DATA PROTECTION ACT AND THE JUDICIAL APPROACH OF RECOGNIZING THE PSYCHOLOGICAL DISTRESS CAUSED BY THE DATA BREACH CASES

*SUNIDHI SINGH [1]

Introduction

We are living in a world surrounded by assisting and adaptive technology where data security has been a growing concern. The lack of cyber security has posed a risk of data breaches affecting millions of people across the globe. The risk posed by data breach like the financial risk and of being potential victim to extortion is not neglected but when we look at the psychological and emotional loss the victim goes through it is often neglected. We have provisions in the statutes laid down by the various legislatures of the world to protect ones data and privacy but when we look at things on ground zero the practical implication is absent. There are many reasons of the failure of practical implications of the laws, but one cannot say that the risk of data breaches is more in a developing country than a developed one. United States of America faces as many in fact more breaches in a year than a developing country like India despite of the USA being technologically advanced and better developed than India.

While the biggest data breaches and hacks are on the news worldwide what the media and judiciary fails to recognize is the psychological harm caused to the victims of such breaches. The courts often refuse to even recognize the psychological harms, compensating it is a long road ahead. We clearly see a grey area in the data privacy acts which fail to recognize the psychological risk posed to the victims.

Need for data protection act

Most of the big data breaches take place in less than a minute but it takes weeks for the companies to realize any breach has happened. After the social media came into existence, the users thought its purpose is to connect people but actually it analyzes human psychology and benefit from the same. While signing up on social media knowingly or unknowingly we surrender certain rights to those particular sites.

[1] Sunidhi Singh, Student, Symbiosis Law School, Noida

After the sites get access to the user's data they utilize it and prioritize which content a user sees in their feed first by the likelihood that they'll actually want to see it. This is known as social media algorithm, the time at which the posts are put up never matters but the news feed is sorted on the basis of relevance. The user are not aware, most of the times don't pay heed to these details as how their data is used by the sites there is no regulation that protects the privacy of the users. At many times the minds of the younger generations are manipulated by falling trap to the things present on the internet, they start thinking on the same lines but the social media is not here to correct it as their only goal or objective here is to increase the screen time of the user. This manipulation gives rise to juvenile crime rate in society and even leads to riots in many places. The objective of the people working for the social media platforms is merely to increase the engagement time of the users on their platform which generates money for them. There is no regulation as such that binds these platforms and due to this they sometimes start acting as de facto government. The need is to inform the users how their data is being used by these platforms, to draw a thin line between feeding information and manipulation. This need to keep the users informed and protect the data can only be fulfilled if these platforms and the internet as a whole are governed by data privacy act.

When we look at brief history of data protection acts, it can be traced back to 1981 when the council of Europe adopted Data Protection Convention (Treaty 108) rendering right to privacy a legal imperative.[2] In the United States of America the federal law for data protection is the Federal Trade Commission Act. Other than this federal act there is no other act which governs data protection on a federal level but there are acts which are sector specific like the Children's Online Privacy Protection Act (COPPA) which prohibits collection of any information from a child below the age of 13 online and from digitally connected devices, if the information needs to be collected from any child it requires parents consent. In the similar lines there are other acts like Video Privacy Protection Act and Drivers Privacy Protection Act. India on the other hand has not introduced any legislation for data protection specifically but the Information Technology Act, 2000 provides for sections 43A and 72A which protects improper disclosure of data. In today's date the General Data Protection Regulation (GDPR) of the European Union

[2] INPLP, International Network of Privacy Law Professionals (1 June, 2018) https://inplp.com/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/

which came into force in 2018 is considered the most updated act for data protection and since its enforcement has inspired many laws across the world. GDPR can be considered which enhance how people can access information about them and places limits on what organizations can do with personal data.

When we sign up on any site, we often tend to ignore the privacy policy and click on 'I accept' without really going through the privacy policies made to protect the consumers. Now these privacy policies are turning into "ownership policies" said Nico Sell, CEO of the Wickr Foundation.[3] To understand what "ownership policies" are we can refer to one of the Instagrams privacy policy which states "Instagram does not claim ownership of any Content that you post on or through the Service. Instead, you hereby grant to Instagram a non-exclusive, fully paid and royalty-free, transferable, sub-licensable, worldwide license to use the Content that you post on or through the Service." This clearly means that whatever we put on our account on Instagram we give consent to Instagram to use it wherever they want; many users are still unaware of this policy. This happens because there is no regulation binding these sites to some law, there is a need of regulation to protect the privacy to inform the users how their data are collected and used and when this privacy is breached the site should compensate.

Psychological harm suffered by people on the internet

We all notice one thing on the internet when we discuss about any particular product with our friend in a conversation on any site we see a pop up advertisement next moment in our news feed. There could be a number of reasons for this one can be algorithms which are much more complicated than we think or the second probable reason could be someone is hearing or reading our conversations. All this happens on the internet which is a much complicated place and manipulates our minds the way it wants. We put up our opinion, pictures share pictures and posts with our friends on our social media not realizing how it will hit our mental health when all this leaks or used by a third party without our consent. E-skimming that is growing with time as online shopping gets common is a type of malware which infects checkout pages to steal payment and personal information of shoppers. Large companies including Macy's, Puma and

[3] Thompson, 2015 (20 May, 2015)

Ticketmaster have been targeted in the last two years.[4] In such cases anxiety poses as harm due to future risk, this means the users whose data are stolen are under constant fear and anxiety that they can be duped of money from their accounts at any point of time.

Anxiety is a form of emotional distress which is an umbrella term to capture a wide array of negative and disruptive feelings such as sadness, embarrassment, and anxiety, among others.[5] The nature of harm suffered by data breach is complex but court fails to recognize the risk and anxiety suffered by the data breach and considers the matter to be trivial. There are other psychological issues suffered by victims like social anxiety disorder which is a chronic mental health condition in which social interactions causes irrational anxiety symptoms include worrying about embarrassment or humiliation in public. Once your credentials are stolen somewhere you are not informed by the company regarding the list of people whose credentials have been hacked or leaked this creates a panic situation amongst all the customers of the company. Secondly due to constant risk and anxiety faced the person may resist to interact socially, for instance if it comes to knowledge of a person that their personal chats or pictures have been leaked in public then they might develop a fear of being judged by the society and prefer living in isolation.

These are only some instances explaining how the victim in a data breach case suffers and many courts refuse to recognize the psychological harm suffered by the victim on the basis that there are no statutes that guides them to do so. The courts fail to recognize that there are precedents and statutes closely related to data breach and the law needs to be build upon them.

1.3 Judicial approach in data breach cases: An overview

The courts around the world often followed a different approach in recognizing the psychological harm suffered by victim. Data Breach causes a risk of future injury, the third party who gets access to financial information of a user does not poses an immediate threat according

[4] Jennifer Schlesinger, Rahel Solomon 'A cyberattack known as e-skimming is getting more common with the rise of online shopping' (https://www.cnbc.com/2020/01/31/e-skimming-cyberattack-is-growing-along-with-online-shopping.html

[5] 2 DAN B. DOBBS, THE LAW OF TORTS § 302 (2001).

to court until and unless the information stolen is used to create a new bank account. Plaintiffs' "credit information and bank accounts look[ed] the same today as they did" before the breach this was held in Storm vs Paytime[6] by the federal court. In most of the data breaches it becomes really difficult to recognize the risk of future injury as cognizable harm and compensate the same. On the other hand in cases where the hackers have accessed personal data and their motive can be inferred the courts have still refused to recognize harm in the same.[7]

The emotional distress cannot be overlooked in such cases, as a federal district court in New Jersey noted, "[c]ourts across the country have rejected 'emotional distress' as a basis for" finding harm because plaintiffs' fear of identity theft or fraud is based on speculative conclusions that personal data will be used in a malicious way.[8] If we try to understand the courts standing on the issue in a layman's language it means that if identity theft takes place now it poses a risk but when the actual harm is caused it is recognized and compensated by the court so it is trivial to compensate the emotional stress caused. Secondly the financial damaged caused can be recognized but it becomes very difficult to compensate emotional stress as it varies from person to person to measure it financially becomes very difficult. The law has evolved to recognize risk, this trend is likely driven by the fact that modern thinking in science and business, among other domains, is deeply focused on risk. Tort law has developed to recognize the "fear of or the increased risk of developing a disease in the future" and "lost chances to avoid diseases or physical injury" as compensable injuries.

Courts have admitted claims of plaintiffs blaming medical malpractices on doctors that resulted in loss of "opportunity to obtain a better degree of recovery" as held in the case of Lord vs Lovett[9]. For example, in Petriello v. Kalman, a physician made an error that damaged the plaintiff's intestines. The plaintiff was estimated to have between an 8% and 16% chance that she would suffer a future bowel obstruction. The court concluded that the plaintiff should be compensated for the increased risk of developing the bowel obstruction "to the extent that the future harm is likely to occur."In the same line damages awarded in environmental suits are in recognition of future harm or risk, in the apprehension that there is risk to lives in the future. In

[6] Daniel Storm et el vs Paytime Inc, et el
[7] Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018, 1019, 1021
[8] Crisafulli v. Ameritas Life Ins (D.N.J. Apr. 30, 2015).
[9] Lord vs Lovett (112 So. 768, 93 Fla. 611)

suits where industries discharge waste without treating it tends to pollute the ground water and poses risk of dangerous diseases to the people consuming water. There is provision of fine in law for the people who drink and drive or drive above the speed limit it is not taken into consideration if there is any accident as it poses a risk to the lives of other people on road.

The risk of injury in a data breach case can be compared to a medical malpractice or reckless driving where there is a risk posed to the victim and is continuing. A driver who is drunk can be cause of accident at any point of time same way if a hacker has accessed personal information of anyone it can be used to commit a crime at any point of time. In India we talk about Aadhaar a twelve digit unique identification number given to its citizen, modeled on the American social security number now if this number is accessed by a third party it can be used to commit any crime or issue mobile numbers in the preparation to commit crime. Also these numbers have a long shelf life unlike debit card number or passwords which can be changed or blocked by the user.

There have been claims for compensation for the anxiety suffered in such cases, in cases where certain personal information are stolen or accessed there are cases of anxiety. In April, 2020 the Maharashtra Cyber Cell reported that some people using porn sites are being extorted heavy amount stating that if they do not pay them, their activities will be leaked to all their contacts. [10] Anxiety is quite obvious in such cases but arguments against the recognition of anxiety focus on the fact that claims of anxiety are easy to make and difficult to dispute. Plaintiffs will quickly learn to make poignant statements about their anguish with details exaggerating their distress. Defendants may have difficulty disproving plaintiffs' accounts of their own subjective mental states. (Citron, 2018)

Earlier the Judiciary did not recognize emotional distress in cases as it seemed it is too easy to fake. As the law evolved it was taken into account, in some instances the emotional distress recognized dates back before to modern era like in tort law we have assault and battery the physical harm is caused when battery takes place assault is merely emotional distress is fear of getting hurt this was recognized long back than modern era. Defamation law protects reputation, it does not require proof that there is some financial or physical injury caused to the plaintiff. The

[10] Bose and Soumitra," Cyber crooks blackmailing porn viewers with stolen data" (19 April 2020)

emotional distress is not only recognized in privacy tort but also in confidentiality torts. For instance I place my trust in my doctor, if that doctor or clinic reveals my medical report which is not defamatory or in other words 'false' but my real reports the doctor will still be liable as there is a breach of trust. There is no physical or emotional harm suffered by me but this breach of trust could cause embarrassment in the society or a feeling of anxiety in me. In Johnson v. West Virginia University Hospitals, Inc., the court held that a police officer could sue for emotional distress caused by the fear of contracting AIDS after being bitten by an AIDS patient. It was not required for the plaintiff to proof in this case that he has contacted AIDS but the fear of contracting AIDS was compensated. In the very same manner the fear of identity theft should be taken into account.

The Indian Approach

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("2011 DP Rules") in Rule 3 lists eight types of sensitive personal data which mentions physical, psychological and mental health conditions. Another statute applicable for data breach cases are Personal Data Protection Act (PDP Act) 2019. Under the 2011 Rules, body corporates are required to have a Privacy Policy, obtain prior consent for collection of personal data, have restrictions on data usage for lawful and necessary purposes and non-transferability of personal data. Therefore, there exists tortious remedies against private entities for any breach of sensitive personal data.

The Supreme Court in the Puttaswamy case[11] upheld that right to privacy is a fundamental right and infringement of that gives the right to individual to initiate legal proceedings in the court. However the two acts the DP rule of 2011 and PDP Act do not provide for vicarious liability of the employer arising out of the act or breach committed by the employee. For instance if a hospital leaks reports of its patient by any employee, the employer if provided that has complied to all the security measures the employer will not be held vicariously liable under these statutes.

[11] Justice KS Puttaswamy (Retd) and others vs Union of India and Other

The COVID-19 Impact

The pandemic has put the world at a position where everything is moving online. IT firms and other offices have given work from home to their employees. The courts are hearing cases on video calls and moving steps in the way of e-filing the hackers and cyber criminals have been active. A survey by Ernst and Young in 2018 titled Global Forensic Data Analytics Survey revealed that 60% of Indian companies were unaware of data privacy best practices such as General Data Protection Regulations (GDPR). According to the survey, only 31% felt that they were GDPR compliant

. During the COVID-19 lockdown, the notion of informational privacy as expressed in the *Puttaswamy* judgment assumes increased significance. Justice RF Nariman described informational privacy as "which does not deal with a person's body but deals with a person's mind, and therefore recognizes that an individual may have control over the dissemination of material that is personal to him". In the same judgement, Justice Dr DY Chandrachud held that "informational privacy is a facet of the right to privacy" and that the "dangers to privacy in an age of information can originate not only from the state but from non-state actors as well".

The pandemic is the perfect time for the sectors to reflect upon if the measures taken to protect data of its employees and users from third party are sufficient. The video call platform Zoom saw a boost of users in the pandemic as office meetings were held through the same after sometime it came to notice that credentials of thousands of zoom users are sold on the dark web in less than a rupee. Zoom CEO apologized to its users to fall short on the privacy measures. The pandemic resulted in showing the users a clearer face of the dark web and alarming the companies on the measures they have took and they need to take to prevent data breach in the near future.