measures put in place could not prevent Edward Snowden from accessing the information. However, the agency could have used CCTV cameras to track down Edward's activities and assigned somebody to monitor him. (Insider Threat Detection, p6). It would have made him to change his mind concerning exposing the information to the media and to the public.

Video analytics tools could be used to identify the psychophysical state of Edward Snowden, especially when accessing high security areas such as the server room and the data warehouse. The agency could also monitor the behavior of employees including their work schedules, usage of USB, phone communications, network logs, email trails, and badge swipes. It would have made it difficult for Edward Snowden to access the vital information, thus, reducing the danger caused by his revelations (Insider Threat Detection, pg5).

Another scenario where an insider may pose a threat to network security is whereby an employee with privileges of accessing vital information in the master database maliciously alters information and changes passwords belonging to other employees thus denying them the services they require. Most security policies focus on hackers and thus it will be difficult to detect malicious employees since their actions will be stimulated by a particular event. In this case the employee could be provoked by let's say low salary or a conflict with a fellow employee, which could influence them to sabotage the network thus posing a serious threat.

Edward Snowden was not a traitor. The agency gave him privileges to access top secret files and thus, he did not persuade other employees to give him their passwords or perform malicious activities so as to obtain the information (Edward Snowden is no Traitor, N.p). The mass surveillance program had been in place for a long time, but what Edward Snowden was not pleased with was the manner in which surveillance with sexual content or people who are naked were circulated among the employees. He felt that this behavior was unethical and therefore, he blew the whistle on the National Security Agency where he was a senior employee (Snowden Is No Hero Yet, N.p).

Surveillance is the avenue through which the internet service providers make money. Everyone is at risk of surveillance as many companies are exchanging personal data to marketing agencies that not only use the information to send us targeted advertisements and offers but also to suggest the prices we are charged for the goods suggested by these firms. The companies use the information to manipulate the news articles and advertisements that we receive in our emails. Governments, on the other hand, use surveillance to discriminate, freeze free speech, and to censor what people can see. The corporations and the governments share the data collected, and in some cases, the data is lost due to huge security breaches in their systems.

Online information saving and cookies are attributes of the Web that many businesses utilize but have significantly criticized in the recent past. A cookie is data generated by a Web server that is saved on the hard drive of a user's workstation. This data, called state information, presents a mechanism for the Web site that stored the cookie to track a user's Web-browsing patterns and preferences ("PARKER INFORMATION RESOURCES"). A Web server can use state information to forecast future needs, and state information can help a Web site resume an activity that was initiated previously. For instance, you may use your web browser to access a Web site that trades a particular product; the Website may store a cookie on your computer that describes what products you were viewing. When you visit the site at a later date, the Website may retrieve the state information from the cookie and prompt you to review that particular product or view similar products ("PARKER INFORMATION RESOURCES").

Other typical applications that store cookies on user machines include search engines; the shopping carts used by Web retailers, and secure e-commerce applications. The information on previous viewing habits that is stored in a cookie can also be used by other Web sites to customize their Web page. One recent use of cookies involves the storage of information that helps a Web site decide which advertising banner to display on the user's screen. With this technique, a Web site can tailor advertisements to the user's profile of past Web activity.

Although Web site owners defend the use of cookies as being helpful to Web consumers, storing of information by a Web site on the user's computers is an invasion of privacy. The data or information captured is private and sensitive. Sometimes the web servers send this information to other websites that use it to track the user's online activities. Users concerned about this privacy issue can instruct their browsers to inform them whenever a Web site is storing a cookie and provide the option of disabling the storage of the cookie. Users can also view their cookies and delete their cookie files.

According to a news article by Cheryl Pellerin (2014) on cyber legislation, the U.S. government must address the issues concerning leaking of confidential information to the media, and establish cyber laws. These were the critical issues emphasized by Keith B. Alexander, a U.S. Cyber Command general, and NSA director. Quoting an example of a previous media leak in his speech by Edward Snowden, Alexander insisted that such activities by National Security Agency officials are restricting the establishment of cyber laws (Cheryl, N.p). Snowden disclosed confidential information to the media about the NSA's surveillance program and fled the United States. However, Snowden has since been charged with espionage and theft of federal government documents.

Alexander also defended the British ruling against David Miranda, a Guardian journalist and a partner to Glenn Greenwald. The verdict illustrates how the British government has successfully established legislations against the release of national security intelligence to the public despite

the “jigsaw” nature of that information. Journalists’ have a professional duty of care to ensure that what they publish does not endanger the public interest, including the lives of the citizens, and the security of the country (Cheryl, N.p).

The Cyber Command has prioritized five critical issues in an endeavor to prepare for the growing cyber future. These issues include creating a secure architecture that will enable them to fix vulnerabilities within the shortest time. Another critical issue is the training of the workforce and acquiring them high standards skills such as those of the NSA’s elite units. The Cyber Command also intends to establish a security policy to streamline command and control. They also seek to develop shared situational knowledge in cyberspace, and grant the NSA and Cyber Command the power to share with the industry confidential information such as malware signatures and information about cyber threats (Cheryl, N.p). In addition, the nation should establish a way of collaborating with other countries to safeguard the cyberspace. The general insisted that the matter of cyber security requires a team’s effort and sharing of information between the country’s security and intelligence units including the FBI and the Department of Homeland Security. The U.S. government must handle the concerns about authority and media leaks before it begins to address the cyber legislations.

According to Eric Lichtblau’s article in the Los Angeles Times (2001), a professed FBI spy Hanssen disclosed to the government interrogators that he exposed the identity of one of the top United States double agents to the Russians a number of years back. The renowned Soviet mole was charged with espionage and executed by the Russian government in 1988. The interrogations of Hanssen have raised concerns about the amount of sensitive information available to the FBI agents, and how Hanssen got access to the information.

As an FBI supervisor, Hanssen had unrestricted access to highly classified information. However, the authorities suspect that he used other means to gain access to information about other U.S. agents (Eric, N.p). The possibility that Hanssen could access information from multiple intelligence agencies raises an alarm about the need for the FBI to enforce strict authentication measures. The FBI should limit the authorization of agents to only those that need to know the classified information.

Following Hanssen’s debriefings the authorities found out that in the late 1985, Hanssen gave out three names of Russian agents who were undercover spies to the United States. The detectives had also been exposed by Aldrich H. Ames, a CIA agent who was also a Soviet spy (Eric, N.p). The Russian government executed two of the agents, Valeriy Martynov and Sergey Motorin, betrayed by Hanssen and Ames. In the process of the interrogations, it was discovered that the third agent betrayed by Hanssen was a top U.S. spy, Dimitri Polyakov, who started working as an undercover agent in the early 1960s (Eric, N.p).

Polyakov, a Soviet Military officer, was highly acknowledged by the U.S. government as the greatest spy the country ever had. He provided the FBI and later the CIA with intelligence about the nuclear activities, and military capabilities of the Russian government. He also gave out names of top Russian spies, and perhaps this gave him fame within the U.S. intelligence circle. The Americans, however, suspect that between the time that Polyakov disappeared and the time he was executed, the Russian government used him to bring wrong information to the CIA (Eric, N.p).

Without net neutrality, the internet service providers have the powers to choose which content the users can access and they can block websites that contain content or political opinion that they disagree (Bell, N.p). The internet companies can also offer preferential treatment to content writers who are willing to pay for the privileges and restrict those who cannot afford to pay. Thus, lack of net neutrality blocks free speech and can be used by governments to deny individuals the right to access information (Bell, N.p). The recent vote on net neutrality paints a bad picture of the United States President Trump's governance. The move will kill the right of the media to provide the citizens with relevant information since some of the content may not see the light in the media or websites (Press Free, N.p).

Small business owners and entrepreneurs depend on the open internet. Net neutrality is important to them because they rely on the internet to launch their businesses, to communicate to their customers, to create markets as well as to advertise their products and services (Press Free, N.p). With the invention of the Internet of Things, many people in the business world have achieved tremendous growth. We require the internet to support competition and innovation. Several enterprises rely on the concept of "Big Data"; information stored in the cloud. The removal of net neutrality rules will hinder the operation of cloud services and this will give an upper hand to internet service providers to deny services to competitors of particular partisan firms that are willing to pay them for preferential treatment.

We can minimize the risks of internet privacy. Installing preventive software such as anti-virus, firewalls and anti-spam applications will help prevent attacks on information stored online. Individuals should avoid shopping on unverified websites to lower the chances of providing information to unauthorized users. Checking if websites are secured can help internet users determine if the security level of the website is adequate before providing personal data ("Online Privacy: Using the Internet Safely"). Clearing the browser's cache memory and browsing history consistently and using very strong passwords can help prevent loss of personal data and safeguard against unauthorized access.

In conclusion, the United States has laws that treat internet companies in a hands-off manner. Online surveillance by the government is a fact of normal life since the people tend to allow it because they are assured of protection. The Americans tend to trust corporations, hence there

is a high usage of online platforms and credit cards to transact which exposes personal data to unauthorized users. With more and more lives getting online, especially through social media, privacy intrusions tend to have a devastating impact. Therefore, it is crucial to foster internet privacy and net neutrality to minimize risks and to safeguard the individuals' right to privacy.