DATA PROTECTION AND PRIVACY CONCERN IN CYBERSPACE

| Authored By : Mr. Ritik Kumar Rath |

2.1. Introduction

"The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual.[1]"

— Earl Warren

Privacy is generally seen as the ability of a person to maintain some kind of secrecy in his activities which enables him to isolate himself from others in order to protect his interests. And it appears more valuable when you do not have it. When threatened by someone's faulty action is the time when we understand the importance of security and trust. This can be a consequence of our lives being transformed into data. Every single second of the lives that we live is being stored on the internet as a data and is available to every living soul on the earth. In such a precarious situation what does the word privacy stands for? This question can only be understood by studying the disparate and complex landscape of the internet of things which would further lead us to realization of how to make sure privacy rights are maintained and respected. In today's world scenario breach of privacy does not occur on a physical level but in the space of internet. This happens because of the mass exposure a person has to this service. Internet when first introduced offered people to transfer their data at high speeds but there was no security vault to keep this data safe, thus disabling the users to control to whom to reveal this data. This disadvantage was ignored by the users due to the compelling nature of the internet and soon more and more individuals and businesses started embracing the power that internet gave us. It was this digitization that required the people to reveal their information. Consequentially protection of online data became important and thus extended the term 'privacy' to 'e- privacy',

[1] The fantastic advances in the field of electronic communication constitute ,(nov 23 , 2018, 10.04 AM) , https://www.goodreads.com/quotes/230601

2.2. E- Surveillance- boon or a bane

Our way of interaction in today's world is affected by the networked nature of digital society. Using online services results in privacy losses that are not always trivial to the users or the regulators. In today's world social surveillance is not only used to keep a close watch on each other, but also the data of an individual user can be used to infer his private attributes. In an individual perspective, users have the opportunity to price their personal information and thus the power to balance the benefits, costs, opportunities and risks of online activities[2]. But this perspective is only available if the users are working in isolation. However, the omnipresent nature of internet leaves such a perspective obsolete and can produce results that are unaccounted for to the individual. Users are entering into numerous interactions online being unaware of the fact that large chunks of traces that such interactions are leaving. Such traces are used to know the private attributes of an individual.

An example of a breach of privacy through surveillance is shadow profiles. Shadow profiles are files that contain the private information that they give to use online services. In other cases, these profiles could be made without their permission. In such cases, the person who is being profiled does not submit to terms and conditions of such surveillance.

2.3. Cyber-security

Individual internet users are the pillars of cyber-security. But these often prove to be the weakest link in respect to cyber-attacks. Personal computers are used as the stage of cyber-attacks to spread viruses and malware. Concerns of these computer users are not the greater harm that would be caused to the people at a large scale but they are concerned about their own personal data and thus privacy and rights in general.

2.4. Privacy and Data Protection

Modern practices of privacy focus on no surveillance of communication (communication privacy) and no handling of information about individuals (information privacy).

Information has always been an important tool for the state to exercise control over its population. It is not possible for people to opt out from providing this information. Information technology, such as that used in data mining, aids in collecting data from various govt. sources to conduct analysis and establishing the usual pattern. One of the main issues relating to the

[2] - E. and Kennedy, C. (1997). The right to privacy. New York, N.Y.: Vintage Books.

collection of data by the government is to maintain a balance between the privacy of individuals and modernization of government function. The government must draw a line so as to restrict itself from using personal data of an individual beyond the necessary government functions relating to public policy. Although in recent years an increase in the appetite of government for collecting personal data for compulsory identification (biometric data) can be seen. Governments authority to collect information, including a provision for lawful interception of information was broadened by the events of 11 September in the USA and various other legislations in other countries[3]. In addition to this EU also has the power to retain data necessary to identify a user for a period of 6 to 24 months.

2.5. Edward Snowden Case – citizen data is not secure

The control that a government holds over the private data of an individual amount to the breach of their privacy. This control came into light by the work of Edward Snowden. On the 20th may, 2013 a fight started between a superpower and a 30-year-old man just for the sake of privacy. In this Edward Snowden risked his life to bring out the true picture and safeguard the rights of the citizens. This fight ended with showing up the real face of a security agency that in the name of national security they are meddling with individual privacy[4]. This fight saw its birth from 1.5 million documents belonging to US secret agency coming before the eyes of individual people making them concerned for their privacy. What acted as a lubricant was the prism program run by the US government for keeping surveillance over its people, moreover they were not only intruding the privacy of their citizens but also that of all 35 world leaders. In addition, there was a program named XKEYYSCORE by which NSA was authorized to monitor everything that you search on the net and that too without consent. NSA to achieve this motive was directly connected to the server of tech companies like Yahoo and Google to procure all the data even those they were not willing to give.

It is not that the US government did not have any reason behind these programs. By the PRISM scheme initiated on September 11, 2001 the government drastically increases the power with the secret agencies using which the intelligence agencies can capture the private data of citizen who are not suspected of any connection to terrorism or any wrongdoing. The tools used by these agencies were evolved after the 9/11 which began under George Bush with the Patriot Act and expanded by the Foreign Intelligence Surveillance Act (FISA) enacted in 2006 and

[3] Ibid.
[4] https://www.bbc.com. (2018). Leaks that exposed US spy programme. [online] Available at: https://www.bbc.com/news/world-us-canada-23123964 [Accessed 25 Nov. 2018].

2007. Also, another initiative of the US government was the XKEYSCORE which is a search engine interface that works by interacting with all the NSA databases for the collected internet traffic, communicated and phone metadata of private citizen. Edward Snowden appreciated NSA's activities as focused and specifically deployed against legitimate foreign intelligence targets that the leaders need to protect the security and integrity of the nation. But what he criticized was the use of these tools for surveillance over the citizens of its land. Thus, explaining the XKEYSCORE as legal when used as a part of NSA's foreign signals intelligence collection system but illegal when used against its own citizens who are not posing any grave threat.

Till now researchers have talked about how government players breach the privacy of individuals but there also are some non- governmental players who play a crucial part in this offense. Some of these players do this for their own benefit for the benefit of others[5]. First researchers would like to talk about those offenders who intrude the privacy of individuals to help the third party gain an unfair advantage over the other. These types of offenders could be easily identified by the study of the case in which a firm allegedly helped establish the government of the largest superpower of the world.

2.6. Cambridge Analytica – And its implications

This issue is related to the US presidential election in 2016 and how Facebook and other company helped Donald Trump in winning the election by manipulating data of its user. The main culprit you can say that is not Facebook but Cambridge Analytica which is a British data firm owned partly by Robert Mercer and his family, huge Republican donor of the republic party whose candidate was Donald Trump. The main accusation that they faced was that the organization was drawing flak for its participation in influencing voters' behavior in the 2016 presidential election. The firm was further alleged to have harvested data of 50 million Facebook users belonging to the US without permission in order to design software to predict and influence people's voting preference[6]. This data also gave an unfair advantage to Donald Trump's campaign. But the question that arises is how did Cambridge Analytica gain access to personal data of numerous citizens. This happens when you use an app on Facebook generally a message pop up that the game wants to use your data and people without thinking for a moment, agree to the conditions. The app using this agreement takes data like name, location,

[5] Ibid.
[6] https://theprint.in. (2018). The inside story of what Cambridge Analytica actually did in India.[online]] Available at: https://www.bbc.com/news/world-us-canada-23123964 [Accessed 25 Nov. 2018].

number. Even though Facebook says that they share very less data to no data with any third party but Facebook intentionally give some of the data to Cambridge Analytica. In 2014, Dr. Aleksandr Kogan, a psychology professor at Cambridge University, was allegedly paid 800,000 Dollars by CA to develop an app called "THIS IS YOUR DIGITAL LIFE" to take important data of the Facebook users. Although more than 270,000 people downloaded this app and gave their consent to their data being collected, company's act superseded this consent when they extracted personal information of each of the user's friends without their consent[7]. Later Kogan passed on all the data collected through his app to Cambridge Analytica and other companies. When people downloaded this app, Kogan not only had access to user's basic information such as the city of residence and details about friends, but also data firm from the profiles of their Facebook friends. To acquire the full data a certain amount of money was paid to the app users to complete a survey by Kogan's firm Global Science Research (GSR). This survey also gained permission to access the user's Facebook account to acquire their personal data. This helped GSR to build personality and psychological profiles of millions of people who were in their radar. The data was allegedly used by Cambridge Analytica to tailor its political advertisement for a group individual, whose liking and interest was already known to them. CA used the same strategy in the 2016 US presidential election when the firm worked for Trump. Under the guidance of Brad Parscale, digital director for Trump, Cambridge Analytica performed a variety of service including designing target audience for digital advertisement and fund, modeling voter turnout and determining where trump should travel to best drum up support. On the contrary Facebook deputy general counsel Paul Grewal has endorsed for the falsity of accusations of data breach. He contended that Kogan gained access to information from the users who have signed up for his app and everyone gave consent to the survey. Thus, according to him, no system was infiltrated, and no password or sensitive pieces of information were taken using unfair means. While the perception of various governments is quite different from that of Facebook. One of the examples is the government of UK, which fined Facebook of 500,000 pounds, maximum fine allowed for its role in the Cambridge Analytica case. UK government no longer is concerned with the number of its citizens affected by this scandal (i.e. very less in number) but with the basic right of its citizens to share their information online without a sense of threat in their minds of personal data being stolen that too by one of the largest social networking sites.

[7] Ibid.

Though both the companies are headquartered on foreign lands but that in no way imply that their actions did not have any adverse effects on Indian citizens. We cannot sit at our homes reading of these meddling with an election in some foreign country but we must understand that a critical threat to our digital privacy clouds our country too. This was also reported by Bloomberg, the report stated how Facebook helped the current Indian government on political campaigning and recent reports show that ruling and opposition parties were in contact with Cambridge Analytica. But the question that must come in mind is why the Indian government is silent? This question has a simple answer and that is the long-term relation between Facebook and India. India is the first country to work with Facebook in disaster management and the Indian government does not want to spoil this relation with Facebook. Moreover, Cambridge Analytica on its website claims it worked on Bihar election in 2010 and also that their client achieved a landslide victory[8]. But the reason for this paper is to understand what Cambridge Analytica has that helped them achieve such results? Before presenting their strategies to their clients, Cambridge Analytica using their local knowledge, global reputation, software for political intelligence & election management, access to foremost behavioral change communications methodology in India etc. does caste research, voter demographic analysis, behavioral polling. Based on all such studies company analyses target audience, consult and even does poll planning and management for its clients[9]. Thus, what companies like Cambridge Analytica is not an easy task and that is the reason that they breach the privacy of such a large number of people and charge large amounts for such tasks.

Next in discussion comes those companies who not for the benefit for the other but for their own store and use some personal data of their users. These companies are more dangerous than the companies discussed above because they generally do not conduct any survey or ask for consent but rather keeps a note of all the step taken by an individual on the internet. All these companies to achieve this motive use a software having an innocent and sweet name but is really dangerous as far as privacy is concerned. This term is Cookies.

2.7. Cookies- hidden danger to privacy

These technologies are small files on users' computers or mobile phones that allows the service provider to record information when one visits or interact with websites, application and other

[8] - https://theprint.in. (2018). The inside story of what Cambridge Analytica actually did in India.[online] Available at: https://theprint.in/politics/exclusive-inside-story-cambridge-analytica-actually-india/44012/[Accessed 25 Nov. 2018].

[9] Ibid.

tools. This means when one visits or interacts with websites, the third party is authorized to use cookies to make users experience better, for advertising purposes and to improve the website and service. Though these may seem as simple software but they perform various functions like authenticating users on a website, providing requested service, keeping track of information, remembering preferences and using above data to tailor the website to cater to user's interest. Till now these may seem a really helpful option but the reality is quite different then it seems. In addition to providing better experience cookies can also be used to track people and do things that people may not prefer like delivering targeted ads. Moreover, this is something that has raised reasonable concern among the people. The most important man in the history of cookies is Lou Montulli, who is also responsible for the earliest web developer Lynx in 1991. Later he joined Mosaic Communications Corporation which came to be known as Netscape in 1994[10]. Cookies were first used to verify whether users had visited the website before and were a handy solution for e-commerce websites to remember what was one shopping the last time and was shown a pop up add at different websites. To this function, people were not aware until 1996, when media started reporting on the potential threat to privacy. This threat was the concern that the cookies were storing information on the user's computer without their knowledge or consent. Clearly, cookies make web browsing convenient for us as we don't have to identify ourselves every time, we visit a website, thus many people don't see any threat to their privacy because from all its upsides. But unfortunately, the original intent behind the use of cookies has been crushed by some unfair entities who have found a path to use this otherwise harmless process to track one's movement across the web. These entities are not even stopping after tracking but they move onto using cookies to make detailed profiles of one's interest, lifestyle. On the face, it might seem harmless and trivial to worry upon by most people, as the worst thing they could do is show targeted ads. But the question is not concerned with the use of one's personal data rather the concern is the mere fact that intimate knowledge of one's preference and private activities might eventually be used to brand each of us as a member of a particular group.

Though unfair use of cookies poses a sufficient privacy threat but it fails to attract attention because of the other major threats like Edward Snowden's revelations about the NSA and government surveillance. Moreover, cookies are not the main problem but are the equivalent and worst technologies that just happen to caught in mainstream awareness. This is because over 95% of the websites use cookies mostly for unimportant things that would never cross our

[10] : https://www.digitaltrends.com/computing/history-of-cookies-and-effect-on-privacy/[Accessed 25 Nov. 2018

minds and not all the websites use the cookies in a bad way but only to count visitors and for a quick response. But what has led to the defamation of cookies is its use by large companies like Google and Facebook. These companies hold a vast amount of personally identifiable information like google search may tell about your medical issues and sexual orientation or which political party you support. Sometimes these companies face suits and other times they are just ignored, like in 2012 Google was made to pay $22.5 million as a settlement to over Apple's Safari Web Browser, where there was a default setting to block third- party cookies that Google bypassed and breached a pivotal law. Certain laws have also seen the light of day against unfair uses of cookies[11]. In the USA there have been attempts to introduce legislation like "Do Not Track" law which gives users the right to opt out of being tracked by third party websites. But this was not a success as the difficulty of establishing standards and agreeing workable legislation seems to have retarded its progress. European Union was the organization acknowledge the grave threat imposed by misuse of cookies and thus introduces a certain set of rules.

2.8. EU cookie law[12]- prevention from threat

The law was changed in May 2011 by the e – privacy directive with regard to cookies in the European Union. According to the new law, website owners were charged with telling visitors about the cookies they use and obtaining their consent. Complying websites now show a pop up when one first visits the link, explaining their cookie policy and allows individual to accept it. In the latest study by ICO, which reveals that on an average website places 34 cookies on your device on your first visit, and 70 percent of them are known as third-party cookies (set by other websites other than the one being visited).

Moving onto the next part of the document that deals with breach of privacy by an individual of another individual. This kind of breach is one of the most dangerous ones due to the difficulty of keeping an eye on each and every individual. One of the most prevalent examples for this kind breach could be Revenge Porn. This is one of the less talked off topics but includes all the essentials of publication of personal data without consent. Further, the researchers would like to elaborate on revenge porn as an act done without consent.

[11] Ibid.
[12] EU Cookie Directive . (2009)

It was in 1964, when a famous line was said by American judge Potter Stewart famously said ''I can't define pornography, but I know it when I see it[13].' The reverberations of these words can be felt across the globe even after fifty years. It is known that one man's art is another woman's erotica is another person's sex tape. In today's world the internet has turned into an intrepid, empathetic and nuanced account of the sexual shopping cart, thus 'Revenge' helps in limiting the scope of this offense to inducement through personal vengeance, whereas such an act could be motivated by a desire for profit, notoriety or no reason at all. All images of nudity are intrinsically pornographic and this can be impliedly derived from the term 'porn'. Following this definition, sexually explicit images created and shared within the bounds of a private relationship should not be considered pornographic unless and until they leave the 4 corners of personal relation to being converted into public sexual entertainment. The history of publishing obscene personal images without the consent could be traced back to 1980s when a magazine named hustler which featured image of naked girl called 'beaver hunt' but the problem with this section was that not all the woman gave their image with consent and they published such images without verifying information on forged consent forms. Revenge porn got its major attention in the year 2012 when Hunter Moore launched a website 'is anyone up' that was a user- submitted pornography site. Moreover, this site contained personal information of the victim and this was also a threat to the personal life of the individual. A person by the name of Charlotte Laws was the first person to criticize this but the fans of this site sent her death threat. At that time there were no established principles for an individual's privacy thus there was no sense of guilt among the fans of this site for they were destroying someone's life. This impliedly means that the concept of consent of the victim was considered as non- existent.

2.9. Revenge porn in India – danger to the reputation of a person

India is the 3rd largest country in term of porn video viewership in the year 2017, and the growth of porn viewership rose by 121% in 2017 only. The main reason is the proliferation of smartphone in 2013 as it was close to 44 million but now it is more than 337 million. Revenge porn is defined in Oxford dictionary as "Revealing sexually explicit images or videos of a person posted on the Internet, typically by a former sexual partner or any other person, without the consent of the subject and in order to cause them distress or embarrassment and degrade the reputation of the subject"[14]. Most popular case in India was the DPS MMS clip. The DPS MMS resulted in arising of amateur videos, it becomes a flood gate in India of revenge porn

[13] Jacobellis v. Ohio, 378 U.S.184 (1964)
[14] - Dealing With Revenge Porn in India. (2018). [Blog] The CCG Blog

videos and the number of videos was shared across the internet. What happens with victim of revenge porn is that they suffer in many ways when clips are leaked and distributed, it forces people to changes their names, identity, and sometimes even their physical attributes. And even if the video is filmed and as always women face the brunt of it. The occurrence of these kind of cases led to multiple platforms in 2015, Facebook, Twitter and reddit, announced banning of revenge porn on their websites. The essential element of revenge porn is that the perpetrator and the victim shared an intimate relationship and that the former has deliberately (and without the victim's consent) released sexually explicit information of the subject online in order to cause distress and harm to the victim's reputation. While revenge porn and non - consensual porn are used interchangeably, there is a noticeable difference between them. Non- consensual porn includes within its ambit sexually explicit images captured without a person's knowledge or consent. But in the case of revenge porn, it is very different as it often includes such sensitive information that was voluntarily been captured or send to the perpetrator in good faith in the course of an intimate relationship that should not have been made public. But later released by the person with whom the act was done or with the interference of a 3rd party. In such a precarious situation what is important is to analyze the number of victims and make the subsequent laws to prevent such act of breach. Although in the national crime record bureau's document on cybercrime against women, there is no official statistics available that pertains specifically to revenge porn in India. A 2010 report suggests that "only 35 percent of the women have reported about their victimization.

46.7 % have not reported it and 18.3 % have not been aware of the fact that they have been victimized. The recent situation of revenge porn has prompted various countries to enact legislation that criminalizes it. Some of these countries include the UK, Canada, Australia, Japan and the Philippines.

In India, nonconsensual distribution of images captured with consent is dealt with by the section 354C[15] of the IPC. However, this section has limited its scope to female victims and male offenders, not vice versa.

Transmission of images depicting the private areas of a person is punishable under section 66E[16] of the IT act. The Explanation to the section limits only to private area to "… the naked or undergarment clad genitals, pubic area, buttocks or female breast". This provision is gender-

[15] Indian Penal code ,sec 354(c),1860
[16] Information Technology Act , sec 66(e), 2000

neutral and captures every aspect of revenge porn and not even addressing it by name. However, the narrow definition of "private areas" in this case could limit the applicability of the act in this type of cases where the victim is captured in an intimate position without showing those particular areas this act will not be applicable [17].

Section 67A[18] of the IT Act punishes the offender who made publication or transmission of "material containing sexually explicit acts, etc. in electronic form". While this can punish perpetrators effectively, it also contains risks including within its ambit, victims who may have voluntarily captured and shared such private content with their partners[19].

In the case of JPH v. XYZ & Ors[20] which is a landmark case in which JPH has been in a relationship with XYZ for a number of months, during the course of which a number of pictures and videos were taken by JPH which showed nudity and sexual activity [21]. XYZ sent a series of communications to JPH threatening to post the images on social media and/or to cause them to be published in magazines the court granted an interim non-disclosure order restraining the disclosure or publication of images and information in a so-called "revenge porn" case.

And this was further proven in the case of MM v. BC, RS and Facebook Ireland Ltd[22] .In this case the plaintiff alleged that she has been the victim of revenge porn. She states that she sent, either one or more, highly sexualized photographs of herself to one of the defendants, at a time when they were in a relationship. That subsequently, after the relationship came to an end, one of those photographs was published by the defendants. She asserts that this undermined her independence, her dignity, her right to privacy and was in breach of the Data Protection Act 1998. Here court said revenge porn victim should be helped to live a life of free from harassment, abuse and instances of revenge porn.

2.10. Conclusion

During the duration of this research, the researchers analyzed different ways in which the personal privacy of an individual can be and is breached. These ways include both government and non- government actors. Though breach of privacy by government actors attracts more of attention as compared to that of non -government actor but that in no way implies that breach

[17] Supra 13
[18] Information Technology Act , sec 67(a),2000
[19] Legal steps to take when someone creates your revenge porn. (2018). [Blog] ipleaders. Available at: https://blog.ipleaders.in/revenge-porn/ [Accessed 25 Nov. 2018].
[20] JPH v. XYZ & Ors [2015]EWHC 2871(QB)
[21] Supra 13
[22] MM v. BC, RS and Facebook Ireland Ltd NIQB 127 [2017]

of privacy committed by individuals is less dangerous to the society and its citizens. With the advancement of technology and widespread use of internet, on one side people are being benefited and on the other side, they are some players using every opportunity they get to exploit the personal information of these people. Government though treated as the savior of a nation and its peace, in this modern world has been accused of breaching the privacy of its citizens. There is very little left to trust upon in the world of internet of things. With the study of concept of revenge porn, researchers explained how the ones we loved become the predators of our privacy and threaten not only our dignity but also our mere existence with liberty. In such situations come up the people who act in favor of the people by disclosing the wrongful acts of the offenders by shedding some light on the truth. But the case finally rests with the government who themselves have used unfair means to come in power. These unfair means include all the acts ranging from keeping surveillance over its own people to befooling them or inducing them through targeted advertisements regarding their campaign.