Internet Privacy: The Affected Of The Dependency On The Internet

1 - Introduction

Internet privacy, or online privacy is defined as the security level of personal data published on the Internet by users. Privacy on the internet refers to how safe and secure your personal information and data is once you publish the data on any website. However the recent rise in the popularity of the internet has led to turmoil amongst the general public when it comes to safety online. Internet dependence is a newly-formed term for excessive use of the Internet and its services to the detriment of a user's physical, psychological, or social well-being, as stated by researchers at Villanova University.

Issue Analysis: This research focuses on the effect of the steep rise in the number of internet users as well as its integration into different aspects of one's life on online privacy. I have focused on the direct as well as influenced correlation between the internet's increased usage over the past few years with the different aspects of increased or decreased privacy, such as identity thefts and hacks.

2.1 - Causes

Internet of Things

One of the major causes of the overdependence on the internet is the Internet of Things (IoT). IoT refers to the connecting of multiple household devices over the internet, so that they can be controlled through any electronic gadget such as mobile phone, laptop etc. In recent years, the number of such devices including smart home devices such as lamps, air conditioners and fans, has risen, and around 140 million such devices were bought worldwide in the year 2019, as stated by statista.com. They are popular mainly because they are marketed for increasing comfort as well as convenience. However, this connection of devices over the internet makes the network susceptible to dangerous cyber attacks, as a person in control of the network not only has access to your information, but also your daily use of electronic gadgets.

A DDoS attack refers to a Directed Denial of Service Attack, where multiple computer systems, or "botnet", which are being used by the general population are hacked into and used to overload an organisation's servers by trying to access their website in large numbers. These computer systems also include the various smart home devices.

In 2016, the largest DDoS attack ever was initiated on the popular internet service provider Dyn using an IoT botnet. This led to a significant portion of the internet going down, including popular sites such as Twitter, Netflix, CNN and Reddit. Although not proven, this attack likely led to a large amount of user data being obtained by the perpetrators.

Rise in usage of social media

Social media sites have grown so popular that a significant fraction of the population is registered on sites like facebook and instagram4. Studies show that a majority of the users are aged 18-30, as stated in a survey done by the London School of Economics and Political Sciences . With everyone posting their photos from vacations to discussing political situations on these sites, it has become a social necessity to be a part of this community.

This poses an increased risk of loss of privacy, as people are constantly aware of your whereabouts. Due to the anonymity features provided by these sites, you may not know the identity of the people who have access to your online profile. This leads to a significant decrease in privacy.

2.2 - Consequences

1. Susceptibility to hacks

The internet, having grown its mass user base, has acquired a lot of new users who are not as adept with technology as others. Without taking necessary precautions, users are susceptible to a vast array of scams, malware and hacks floating around the internet. These threats pose a lot of risks, some of which include the other party gaining personal information, deleting or modifying data, remotely accessing the user’s device, etc.

The Internet of Things has skyrocketed in popularity in the previous few years, mostly due to being a new concept. With all the benefits offered, however, comes an increased susceptibility and vulnerability to hacks. With a variety of home automation devices connected to the same network, an outsider gaining access to that network can directly intrude in a user’s life by using these devices without permission.

2. Identity theft

Identity theft refers to the act of posing as someone else after gaining access to their personal information. With the rise in popularity of the internet, identity theft has become a much more prevalent issue. Around 33% of the population of the United States of America has experienced identity theft.

Essentially losing your identity to someone else poses a lot of risks. Crime ring syndicates, or even individuals who have access to a user’s personal information, are capable of extracting both money and information from banks, email accounts, social media applications etc.

This is a prevalent issue due to the recently popularized use of social media. Users often post their contact information while creating their profile, which is available to anyone who visits it. As stated earlier, data collected from the user is also shared with third party organisations, which also poses a risk of identity theft in case of a security breach

3. Perspectives

3.1 - Global Perspective

The year 2018 saw over 3 million identity theft reports, which likely suggests that many more

went unreported, as stated by Insurance Information Institute.

Private International is an international charter organisation based in London which diverts its resources towards research on internet privacy. It frequently challenges governments and private organisations that collect personal data and information online, or permit it. It states that over 40% of international privacy law brochures altered rights against mass surveillance. For example, in the United States of America, Internet service providers (ISP) such as Comcast can now increase or decrease your internet speed depending on the type of content you want to access,for eg. your internet speed may be drastically reduced if they notice you trying to access movies online, compared to images. The fact that ISP's can monitor your activity and take action against you accordingly is a huge violation of your privacy, and Privacy International is constantly working towards undoing such violations.

40 years ago, the Council of Europe's Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data was signed. This Act set guidelines for the flow of private data over the internet, and the restrictions upon it. Although these laws were reviewed again in 2013, many countries still don't have a comprehensive data protection framework in place. Countries in today's world have to counter cyber attacks, push for these laws to pass, and enforce these laws to punish those who break them, a much harder task in a world of anonymity.

The countries part of the European Union have been working on reforms to take back control of online privacy. Privacy in today's world is perceived as a question of power - "who is in charge here?".

3.2 - National Perspective

Singapore is an avid supporter of transparency when it comes to internet privacy.The government passed the Personal Data Protection Act in 2012, which aims to regulate the flow and disclosure of a user's sensitive data, and later established the Personal Data Protection Commission in 2013 to make sure that the Act is implemented correctly.

Singapore along with the PDPC aims to balance the need to protect an individuals' sensitive data and the needs of organisations to use this data for legal and legitimate purposes. This includes contact information as well. PDPC serves to enforce the Do Not Call Registry, which exists to make sure citizens do not receive unnecessary telemarketing phone calls and messages.

Singapore's healthcare database was a victim of a cyber attack in the year 2018, where close 1.5 million citizens' personal healthcare data was illegally accessed, including prime minister Lee Hsien Loong's prescription data

Singaporean citizens are globally the second most concerned about their online privacy, with close to 47.8% voicing their concerns about the privacy of collected data, as stated by the Singapore Business Review. With a significant percentage of the population being above the age of 50, keeping data private is a significantly important task for the government, as many citizens are not adept with the rules and risks that come with the internet.

4 - Courses of Action:

1. Involvement of Governments

Governments around the world are starting to take strict action against companies who are not transparent with how data is used. They are being pressured by the citizens to intervene and protect their data, but these are the same citizens that also want the best possible user experience . Regional and global laws regarding declaration of use of user data will significantly end up reducing privacy risks online

2. Involvement of Powerful Organisations

Even browsers such as Google are starting to punish websites without a secured communication certificate or SSL certificate, by ranking them lower on a search results page. Such certificates are offered to websites that allow communication with the user on a secured channel, where data is encrypted on both ends. Lowering websites on search result rankings allows them to decrease traffic for websites which do not offer a secure method of data transfer and storage.

Up to 93% of users do not read the terms and conditions before creating an account or downloading an app. Often, data is collected from the clients' side while the user is in the process of using an online service or just browsing online. This data is used, as claimed by various organisations and companies, for the betterment of the services offered. Hidden in Facebook’s settings, one can see close to 98 different data points that Facebook compiles from each individual: the user’s exact location, income and net worth, and even their home's value, says gen.medium.com. Evidently, the best course of action regarding internet privacy is to support Private International’s stance on data transparency.

Various studies have found that transparency about the utilisation and protection of user’s data reinforces trust. To assess this effect, Harvard Business Review surveyed consumers from close to 46 companies, from which the highest “trust rating” was given to those companies which were completely transparent about their utility of user data, some including banks and credit card companies.

5 - Personal Perspective and Conclusion

I believe that the definition of privacy becomes fluid when we talk about the internet. With the advancements in technology being made, data from the user allows service providers to focus on popular services and features of their products, and improve henceforth.

Often taken as cookie data, this data refers to the genre of websites visited, browsing habits, preferred devices to browse on etc. However, the user often has no information about how much data is being collected, when it is collected as well as how it is used. This leads to a drastic decrease in terms of privacy and anonymity on the internet.

In my opinion, transparency on the side of organisations and companies is crucial for the safe advancement of the internet. I believe that the public would be able to judge websites and sources better if they had information about how, where and when their data is used.

I also believe that the anonymous features offered by the internet lead to a major increase in privacy online. The internet serves as a platform for anyone to state their views and opinions while keeping their identity hidden, which has many positive benefits.

6 - Source Evaluation

A majority of the sources used for research date from 2016 or later, which makes them recent enough to count as valid sources. Sources like Private International's website, as well as government websites for USA and Singapore, are verified expert sources which provide more credibility.

On the other hand references have been made from multiple blogs, some of which were part of a product selling page, which may lead to biased opinions. However, these sources do provide in-depth analysis and statistics as well as can be considered expert sources due to being involved in the same field.