Analysis of Recent Privacy and Security Breaches

Tanmaya Nanda
North Carolina State University
tnanda@ncsu.edu

Amit Mandliya
North Carolina State University
amandli@ncsu.edu

Dyuti De
North Carolina State University
dde@ncsu.edu

ABSTRACT

Online data are being produced in increasing amounts due to extensive use of Internet, IoT devices and generating previously physical data in digital form. These data are stored in diverse formats. Practitioners and researchers can be benefited significantly if these massive heterogeneous data could be integrated and made accessible. But often data can reveal user identity and sensitive information that can lead to loss of privacy which in turn leads to loss of trust, reputation and user base of a company/government. In this paper, we have provided a state of the art review of the privacy threats by studying the recent data breaches. According to our study, loss of user privacy leads to great loss of reputation and monetary value of any institution We have tried to understand the perspective from the victim's point of view for the incidents. We have provided few measures in relation to the incidents through which it can be avoided in future.

KEYWORDS

Privacy, Data Breaches, User Survey, Equifax Data Breach, Cambridge Analytica Data Breach, Aadhaar Data Breach

1 INTRODUCTION

In today's time, the frequency of security breaches has increased significantly. This is expected as users and their data are growing at an alarming rate. Although companies have found new and robust technology to tackle the flow of data traffic and successfully managed to preserve them, the question arises whether they have invested as much to ensure privacy? In our breadth-wide study, we have analyzes several recent security and privacy breaches and attacks that have affected regular users of the Internet. The study of these recent attacks followed by a more in-depth analysis as to what led to those attacks, what were the vulnerabilities and the aftermath. Our study comprise of a full description of attacks, the loopholes that led to such breaches and the impact it had on users. Through surveys, we have tried to obtain the user's side of story on how these attacks impacted them and if their grievances were taken care of. We will conclude by summarizing the survey results and understanding user perspective.

2 MOTIVATION

The motivation behind this project is to analyze the recent data breaches in depth and understand the consequences faced by the victims of those breaches. There is a massive boom in use of the Internet, applications and technical devices over the past decade. And with that the data breaches are becoming stealthier and more malicious than ever before. Many threats are programmed to remain unnoticed for as long as possible. These are unleashed at an opportune time chosen to inflict maximum damage [1]. The modern applications have a long list of terms and conditions which users do not read before using and often don't understand how their data can be extracted and used and for harmful purposes. Companies tend to not provide proper protection mechanisms and even after it is a victim of the data breach where confidential customer information is leaked, they do not bother to safeguard or reimburse the customers. Every year a large number of users are falling victims to these breaches. The main motivation of our project is to conduct surveys and analyze the trends of recent breaches to protect the general users from getting exploited further in future. We want to come up with approaches and preventive measures that can be followed by users and companies to restricted data leaks and breaches. Finally, we want to make a conclusion on what steps companies can take in order to retain customer faith and good brand value after a data breach takes place. We take the following data breaches into consideration.

2.1 Background

2.1.1 Aadhaar Data Breach. Aadhaar is an Indian Government program under which residents of India can get a unique identification number by the Unique Identification Authority of India (UIDAI). As part of the program, the government collects biometric and demographic data from the people. Although getting an Aadhaar card is voluntary, some of the basic services provided by the government have been mandatorily attached with Aadhaar cards. Around 1 billion users' personal data have been stored as part of the program. On January 4, 2018, The Tribune, a newspaper in India, investigated and revealed that the Aadhaar details of people can be obtained in as low as $7 and in 10 minutes. And in another $5, Aadhaar cards of anyone can be printed online illegally. Government hired village-level enterprise (VLE) operators to facilitate the government in making Aadhaar cards for the people. Later, the task was given to post offices and banks. However, VLEs got illegal access to the data of the people and some of them lead to security breach.

2.1.2 Equifax Data Breach. The Equifax breach led to data leak of nearly 143 million U.S. consumers. The data leaked were names, SSNs, Date of Births, Addresses and Driving License numbers. The attack happened on 7th September 2017. On March 9, 2017, an internal email notification was sent to Equifax administrators directing them to apply an Apache software patch. Equifax's information security department ran scans on March 15, 2017 that were meant to identify systems that were vulnerable to the Apache Struts issue, but the scans did not identify the vulnerability. Not taking enough actions on this, the vulnerability was left unpatched until July 29, 2017 when Equifax's information security department discovered "suspicious network traffic" associated with its online dispute portal and applied the Apache patch. However, it was too late as millions of personal data remained exposed for several months. Unfortunately, some of the measures taken by Equifax in the aftermath of the breach, turned out to be a disaster. Equifax created a separate domain—equifaxsecurity2017.com— for consumers to find out if their information was compromised in the breach. This caused the site to be flagged as a phishing threat by browsers. The new domain was easier to imitate and confuse people. The Equifax Twitter account accidentally tweeted a link to the spoofed site. Consumers who contacted Equifax in the immediate wake of the breach to freeze their credit were given PINs that corresponded to the date and time of the freeze, making them easier to guess. Equifax advised people to sign up for their credit monitoring service TrustedID Premiere, but in doing so consumers agreed to terms of use with a mandatory arbitration clause which barred them to take class-action lawsuits against Equifax related to this protection. After public outcry that Equifax was forcing consumers to give up their right to sue, the company issued a press release explaining that the arbitration clause would not apply to claims arising from the security breach.

2.1.3 Facebook Data Breach. Cambridge Analytica is a political data firm that was hired by President Trump's 2016 election campaign. They gained access to private information on more than 80 million[20]. They used user profile data from Facebook to manipulate political results without the consent of Faceook or the users. The firm offered tools that could identify the personalities of American voters and influence their behavior to manipulate the voting tendencies of American Population. Cambridge Analytica used that harvested data to make about 30 million "psychographic" profiles of voters in total. Facebook had not previously disclosed how many accounts had been harvested by Cambridge Analytica, the firm connected to the Trump campaign. Facebook's problems stretched back before the reports about Cambridge Analytica, to earlier investigations into how Russian actors infiltrated the platform by placing ads and posts to influence the 2016 election. Being an extensively used application all over the world, Facebook has high density of user data that could lead to dangerous consequences if misused.

3 RELATED WORK

A lot a work has been laid out in the field of analyzing data breaches and the privacy risks that comes with it. Privacy and security of Big Data has gained momentum in the research community, also due to emerging technologies like Cloud Computing, analytics engines and social networks. An overview of state-of-the-art research issues and achievements in the field of privacy and security of big data has been laid out while highlighting open problems and actual research trends, and drawing novel research directions in this field[1]. In

another paper, the potential relationships among categories of personal information, beliefs about direct marketing, situational characteristics, specific privacy concerns, and consumers' direct marketing shopping habits has been examined. The findings indicate that public policy and self-regulatory efforts to alleviate consumer privacy concerns should provide consumers with more control over the initial gathering and subsequent dissemination of personal information. Such efforts must also consider the type of information sought, because consumer concern and willingness to provide marketers with personal data vary dramatically by information type [2]. There are many works based on concerning consequences of the recent data breaches, their analysis and how they could have been avoided [3][4][5].

Equifax being one of main data breaches of this decade that has been analyzed by us has been studied deeply [3][6][8]. The user perspective has also been gathered and the authors conclude that enough precautions has not been taken [7]. The Aadhaar card data breach is considerably lesser known, but there is ongoing research about how privacy leaks are happening[9][10]. Our research is unique in terms of covering the user perspective and understanding people's decreasing trust on government, but several research papers compare and contrast India's unique identification system with other countries like US, Europe and China[11][12]. Cambridge Analytica Facebook Data breach has fueled growing interest in the debate over technology's societal impact and risks to citizens' privacy and well-being and increased awareness among the general consumers world wide from sharing personal data on Internet[13][14]. There has been research to understand to user's perspective towards growing privacy concerns over social media[16], but surveying victims about awareness, impact and company reputation remains unique to our work.

4 EXPERIMENTAL DESIGN

A google form https://forms.gle/ejTraPMGp4u2chdV8 has been designed to understand the general privacy concerns and the victims of given data breaches are also asked the questions specific data breaches' questions. Answers from users have been collected via the online survey for the questions below to understand the impact of the data breach on the users. We have successfully gathered a total of 109 participants from varying demographic. To recruit the participants we looked at relevant Reddit threads and Facebook groups where privacy concerns are being discussed by the victims or users affected by these data breaches. User who participated in the study have a diverse range of profession including - university students, academicians, businessmen, etc. Users are expected to answer in one of the following categories: Strongly Agree, Agree, Neutral, Disagree and Strongly Disagree or ratings and options if necessary.

4.0.1 General Privacy Evaluation.

- Consumers' privacy is at risk if they are sharing personal information online
- What information would you be comfortable in sharing online?
- Do popular private Companies like Amazon, Flipkart keep your data secure from getting hacked?

4.0.2 Aadhaar Data Breach.

- Government took strong measures to mitigate the risk in future?
- Government should compulsorily collect sensitive information like Bio-metric data of each individual?
- Government has the will power and resources to keep the collected personal and sensitive data safe from malicious hackers?
- Did your trust in the Government decrease after the incident?

4.0.3 Equifax data breach.

- Have you been a victim of following breach?
- What type of breach? Credit card, bank fraud, social network
- What measures did your company take?
- What measures did you take?
- Did you remove your membership from organization/moved to another organization?
- Did you sue the owners?
- Did you stop giving personal details on sites?

4.0.4 Facebook Data Breach.

- Are you aware of the kind of data that was leaked during the Facebook Data Breach. Eg. messages, pubic profiles, private posts etc.

- Are you comfortable with sharing profile data for voting purposes?
- Do you think the Facebook took enough measures to restore user privacy?
- How much risk do you think a Facebook data leakage can pose for you or other user?
- How did Cambridge Analytica data breach affect your Facebook usage?
- Do you feel Facebook has determined your voting decisions in any form during American Elections?
- On a scale of 5, How much has it damaged company reputation and user trust from your perspective?

Based on the above questions, we will evaluate the trends of how user's trust has changed in the aftermath of the studied data breaches. We will study if these attacks led to other fraudulent activities related to the personal information leak or whether users are comfortable sharing information with these companies or government in future. We will also analyze this based on user's demographic to understand any prevalent biases.

5 EVALUATIONS

We have gathered the survey results and the answers lead to some interesting insights. A total of 109 users participated in the study.

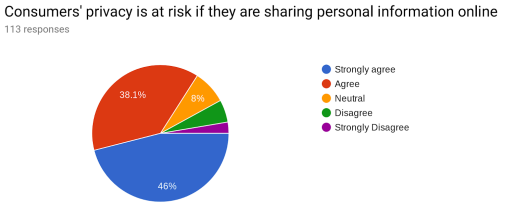

Figure 1: Sharing personal information online

80% people of age below 30 years think that Consumer's privacy is at risk when they are sharing information online, while the people of age above 30 years think more so. Most of the people are neutral to Online companies like Amazon, Flipkart keep their data safe from hacking. But people do have an opinion on kind of data they want to share online and it is evident from the chart below that users are least comfortable with sharing bank details though online payment gateways are becoming popular each day.

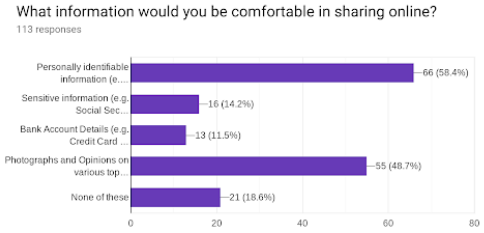

Figure 2: Types of Information users are comfortable sharing

5.1 Results of Data Breaches

5.1.1 Aadhaar Data Breach. We identified 21 victims of the incident who participated in our survey. Here is the chart showing the distribution of users who believe that the Indian government took strong measures to mitigate the risk in future. Surprisingly only 10% agreed with the statement. Most of the people feel that Government did not take strong measures to mitigate the risks in future.

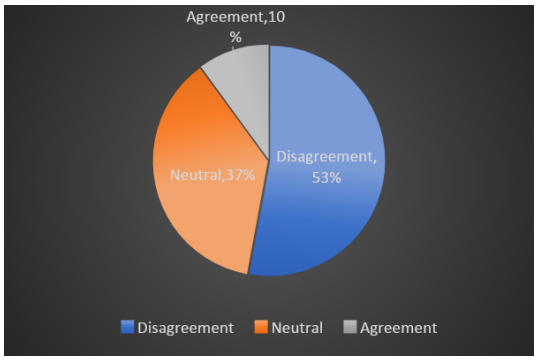

Figure 3: Distribution of user believing government took strong measures to mitigate the risk in future

Here is another chart which shows users' responses when asked if they think that Government has the resources to keep their data safe, and a large portion of users believed that government did have the proper resources to keep their data safe.

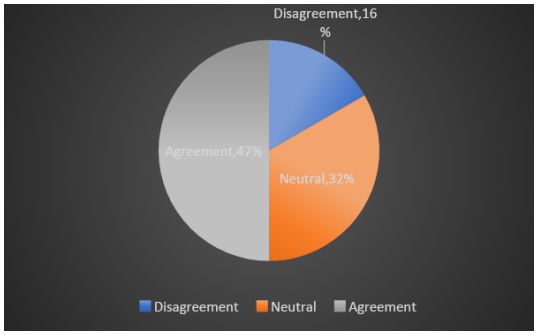

Figure 4: Distribution of users thinking that government has the resources to keep the data safe

Here is another chart showing the people's responses to if their trust decreased in the Government after the incident. As is the usual case with any privacy breach, the most of the users' trust on the Government decreased after the incident.

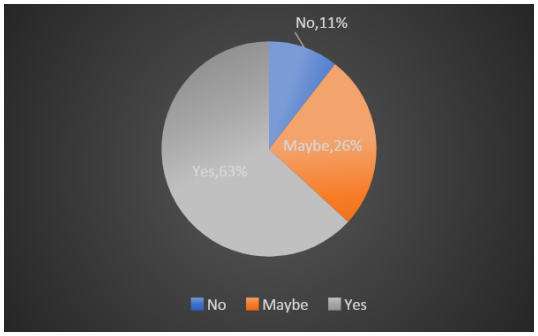

Figure 5: Has the user's trust decreased in the Government after that incident

Even though most of the people's trust decreased on the Government after the breach, surprisingly, here is another chart which shows that people's response when asked, whether the government should collect the bio-metric and demographic data from the citizens of the country. The chart below clearly indicates that most of the people still feel that it is important for the country to have a database of the citizens which records all the identifiable information of the people. This also indicates that people are aware that, having an Aadhaar based identification mechanism is an important backbone of the country.

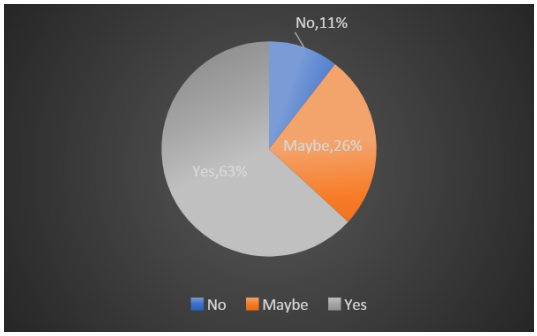

Figure 6: Government should collect the biometric and demographic data from the citizens of the country

The above charts show that most of the people believes that government has the resources to keep users' data safe, however, very few think that it actually took strong steps to mitigate the risk. This clearly states the lack of willpower to take strong steps to deal with such critical data of the citizen of the country.

5.1.2 Equifax Data Breach. We surveyed 21 people identified as Equifax victims, asking them about how they feel about sharing information online.

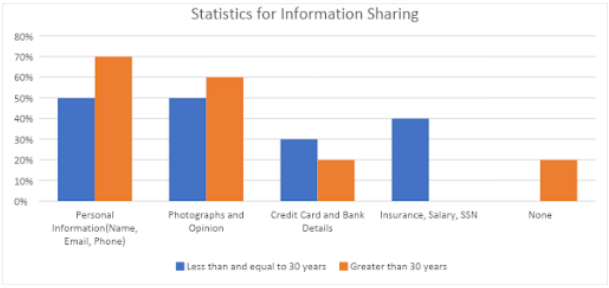

Figure 7: Statistics for online information sharing

- This age group above 30 seems to have a more fundamental approach towards information such as Credit card details, Bank details, Insurance, Salary and SSN. Only 20% is comfortable in sharing bank and credit information.
- None of the participants in our study in age group greater than 30 feels comfortable in sharing Insurance and SSN details. This points to an observation that, people in this age group become more concerned about health insurance frauds and misuse of SSN.

- 20% of older age group feel that none of this information should be shared.
- 70% of the older age group feel most comfortable in sharing Name, Email and Phone. The age group below 30 is only 50% comfortable here, which shows that youth is more aware of the risks of sharing this information online.
- 60% feel are comfortable in sharing opinion and photographs on social media. This number is more than the counterpart age-group. One can say the youth is more concerned about social media.
- It can be observed that the youth age group has pragmatic approach to information sharing.

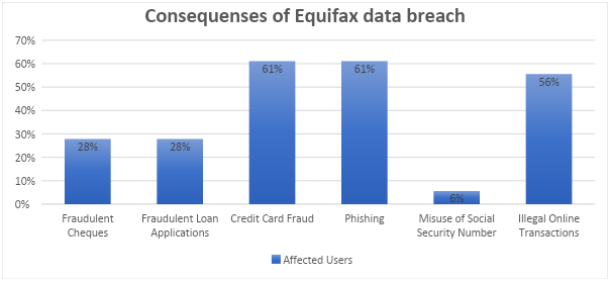

Figure 8: Consequenses of Equifax data breach

Following are the findings as to what consequences took place due to the breach. The breach of personal data such as Credit card, SSN and Addresses easily leads to more problems such as identity theft, fraudulent loan applications and illegal online transactions. 61% fell victim to Credit card frauds. This happened before Equifax took enough measures to freeze the credit cards. Another 61% received suspicious emails that pointed to Phishing scams. As for anyone, it is hard to detect a phishing scam until one actually becomes a victim. 28% of victims found out there were fraudulent loan applications under their name. Loan can be obtained from someone's name, address, credit history and SSN. As for Equifax breach of personal data, it was an obvious consequence. Another 28% were victims of fraudulent cheques and a few of them (6%) registered cases of misuse of SSN. All of these people were victims of identity theft. 56% fell victims to Illegal Online Transactions. Equifax's cash settlement did not take into account the amount of money victims lost through illegal online transactions, identity theft and phishing scams.

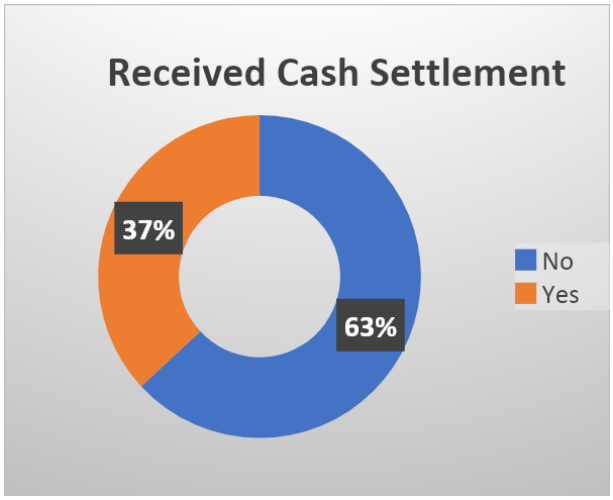

Figure 9: Received cash settlements

Even though almost 90% fell victim to payment frauds, only 37% received cash settlement as of today. Only 26% of the victims sued Equifax which is much less than the number of participants who were victim to illegal payment frauds and identity theft. A majority of them did as much as withdrawing accounts from Equifax.

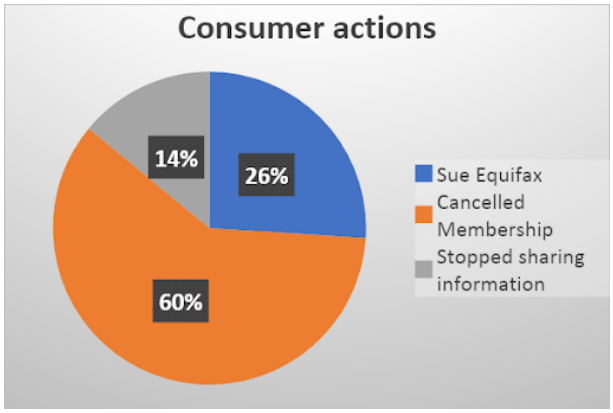

Figure 10: Consumer actions

5.1.3 Facebook Data Breach. We surveyed the 22 users about how their trust and usage of Facebook was affected as a result of Cambridge Data Breach. Most of the users believed Facebook did not take enough measures to restore user privacy.

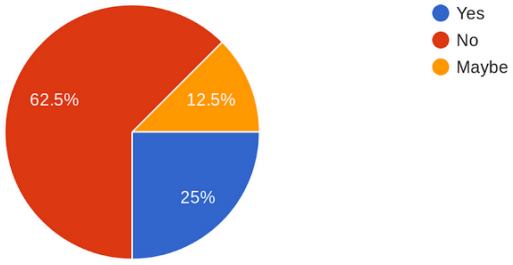

Figure 11: Measures taken by Facebook

50% users did not think that the Cambridge Analytica Data breach did not affect the company's reputation and the rest 75% users were neutral. Also the Facebook usage of most of the users remain unchanged but when we divide the users based on their age, we find a pattern that the younger people are more fundamentalists. The below chart shows that the trust, usage and reputation for Facebook as a company has decreased more among the young users aged below 30.

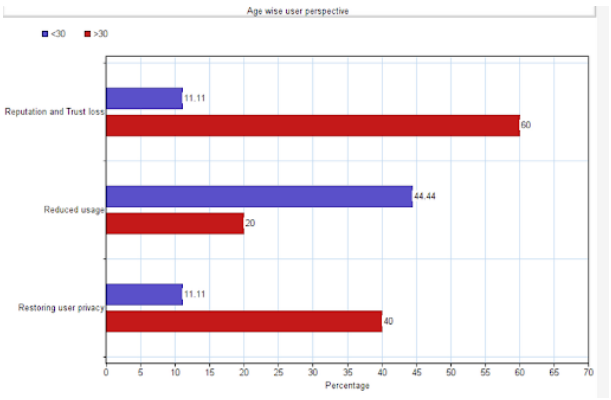

Figure 12: Age wise reputation loss

Another perspective that has been revealed by the survey is related to how the users feel about their profile data being used for voting purposes. 66% of the users feel that the profile data that is shared online can be pose high risks for themselves and other users.

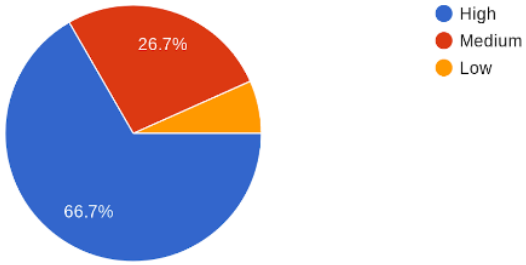

Figure 13: Risk in data leaked

Among the victims affected by the Data Breach, around 50% felt that they were aware of the kind of data that was leaked and most among them were not comfortable sharing their profile data for voting purposes. Yet 80% of them consciously felt that their voting decisions could have been manipulated by Cambridge Analytica using targeted content and advertisement. There was significantly high amount of people who thought their decisions were being manipulated in this group compared to the people who did not have awareness of the kind of Data that was being leaked.

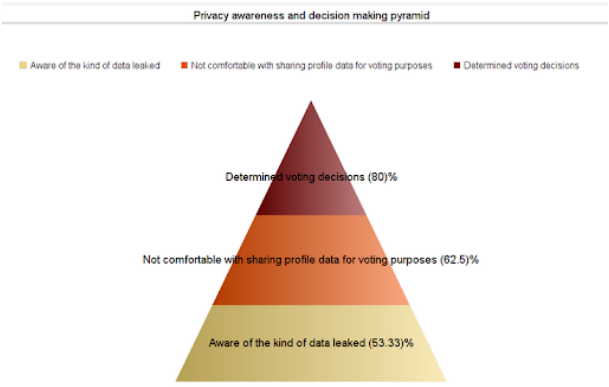

Figure 14: Awareness of data breach and manipulation inference

Though these charts covers a broad spectrum of perspective, they fail to cover the unconscious biases that would have significantly affected victims of Cambridge Data Breach.

6 DISCUSSION

6.0.1 Aadhaar card Data Breach. A few measures worth noting for the security of the Aadhaar database are:

Stricter policies over the database breaches – Indian Government should have more strict policies for the data access and protection, the government is coming up with data protection bill, but it has still not passed in the parliament. Secure third parties with API access to the database - Aadhaar data is linked with basic schemes like issuing of bank accounts, subsidiary schemes, authentication for buying mobile sim cards. The third-party cases should be more secure and fine grain access control should take place over who is allowed to access what portion of information. This will help save the data breach from the expanded private sector use of Aadhaar that has already been allowed by the government. One of the measure that was proposed in media was: Rather than having a software installed on the machines of private enrolment operators, a web based mechanism should have been adopted where the enrolment software would be installed on the UIDAI's servers and enrolment agencies would login from there.

6.0.2 Equifax Data Breach. Studying the Equifax breach, certain measures could have entirely prevented such a breach. In short: it's all in the code!

(1) Data vaults: Where Equifax failed was when attackers got inside the system, they found these data to be exposed in plaintext. Supreme security standards must follow layers of security measures. Data must be secure as if they are protected inside a vault.
(2) Network vulnerability: Systems that have backend databases must be safely guarded in virtual private subnets, such that even though attackers enter the application, the data must be in different networks that will only not allow requests from unknown IPs. [21]
(3) Regression and Penetration test suits must cover maximum code coverage to check for security lapses in the code. Common Vulnerabilities and Exposures can be tracked on mitre.org. [22]
(4) Configuration management and DevOps tools that the application must use to handle release dependency. [23]
(5) Give consumers more control on what they would want to share like credit card details, Insurance policies details or SSNs.
(6) Consumers must have free and easy access to their credit information, and control over when and how that information is disclosed. An idea is to give users an interface where they can remove the data, they have previously shared. This removes data from server as well.
(7) Companies collecting consumers' personal data must establish effective safeguards, including requirements for prompt disclosure of any data breach.
(8) Experts suggest there's no need to collect social security numbers, one may use other measures to identify users. [24]
(9) Credit reporting agencies should change the default on access to credit reports by third parties. Instead of the current setting, which allows virtually anyone to pull someone's credit report, credit reporting agencies should establish a credit freeze for all disclosures, with free and easy access for consumers who wish to disclose their report for a specific purpose. [25]

6.0.3 Facebook Data Breach. While Facebook said that most users only had their public profile and a few other pieces of data disclosed to Cambridge Analytica, the company did not know which users had more significant information, such as private status messages or wall posts. It also mentioned that a small number of people who logged into an app called 'This Is Your Digital Life' also shared their own News Feed, timeline, posts, and messages, which may have included posts and messages from others which can result to affect higher number of user than tracked officially[17]. Facebook begun to notify users who were affected by the Cambridge Analytica data breach and released a detailed document stating all the measures taken by the company to restore user trust and prevent future similar data breaches [18][19]. Though the breach happened due to a third party application, a few steps could be taken by Facebook to protect its users.

Any new application, code or advertisement etc can be verified by Facebook before its upload or push to production that is using Facebook user data. There are a few specific ways blockchain could alleviate the situation[19]. In a blockchain solution, users would be the primary owners of their information, and they would grant access to which parties can access their data. This practice is already being used in the medical industry with MedicalChain and EncrypGen[20]. Blockchain being a chain of blocks, everything is recorded and stored—a principle lending to immutability. This means that every interaction with the system can be tracked

to its deepest origins. This would have helped Facebook detect where the harvested information was going.

7 CONCLUSION

We evaluated the survey results of common users and victims and we can conclude that privacy concerns are an important factor for any consumer and any such data breach poses high risk of losing people's trust from the government, company or any other organization responsible behind these attacks. We have broadly studied the measures that can be followed in the future to prevent such data breaches but as we know, most of the data breaches could not be predicted on time. Thus it is important to deal with privacy issues with utmost priority and efficacy.

8 FUTURE WORK

Some of the major limitations that we faced during our project involved finding the victims who were consciously aware that they were affected by the data breaches that we surveyed for. In our future scope, we would like to recruit more participants in our survey to provide more in-depth insights and reflect patterns of the actual population demographic who were impacted by these data breaches. We would also like to conduct face to face interviews to understand the users' perspective in depth and conduct a semi-structured survey.

9 INDIVIDUAL CONTRIBUTION

As part of this study, all of us sat together and decided the plan of study. Post that, each one of us came up with one recent privacy breach incident and did a study and analysis on the same: Tanmaya - Equifax Data Breach, Amit - Aadhaar Data Breach, and, Dyuti - Facebook Data Breach For the documentation part, each one of us has written about the evaluation and analysis of breach that we studied. And the common sections were divided equally among us.

10 REFERENCES

[1] Alfredo Cuzzocrea. 2014. Privacy and Security of Big Data: Current Challenges and Future Research Perspectives. In Proceedings of the First International Workshop on Privacy and Secuirty of Big Data (PSBD '14). ACM, New York, NY, USA, 45-47. DOI=http://dx.doi.org/10.1145/2663715.2669614

[2] Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. Journal of Public Policy Marketing, 19(1), 27–41.

[3] Selena Larson. 2017. The hacks that left us exposed in 2017. CNN News USA.

[4] Devon Milkovich. 2019. 15 Alarming Cyber Security Facts and Stats https://www.cybintsolutions.com/cyber-security-facts-stats/

[5] Cynthia Dwork,Adam Smith,Thomas Steinke,and Jonathan Ullman. 2016. Exposed! A Survey of Attackson Private Data 10.1146/annurev-statistics-060116-054123.

[6] Alfred Ng. 2018 How the Equifax hack happened, and what still needs to be done

[7] Yixin Zou and Florian Schaub. 2018. Concern But No Action: Consumers' Reactions to the Equifax Data Breach. In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18). ACM, New York, NY, USA, Paper LBW506, 6 pages.

[8] Gressin, Seena. "The equifax data breach: What to do." US Federal Trade Commission, as viewed Oct 1 (2017).

[9] Raju, Raja Siddharth, Sukhdev Singh, and Kiran Khatter. "Aadhaar Card: Challenges and Impact on Digital Transformation." arXiv preprint arXiv:1708.05117 (2017).

[10] Mali, Nidhi Vij, and Martha A. Avila-Maravilla. "Convergence or Conflict?: Digital Identities vs. Citizenship Rights: Case Study of Unique Identification Number, Aadhaar, in India." Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance. ACM, 2018.

[11] Dixon, Pam. "A Failure to "Do No Harm"–India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the US." Health and technology 7.4 (2017): 539-567.

[12] Shahin, Saif, and Pei Zheng. "Big data and the illusion of choice: Comparing the evolution of India's aadhaar and China's social credit system as technosocial discourses." Social Science Computer Review (2018): 0894439318789343.

[13] M. Kosinski et al., "Manifestations of User Personality in Website Choice and Behavior on Online Social Networks", Machine Learning, vol. 95, no. 3, pp. 357-380, 2014.

[14] Pinchot, Jamie L., and Karen L. Paullet. "What's in your profile? Mapping Facebook profile data to personal security questions." Issues in Information Systems 13.1 (2012): 284-293.
[15] Gagneja, Kanwalinderjit Kaur. "Global perspective of security breaches in facebook." Proceedings of the International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2014.
[16] Hossain, Al Amin, and Weining Zhang. "Privacy and security concern of online social networks from user perspective." 2015 International Conference on Information Systems Security and Privacy (ICISSP). IEEE, 2015.
[17] Robinson Meyer. "My Facebook Was Breached by Cambridge Analytica. Was Yours?" The Atlantic,April 10, 2018
[18] "Facebook Sends Privacy Alerts to Users Affected by Data Breach" October 2018
[19] David Petersson. "How Facebook's 50m file leak could have been avoided" Hackernoon. March 2018
[20] Akarca, D., et al. "Blockchain Secured Electronic Health Records: Patient Rights, Privacy and Cybersecurity." 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT). IEEE, 2019.
[21] Glenn, Ashton. "Equifax: Anatomy of a Security Breach." (2018).
[22] "What Could Have Prevented Equifax's Security Failure". Atlantic BT. July 2018
[23] Ed Price. "The Equifax fallout: How organizations can prevent data breaches". August 2019
[24] "Equifax Data Breach". Epic.org.
[25] Ted Ringrose. "The Equifax Breach: What happened, the bungled response and some observations". October 2017