IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 18, Issue 5, Ser. I (Sept. – October. 2023), PP 25-27
www.iosrjournals.org

Should There Be Surveillance Of The Internet By Government And Private Companies In The 21st Century?

Akshat Jain

Date of Submission: 03-10-2023 Date of Acceptance: 13-10-2023

I. Introduction

Privacy protection is an overly sensitive and important topic in today's world. Nobody knows if they are exposed on the internet or not. By exposed I mean, if they know if they are there or if what all details about them are there or if something about them is true or not. I feel every person whether famous or not has a right to their privacy. Privacy is the right given to every person on the internet about what they want to show or not and privacy protection is to protect their data uploaded from being misused without the persons' permission. It is extremely hard to control this as people don't get to know if they are getting hacked or not. For example- T mobile got to know that more than 40 million people's data got stolen from them, but no vital information was out.

Cybercrimes are one of the most important and growing problems related with digital world. Cybersecurity, which is the technique of protecting computers, networks, programs, and data from unauthorised access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information is one of the issues of growing relevance at a time when internet use is increasing at a rapid pace. Encryption is present in many social media applications and texting platforms like WhatsApp. They have end to end encryption which means that no one can access the texts between the two users. Encryption means to convert readable data into an encoded format. The data then can only be seen when it's decrypted. Surveillance of the internet is when there is constantly someone checking the data to protect it from various malware and viruses. It helps the customer when a company surveillance the data, but it still raises the problem of privacy. It might be that some customers do not want to share their data with the company they are using, and some customers might want it to save their device. In my report I am going to develop the argument of why there should be surveillance of the internet. [1]

Case for surveillance of internet:

There are many risks, some more serious than others. There are a lot of people who are getting hacked. Important and confidential data like images, presentations, etcetera is getting lost or is seen by people who don't need to see them or are being put on the internet without permission. Among these dangers is malware erasing the entire system, an attacker breaking into the system and altering files, an attacker using the computer to attack others, or an attacker stealing credit card information and making unauthorised purchases. There is no guarantee that with the best precautions some of these things will stop. So, to prevent and keep data safe people buy paid software like antivirus, etc. There is encryption present in some apps but not on everything else so, with the help of the paid antivirus and stuff the consumers are protecting their data from being hacked. Also, there is cyber security in which the consumer can directly take help from them to catch the person who injected the virus into the device. Then there is surveillance of the internet which is already there and is seen by the government officials of every country or by the officials working in the specific company being used. For example, the recent case in which the social media companies were removing the accounts of Taliban users to stand against them and for them to not access the whole countries data on the platform. Another example of Alibaba getting hacked in 2019 and more than 1.1 billion pieces of data got stolen[2]. So, the need for surveillance is especially important and crucial in these times of growing technology where even a small piece of data can destroy lives of many.

Case for against surveillance of Internet:

There are some cases against the surveillance of the internet because sometimes surveillance can lead to exploitation of the data or the data being used for other purposes which are not supported by the customer. For example, Governments in Europe, India and elsewhere are demanding change since they understand many of today's tech-business models depend on the violation of consumer privacy.

What are the consequences of surveillance? [3]
There are many consequences of surveillance, some which are beneficial and some which are very harmful.

In positive manner:
- The data will not be stolen and hence there won't be any 3rd person hiding in the texts.
- Hacking, phishing, etc. chances of happening will decrease.
- Safer on the browser, credentials typed such as from debit and credit cards are safe.

In negative manner:
- No privacy left, the texts, search history, etc is all with company and nothing can be kept private.
- The location will always be shared with the company and the transaction and stuff will be all shown.
- Evidence shows that mass surveillance takes away intellectual freedom and damages the social life of affected societies, it also opens the door to flawed and illegal profiling of individuals. Mass surveillance has also been shown to not prevent terrorist attacks.
- Mass surveillance can change the behaviour of people trying to use the internet.

Comparison between having cyber security and surveillance vs not having:

Having cyber security will prevent attacks on the system and its data while not having it will make life much easier for hackers who are hacking and stealing data, money, and resources every day. With surveillance users can get help from professionals to get rid of people who are stalking and texting even when the user does not want them to. Not having them will give the user privacy, which is a basic human right and can do anything they want on the internet but with a lot of risk which could lead to dangerous situations which can put them at risk.

Personal Perspective:

Personally, I have had issues with this whole thing. Somebody had sent me a link to download an application. With the benefit of the application, I got a virus on my phone. Luckily, my phone didn't have any data otherwise the risk was higher. With less surveillance people can enjoy being on the net because it can help them to relax and have fun as this is immensely helpful. My family also keeps checking on what I do on the internet but in a limited way, so that I could enjoy being there while being a responsible child. So, I and my whole family think that surveillance by government and private firms is particularly important for the well-being of a person on the vast internet and technology world.

National Perspectives:

In India there are cases of people getting hacked or suffering from something from the internet is increasing day by day. Now with the frequent use of the internet because of online classes, work from home, etc., there could be days when someone clicks on something which they shouldn't have and leads to serious issues like fraud, etc. Cyber security and surveillance of the internet has increased in India since 2010 as the government found out that the rate of crime is increasing though the strict checking will only be done when a case has been registered. India is fully committed to an 'open, secure, free, accessible and stable cyberspace environment' and would like cyberspace for 'innovation, economic growth and sustainable development.' as per the IISS report. The people in India majorly think that this causes their privacy to decrease and start growing concerns on their personal and public life but have also started to like this because of the help they are getting from these sections in the digital world.

Global Perspectives:
There are 126 countries in the world, having national data protection legal framework.
Still many countries in the world do not have comprehensive data protection laws.

Though, there are ongoing challenges with enforcement of the laws and failure to uphold the privacy protection standards.

Furthermore, some of the countries have a weak rule of law and power dynamics skewed by socio-economic and political challenges which raise additional factors which must be addressed in advance before enforcing a surveillance on people.

Course of Action:

So, to prevent this every single device should have an anti-virus, offered by many companies and people should have strong passwords which are hard to guess. It should be person to person. This will give at least some protection to the user, other than that the government needs to secure their internet so that it is hard to enter it. This will prevent all the attacks but will be an exceedingly difficult thing to do. Also, to stop money

stealing, people need to stop saving passwords and other information on their system as this won't give anything away. Though this will be tiring and tough to do because mostly everyone is in the habit of saving everything. Other than that, they should stop opening unknown emails with promotions and stop opening websites or downloading things from unsafe sources. For example: Famous companies like Amazon, Apple, etc Salways send emails with the user's name written and have mail ids like Example@no-reply.com and all the fake mails never mention the name and don't have this kind of id.

II. Conclusion:

In Conclusion, one's privacy on the internet is very important because of all the applications, services, scams, and viruses on the internet that are waiting for any given chance to steal someone's personal material. If all people could protect themselves and use the right software, they would be much safer, and it would be harder to have personal information stolen from them. Anyone using the internet should take into consideration this information will help them in the future to protect their privacy and maintain security.

Sources-

[1]. Https://Www.Hrw.Org/News/2021/03/04/Technology-Enabling-Surveillance-Inequality-During-Pandemic
[2]. Https://Edtechnology.Co.Uk/International/Study-Shows-Annual-Increase-Global-User-Data-Surveillance/
[3]. Https://Us-Cert.Cisa.Gov/Ncas/Tips/St04-001
[4]. Https://Economictimes.Indiatimes.Com/Definition/Cyber-Security
[5]. Https://Www.Cjfe.Org/How_Mass_Surveillance_Harms_Societies_And_Individuals_And_What_You_Can_Do_About_It
[6]. Https://Legaljobs.Io/Blog/Cyber-Crime-Statistics/
[7]. Https://Cobalt.Io/Blog/Business-Cost-Of-Cybercrime