NEED OF A MODEL DATA PROTECTION FOR THE RIGHTS OF MARGINALISED (WOMEN, LGBT COMMUNITY, DALITS, TRIBALS, ECONOMICALLY WEAKER SECTIONS, OTHER GROUPS)

Shifali Sethi
amity university uttar pradesh

ABSTRACT

Organizations of all types have data collection and increasing data collection always calls for higher data protection. There have been cases of data breaches by Cambridge Analytica (Nandi,2020) quite recently. It was a case where Cambridge Analytica used the information of people without their consent for political advertising. The companies trying to improve like Google, IBM, Amazon are discussed briefly. In this paper we attempt to explore- How to stop these data breaches? What measures should be taken for marginalized groups is the main aim of the research. The need for a model data protection for protecting the rights of marginalized will be largely looked upon.

KEY WORDS- data protection, data breaches, data protection bill, marginalized groups, data privacy.

INTRODUCTION

The Personal Data protection bill was introduced in Lok Sabha on 11th December 2019, by the minister of electronic and information technology, Mr. Ravi Shankar Prasad. We live in an age where we are the sum of data that we generate. Therefore, how our data is collected, stored, shared and used directly affects our daily lives. Meanwhile data we share mediates our relationship between government and private companies, the existence of a data protection law becomes necessary for the state to ensure that "the state acts like a model data controller that ensures both data security and more importantly respects citizens' privacy." (The Personal Data Protection Bill, 2019, 2020). The bill also calls for the establishment of a Data Protection Authority of India (DPAI) to regulate the misuse of data. Yet privacy advocates have raised concerns that the bill might be giving government the exemptions on processing even the sensitive personal data. For the same, bill is said to be "controversial". According to the bill, the government can keep tabs on private companies storing people's personal data, while government itself will have no restraints. Which also raised questions for the alleged snooping incidents reported by Google and Facebook earlier this year. The exemptions provided to the government can make them process even the sensitive personal data.

Data protection is one of the concerns of the society today as data happens to be the most important asset a company has at all times. Data protection is needed to minimize corruption, loss, or compromise. The importance of data protection keeps on increasing with the increase in amount of data that is stored and processed. The importance of data protection should trickle down to each section of the society and should help each section of the society equally. There are several disadvantaged sections of the society we call as marginalized, which means they have less control over their lives and provided with less resources. These marginalized sections include women, Dalits, LGBT community, tribal, and economically weaker sections. My study of data protection is confined to these marginalized groups and how they can be benefitted by the way of data protection.

The social empowerment of these marginalized groups through legislative routes can help them grow out of the distress they face throughout their lives. This can be the most important agenda for any society that wishes to flourish in the near future. However, this is possible only when government takes measures to ensure that the weaker sections are truly empowered. The Government of India seems to have taken steps to ensure the safety of such marginalize groups in past 4-5 years. Modi government has taken few miles to ensure greater protection for SC/ST's. For instance, speedy dial courts have been set up for redressal of offences and a new chapter has been added with regards to "Rights to victim and witnesses". Likewise, there have been efforts made for data privacy for such groups and that would help them a great deal in making their lives better.

OBJECTIVES

The objectives of this study are quite limited as the topic chosen is not vast and has recently been updated everywhere on the internet.

First objective is to find out what all challenges do people from marginalized sections face.

Second is to find out the reasons why people belonging to marginalized sections of the society need to be protected against the data breaches which happened due to unauthorized access to data by any third party.

Third, would be to compare the data of privileged sections with the marginalized ones.

Fourth objective would be to form and describe a model which brings down the number of data breaches and helps the underprivileged.

LITERATURE REVIEW

Needs are better understood when challenges are clearly highlighted. Challenges faced by different marginalized groups are explicitly explained to connect them with data protection needs. For needs to be fulfilled, a model is required which would keep a check on how data is being processed, for how long will it be held by the company, which all agencies would keep a record of the data being processed and what are the legitimate reasons for processing the data. One thing that should be kept in mind is no data fiduciary should be allowed to process data against the will of the data subject. Nobody in the world deserves to feel unsafe. Data protection bill was panned out for the same reasons but it ended up putting the entire world in dilemma as government will regulate which all companies can process the data but any government body can process even the sensitive personal data anytime. While data protection talked about, there are sections/communities/groups other than the general public in the society that are not given equal status and hence are exploited severely by bureaucrats. How will they be protected if the data remains unfolded in the hands of government. These groups include Dalits, women, LGBT community, economically weaker sections etc. The population of SC/STs stand around 16.6% of total population in India, there is no data yet given for LGBT identifying population in India while they constitute 3-5% of the total world population, and there are approximately 73 million people living in extreme poverty in India and this makes 5.5% of total population. These groups are as important for the society as the richer ones. Their privacy is as important as of any other person in the society who does not belong to any of these groups. For this, various steps have been taken to improvise the level of data protection.

Now is the time to understand how important it is to consider how biased internet access can affect the marginalized groups in the society. Taking the case of LGBT community, it is still difficult for them to decide with whom can they share their sexual orientation and think about the repercussions of the same. A privacy data breach of LGBT identifying person can have a profound impact on his/her life. This may include loss of relationships with family, loss of employment, loss of friendships and may even lead to physical or mental harm. They should have enough control over the data they share so that the data shared is not processed unnecessarily processed. Phones/mobile devices play a crucial role in the life of people belonging to LGBT community for it helps in connecting them with their community that will support and welcome them. Ipso-facto, they tend to be heavier users of mobile phones than their heterosexual counterparts. Access to technology has instilled in them a greater spirit to look for their community and become a part of it. Largely for the ones living in remote areas and think they are the only ones identified as LGBT have mobile phones as the only source to connect with people of their kind. By numbers we can examine how important it is for them to have data privacy.

LGBT tech shows that “81% of LGBT youth have searched for health information online, while just 46% of non-LGBT youth. It has also shown that 80% of LGBT youth participates as respondents in social networking sites while only 58% of the general public”. Adding to this, researchers say that health information is more surfed by Lesbians as they are overlooked and deprived of health services. The internet has not only offered life-saving information but much more. Wireless devices have helped LGBT community to connect them with the people in remote areas and provide all the support they need. This social connection covers the globe for everyone but can be of immense help in saving life of an LGBT individual. For all of the reasons stated above, data privacy is important for them. Any data breaches can harm them in the worst possible way. While data privacy is crucial for anybody over the internet, it is of life-saving importance for an LGBT identifying ones. Without proper data privacy, repercussions can be catastrophic. It is not just about data privacy issues they face but further occurring consequences of harassment, loss of jobs, loss of family relations, etc. Allowing people to have some amount of privacy in their life, helps them to grow out of the consequences they may face in future. (Stop.Think.Connect,2020)

Second comes Dalits, they are the most overlooked ones in the society and this can be witnessed in the real-life situations they face. For instance, these people are denied to even rent an apartment, if their better-off counterparts are the owners. Even if they are educated, they are pre-assumed by the people to be illiterate. For reasons they are always flooded with filth by the people, they are forced to move to places in villages, sometimes. The same consequences are faced by SC/STs and tribal. In order to control data breaches a company can shift from being centralized to decentralizing by blockchain method. Google and IBM have announced o work on their own blockchains, this decentralized social media is not far off now. Decentralizing the company would build trust of the users as blockchain method encrypts the private data of the consumer and it can only be unlocked when the user wishes to do so. When the data user wants to share more data, he will provide access to his friends or third parties to access the data. It does not matter what measures a company takes to protect the user’s data as long as it is satisfactory for the people associated with it. Decentralization, through the means of blockchain, is the future of data privacy and security.

Women need data protection law

Before I post on my Instagram profile, the first thing that comes to my mind is how it will be analysed by people. Not only this, but how it can be used by them without my permission. I might sound like a hypocrite for I also do things I discussed above. Although apps like Instagram and Snapchat (photo-based apps) notify the person if their content is being shared or screenshotted by other people. Today, while the need for data privacy has increased the expectations have reduced. An individual almost all the time is kept under surveillance in a public area; be it CCTV cameras or credit card swipes. The data stored online is much likely to be stored, shared and used by people who do not have direct access to it and hence, the data sharer can be targeted in many ways. There are several studies by experts which showcase how likely it is that impact on women is different than on men. To examine the privacy in public areas, there was a study conducted at university of Washington which says that women seemed to be more concerned than men. They were given a case where men and women were asked whether they will be comfortable if their images are recorded or being used as real-time display. A lot of men were comfortable with getting their images recorded than being used for real-time display. However, women did not agree for either of the two. This makes me believe that women are more concerned about their privacy. There is nothing obtrusive about the fact that an individual's profile is scanned for their information to provide them with individualised experience and the choices made by them are stored and used to observe and manipulate the data subject. The recent scandal of Cambridge Analytica set an example of how an individual's data can be harvested and used as a weapon against somebody, nudging companies to reform their data protection and privacy norms. Women of age group 18-49 are the most vulnerable with regards to internet marketing opportunities. For instance, a new yorker cited about iVillage that pregnant women update their information online and they are updated with a calendar which shows what will be happening inside her the consequent days and she is also directed to a group where the women with same calendar interact and can get support and advices related to their health. Now they are also urged to purchase items such as books from amazon, baby products from iVillage's iBaby etc. there have been times when you add things to your car and do not complete your purchase and after a few hours start receiving mails with sentimental messages like "your cart misses you" or you might come across advertisements related to your searches on google. If one compares internet marketing opportunities to coal mines, then sites dealing with women are mining diamonds. Data which is not regulated may pose threat to a lot of its data subjects. The number of women that shop online has increased, and they are exposed to consequences more than women. These online sites have targeted women for collection of information as they look after the pattern and spending habits of their households. Data store should be managed and controlled timely to protect women from being targeted.

Data breach is a huge problem that the world is facing at present. "The Privacy Rights Clearinghouse (2013) has witnessed more than 3500 separate reported breaches disclosing more than 600 million records containing Personally Identifiable Information since 2005." Sharing is seen as public good. To be a good corporate resident and to vanquish the digital lawbreakers, data security experts are educated that sharing data about breaks, the nature of assaults and effective procedures for managing assaults is something that acceptable corporate residents ought to do. In any case, since most data assets and the business capacities that they support are in private hands, data security experts are administered by the corporate culture, nearby information administration, laws applying to business exercises and the serious weights that exist with the business condition.

Sharing reduces criminal activity. Although there is little research concerning the deterrence value of sharing information about cyber-attacks, other research shows that some activities on the part of victims, like there are chances of less crimes taking place if the crime happening gets reported at the earliest. (Goldberg & Gold, 1980). It is contended that revealing digital wrongdoing, regardless of whether to industry gatherings or to the specialists would have the impact of diminishing crime. The mystery encompassing digital interruptions and the low likelihood of being found is more likely than not a factor in this sort of wrongdoing. Sharing the strategies used to relieve the assault. Moderation techniques, regardless of whether they square or mislead or dispense with the danger are regularly shared, yet without the data about how the risk was distinguished, such data is less valuable. Realizing how a risk was recognized uncovers when to utilize the strategy depicted to alleviate the assault. Moderation information without information on when to utilize it is substantially less helpful. There are many states that take steps to inform the data subject about the data breaches that have taken place (CLLA, 2011) and most of those individuals report the "three national credit reporting bureaus", but no need to report compromised accounts to the credit reporting bureaus and no structured way in which the accounts affected are marked, many merely being marked as "closed at customer request" (InfraGard). InfraGard is a platform shared by FBI and the private sector for providing information, sharing and analysis on a non-disclosure basis. Cleveland FBI field office created in 1996, headquarters adopted the program as a response to PDD 63 with local chapters linked with every FBI field office. The goal of program has been to directly involve the FBI in the protection of critical national infrastructure. There have been a lot of cases for why we need data protection and security.

RESEARCH METHODOLOGY

I have gathered information from the sources online. I have gone through various articles and journals that gave me knowledge of how data breaches happen and how they can be encountered. Although there were limited articles and journals that talked about data protection for rights of marginalized but the ones there clearly highlighted the idea and provided appropriate data for research. Most of the data is from the recent years i.e., 2017,2018 and 2019. This concept became more prominent after the 2018 scandal of Cambridge Analytica and that created awareness among people for why their data needs to be regulated and protected. The laws have been reconstituted and actions have been taken in December 2019 for the same.

FINDINGS

A global database of public data breaches called breach level index released latest findings unfolding that 945 breaches happened in 2018 which resulted in 4.5 billion data records being compromised. During first half of 2018, there were 291 data breaches recorded every second, 17,469 data breaches recorded every minute, 10,48,152 recorded per hour and 2,51,55,650 records are stolen or lost per day. The amount of missing, stolen or damaged records rose by 133 percent compared with the same timeframe in 2017, while the overall number of breaches decreased significantly during the same period, suggesting an improvement in the seriousness of each incident. According to breach level index there have been 15 billion data breach cases recorded till date since 2013. The largest percentage of data breaches were caused by outsiders i.e., 56%, there was decrease of 7% in the second half of 2017 and constitute 80% of stolen or lost data. Accidental losses are the second major type of data breaches. The data breaches due to accidental losses stand around 879 million which makes up 9% of the total breaches that took place. The total number of data breaches came down to half in 2018 as compared to 2017.

ANALYSIS AND INTERPRETATION

After doing in-depth study on the topic "Need of a model data protection for the rights of marginalized" I came across certain facts which I would like to produce here. The first fact that is one of the major concerns of the society and because the major share of marginalized is held by women that are yet considered a minority in a fast-moving world. "Women is nonetheless the targeted group that feel insecure in public areas and are overlooked by many. Then LGBTQ identifying people are the ones who acquire 3-5% of the total world population and any data breaches could jeopardize their career, jobs, relationships and what not. Dalits, being the community people supress a lot and that is evident from cases where they are denied even rental stays if they expose their true self. This makes me believe that data stored online of such people communities should be regulated timely. Recent case of George Floyd, which showcases racism is another major concern and provides a ground for why protection of marginalized people should be pondered over, and laws should be reconstituted.

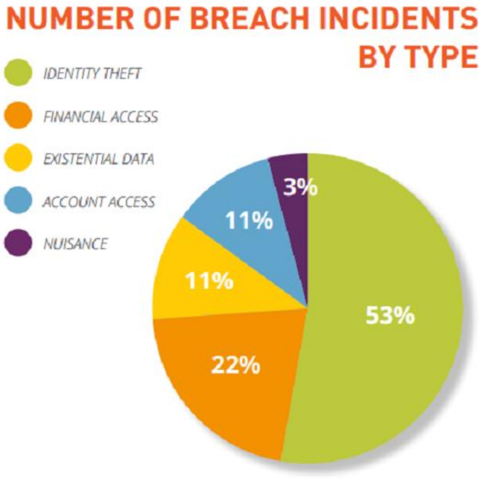

Figure. 1 shows number of data breaches by type wherein maximum number of breaches are due to identity thefts that is 53%.

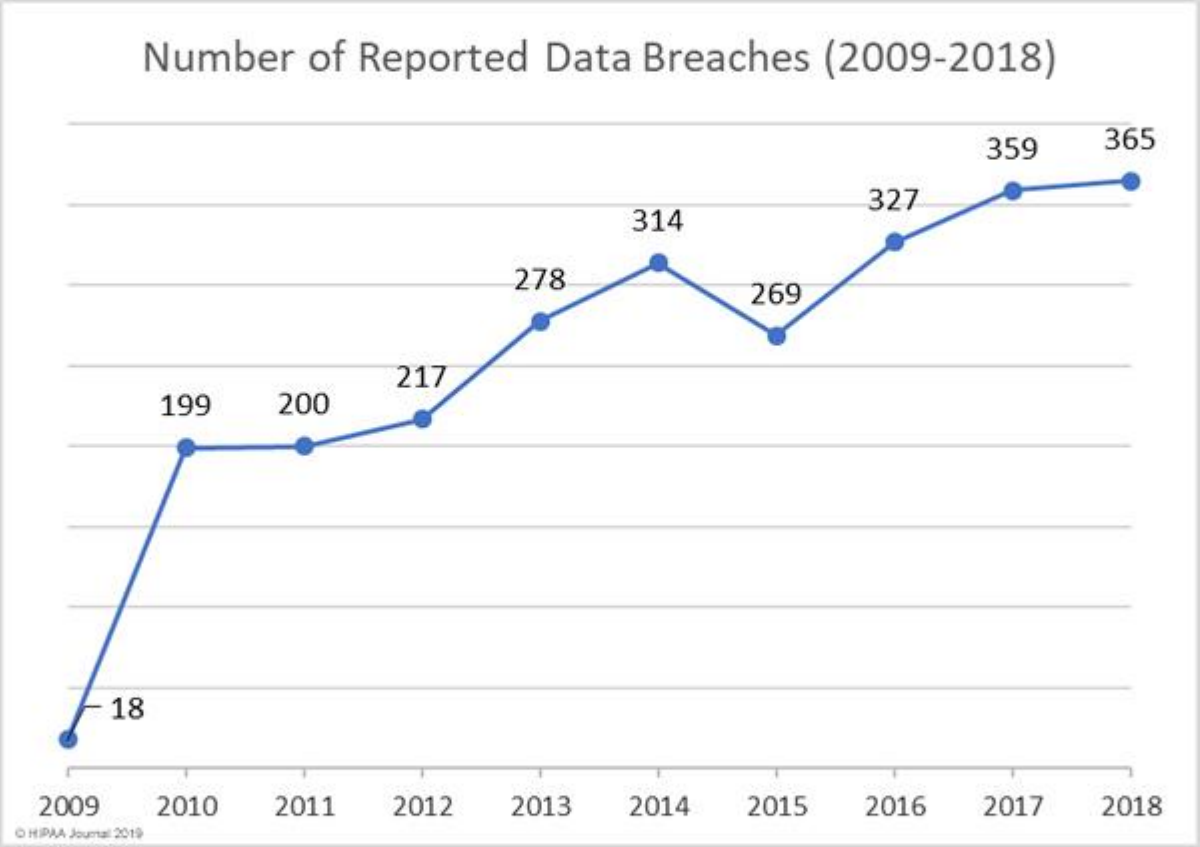

Figure 2: shows the number of data breaches that took place from 2009-2018. The graph clearly depicts the upward trend of data breaches which calls for increased data privacy.

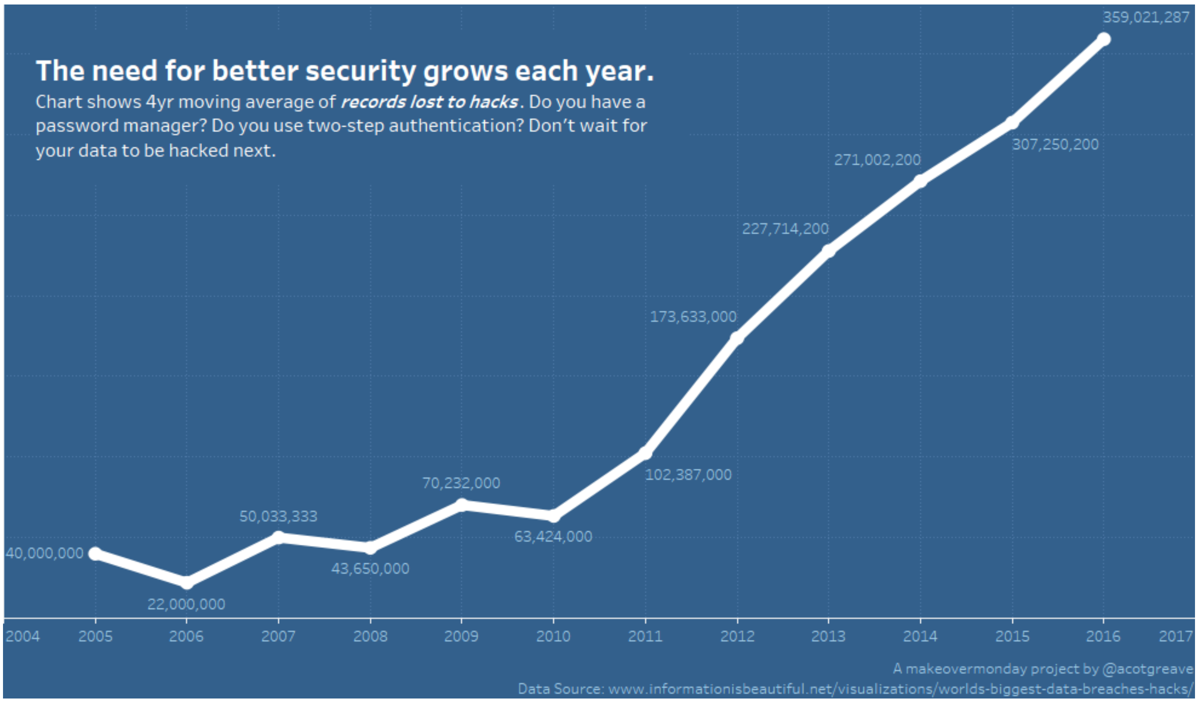

Figure. 3: shows how important it is to cater the data security needs because of increasing number of data breaches every year mostly happening due to identity thefts.

CONCLUSION

To sum up, data breaches is a known phenomenon in today's world, and it needs to be addressed at the earliest. The laws framed to address the problem are not appropriate as for government still has exemptions. The model needs to be fabricated in a way that it helps marginalized people. A system that deals with blockchains model where centralized companies are ordered to work as decentralized ones, where users have their personal data encrypted in a way that third party is only able to access the data when data subject allows. So that they gain the confidence of users and benefit the economy. The model should be structured in a way that it explains how the data should be secured, who all can have access to it and what all information they are allowed to process and lastly, what all consequences/ repercussions one may face if they do not adhere to the law. There should be a proper mechanism set up for surveillance for cyber intrusions taking place. Only then will there be a way we would be able to help people in need of data protection. Although it is required by everyone but for few it is a life-saving measure.

SUGGESTIONS AND RECOMMENDATIONS

The measures that companies can take to prevent data breaches are as follows:

The first and important measure would be to provide training on security awareness. Employees constitute an important part of any organization and training them on security awareness would serve a great deal. As against this, they can act as weak link in data breaches, and this may bring vulnerability. An effective training means educating the employees about data breaches, how they happen, how they can avoid it and they should be encouraged to report any such incidents. It is also important for them to know about the consequences of the same.

Second comes the investment in right technology. For every industry requires some measure for cybersecurity to protect personal data, it is important for these businesses to possess firewalls, intrusion detection and antivirus detection. Also, for a company to have good quality protection system, it is necessary that they look after the security risks which they might come across. Usage of encryption system thus is believed to be crucial to minimize vulnerability related to networks. Endpoint protector being one of the Data Loss Prevention solutions prevents data theft by enforced use of protection policies. It restricts the end users from passing the information to any other company/individual as well as blocks those with unauthorized access. Digital security has become a need for not only big companies but also for small or medium sized firms.

Third suggestion is to stick to data protection guidelines. There are agencies affecting a few countries, which regulate data protection such as GDPR (General Data Protection Regulation) and California Consumer Privacy Act (CCPA). When any organization decides to protect its content to comply with data protection regulations, it has lesser chances of data breach and more chances of avoiding penalties. There are also different agencies set up for some selective industries to see if the regulations are being followed. For instance, for companies which use credit card information, PCI DSS (Payment Card Industry Data Security Standard) is the agency which regulates how data will be processed and who all can access the data. Similarly, HIPAA (Health Insurance Portability and Accountability Act) regulates data within health centres.

Regular vulnerability assessment is another process which involves identification, classification and prioritization of security threats to assess the risk they pose to the organization. The security audits act as a checklist and help in data protection in a better manner.

There are many companies that do not have data breach response plan yet. However, these help in building public and employee trust and help in limiting damages. GDPR in its regulations has highlighted the importance of having a data breach response plan. As one of the regulations commands to take actions against the data breach within 72 hours of identifying it. It includes gathering all the relevant information, holding the associated regulator accountable and informing the data subject.

These are the few ways how data privacy and protection can be maintained for not only marginalized but for the society.

REFERENCES

PRS India. 2020. The Personal Data Protection Bill, 2019. [online] Available at: https://www.prsindia.org/billtrack/personal-data-protection-bill-2019

[Accessed 15 June 2020].

*Search Data Backup. 2020. What Is Data Protection and Why Is It Important?
Definition from Whatis.Com. [online] Available
at: https://searchdatabackup.techtarget.com/definition/data-protection*

[Accessed 15 June 2020].

2020. [online] Available at: https://www.narendramodi.in/empowering-the-marginalised-through-the-legislative-route-19-march-2019-544128

[Accessed 15 June 2020].

*India, T., 2020. The Problems of Marginalized Groups In India - Academike.
[online] Academike. Available at: https://www.lawctopus.com/academike/problems-marginalized-groups-india/*

[Accessed 15 June 2020].

Bing.com. 2020. Lgbt Population India - Bing. [online] Available at: https://www.bing.com/searchq=lgbt+population+india&qs=AS&pq=lgbt+popu&sk=AS2&sc=89&cvid=56E470A8152F440C9F5F508C6633E002&FORM=QBRE&sp=3&ghc=1

[Accessed 16 June 2020].

Stopthinkconnect.org. 2020. Stop.Think.Connect.. [online] Available at: https://stopthinkconnect.org/blog/data-privacy-is-crucial-for-the-lgbt-community

[Accessed 16 June 2020].

Forbes. 2020. What Can We Do to Solve The Data Breach Problem?. [online] Available at: https://www.forbes.com/sites/quora/2018/04/20/what-can-we-do-to-solve-the-data-breach-problem/#290e93c47fee

[Accessed 16 June 2020]

Uniassignment.com. 2020. Data Breaches Are A Huge Problem Information Technology Essay. [online] Available at: https://www.uniassignment.com/essay-samples/information-technology/data-breaches-are-a-huge-problem-information-technology-essay.php [Accessed 16 June 2020].

Nandi, S., 2020. The Importance Of Data Protection | Techno FAQ. [online] Techno FAQ. Available at: https://technofaq.org/posts/2019/02/the-importance-of-data-protection/

[Accessed 17 June 2020].

Hindustan Times. 2020. How Privacy As A Fundamental Right Brings New Hope To India's Marginalized. [online] Available at: https://www.hindustantimes.com/analysis/how-privacy-as-a-fundamental-right-brings-new-hope-to-india-s-marginalised/story-3hNuzNyUkK9LtYD8CjyNpI.html

[Accessed 17 June 2020].
ACCESS NOW, 2019. Honoring Fred Korematsu: Why data protection matters for marginalized communities. Available at: https://www.accessnow.org/honoring-fred-korematsu-why-data-protection-matters-for-marginalized-communities/

[Accessed 19 June 2020].

Berecki, B., 2019. 5 Best Practices for Data Breach Prevention in 2019. [Blog] endpoint protector, Available at: https://www.endpointprotector.com/blog/5-best-practices-for-data-breach-prevention-in-2019/

[Accessed 19 June 2020].