

## Effect of Data Breaching on Socio-economic Condition of Countries from Social Networking Sites

Nitin Sharma<sup>1</sup>

Available online at: [www.xournals.com](http://www.xournals.com)

Received 24<sup>th</sup> January 2018 | Revised 28<sup>th</sup> April 2018 | Accepted 21<sup>st</sup> May 2018

### Abstract:

*Data breaching is defined as any instance in which there is an unauthorized release or access of personal information or other information not suitable for public release. It is a security incident in which sensitive, protected or confidential data is imitated, transmitted, viewed, stolen or used by an individual unauthorized to do so. Data breach can cause a massive impact on social and economic condition of any country. Drawing upon Cambridge Analytica as a case study, a countries election is the spine of democracy, once it gets jeopardize the very essence of justice and equality gets hampered. The forensic application is helpful in determining whether the incident has occurred or not as well the one who involve in the particular breach. This present review paper focuses on the future steps to prevent data breach reoccurrence and how social networking sites are responsible for data breaching.*

**Keywords:** Data Breaching, unauthorized access, Cambridge Analytica

### Authors:

1. Anand Engineering College, Agra, UP, INDIA.

## Introduction

Information Security is considered as one of the important part these days to any user of a computer or to any organization that are having computers installed in their daily operations. In the modern time, the information technology authorized the storage and the collection of huge amount of the personal data of an individual. These activities will surely provide the economic advantages and proved to be impossible to keep the data completely secure against criminal misuse. The evidence collected from the data breach plays a very significant role and also poses many unique challenges both legally as well as technically. The present review contains the data in chronological order on how, from time to time personal data had been stored by companies and its leak have led to massive social-economic downfall of a country. Information Security is categorized into three of the major parts refers as CIA of information security which are confidentiality, integrity and availability. The section of confidentiality deals with providing the information to authorized people who have access to the information whereas integrity refers to ensure that only the authorized people have access to the particular information. Availability is ensuring that the assessment of information is done and where it is supposed. This protects the information in the form of storage, transmission and processing (Hiatt and Choi 2016).

All these application which are web based provide users to connect to each other, communicate, and interact and the sharing the web information. There are number of social networking sites which are Twitter, Facebook etc. and all connects the people to each other. The personal profile that contains information for different sites of social network is created by the individuals to share their photos, videos, ideas, e-mails, instant messaging (Vadisala and Vatsavayi 2017).

Drawing attention to the latest case Cambridge Analytica, famous social site Facebook has been saving data of everyone from very long which recently came in light. Elections of any country has been very essence of the democracy. Since this case people have been skeptical about U.S. elections, whereas in India certain questions has been raised upon opposition party for having link to the company (Roberds and Schreft 2009). According to Symantec, Some of the common examples of social networking sites are Facebook, Myspace, Mixi, Orkut and Twitter such as Facebook is the most active used social networking sites worldwide. Facebook has announced in July 2010 that the registered users of Facebook crosses 500 billion. This system of network allows the active users

to create profile where they can share images, or videos and anything that is going on in their mind.

**Social Networks Spamming** - Spam is considered as one of the classic attacks and is adapting new technologies numerous times from the area of email spam to instant messaging spam. Some of the network system only allows the messages, if in case both the users of the social media sites are connected. To overcome all the restrictions, fake or dummy accounts are created by the attackers and the friend requests thousands in number are sent automatically and same will accept these requests.

As the social networking sites are growing in size and number, the unprecedented information is collected by owner about the online social networking users. The preservation of privacy of social networking data is considered as more complex behavior than the relational data preservation because of the structural properties of the network data. The facebook which is currently the most famous social networking site was launched. Marc Zuckerberg, the CEO of facebook proposed a technological conference in January 2010 in which he stated that these days privacy is no longer considered as a social norm as the users of these social networking sites have adapted the information sharing online over the blogs and on the other social media sites and for prevention, company structured its privacy settings (Alhaddad and Jadaibi 2014).

Cyberbullying is considered as a product of unwanted disclosure which has emerged as a major safety concern in internet over the past years. This term Cyberbullying comprises as an abuse or violation of the rights of privacy that protects against the private facts disclosing that would be considered as offensive. There are two mediums such as Facebook and MySpace where cyberbullying has occurred (Spinelli 2010).

## GOALS OF FORENSIC ANALYSIS IN DATA BREACH-

The investigation of data breach are started with the identification, collection and assessment of potentially relevant digital evidence. It reveals the information like the determination if a breach has occurred, determining the extent of loss, preserving the evidence, preparing the findings for the regulators/law enforcement/civil litigation. The legal team includes the corporate defense and privacy litigators with the involvement attorney experienced in the nuances of reviewing insurance policies and maximizing the chances of having such as intrusion covered by insurance carrier. The data breaches are discovered or suspected waiting an extra day which could result in

permanent loss of data beyond recovery. Hence to discover whether a loss occurred a forensic expert rely on the sources of digital evidence that address four key questions i.e. who, what, where and when.

### TO PREVENT DATA BREACH IN FUTURE -

- Encrypt private and sensitive data especially the credit card numbers and debit card PINs. It is revealed that whenever data is encrypted, it decreases the potential value of the data for the attacker.
- It is important to consider cyber and data breach insurance as cyber insurance can help to respond to and minimize the damage of data breach or cyber-attacks.
- Consideration of hiring pre-selected data breach resolution vendor in order to manage the cost of data breach and choose protection products for individuals effected in the breach.
- Facebook will investigate all apps that had access to large amounts of information before it changed its platform in 2014 to reduce data access. If Facebook removes an app for misusing data, it will tell everyone who used it.
- Do not assume the privacy on social sites and for both the usage i.e., business and personal, the information that is confidential should not be shared.
- Before posting any kind of information or commenting about anything in the world, use directions. Once the information gathered is posted online, it can be visualized by anyone (Schneider; <https://www.itgovernance.co.uk/blog/six-steps-to-help-prevent-a-data-breach/> ).

For Example In case of Cambridge Analytica - Alongside social media giant Facebook, Cambridge Analytica is at the center of an ongoing dispute over the alleged harvesting and use of personal data. Both companies deny any wrongdoing. Britain's Channel 4 News on Monday filmed senior executives at Cambridge Analytica, including its CEO Alexander Nix, suggesting the firm could use sex workers, bribes and misinformation in order to try and help political candidates win votes around the world. The saga is significant because of the way the harvested data might have been used. It was allegedly utilized to direct messages for political campaigns supported by Cambridge Analytica, most notably Trump's election victory and the Brexit vote.

There are some advantages of the usage of social networking sites, as sometimes it becomes profitable to the companies or businesses for the conduction of their activities related market online. These sites help

companies to generate strategies for marketing and also to find out the opinions of customer about their products. Social sites allows the user to share anything and everything on the internet and they can also share and organize their social or political lives online. The representation of the economic opportunity for social networking sites has been recognized by The European Commission for the European Industry (<https://www.duo.uio.no/bitstream/handle/10852/22928/CvetankaxTrichkovskaxThesis.pdf?sequence=1>).

### Literature Review

**Alessandro Acquisti 2006** - In the present study, the information gathered and combined privacy incidents and breach data from different sources for the 1999-2006 (until March) period. This study shows that there exists an impact for privacy violations. This impact is statistically significant and negative, although it is short-lived. The difference in our mean and median results suggests that a number of outlying firms are driving significant portion of the negative results.

**William Roberds- April 8, 2009** - In the present study, one can focus to facilitate trade, agents join clubs (networks) that compile and secure data. Too much data collection and too little security arise in equilibrium with non-cooperative networks compared to the efficient allocation. A number of potential remedies are analyzed, this paper has presented a model in which identity theft arises endogenously and the concept of efficient confidentiality for personal identifying information (PID) has meaning. However, the basic idea behind this approach—that the compilation, exchange, and storage of PID, despite its risks and costs, can enable otherwise infeasible inter-temporal exchanges of goods—can be generalized and should provide impetus for further research.

**Spinelli 2010**, evaluates the lack of the regulation in the social media website such as MySpace and Facebook. Researcher has discussed the case study that helps in exploring the concerns of the society that are brought out within the legal system with an increasing rate.

**Alhaddad and Jedaibi 2014** presented in his research paper the security methods in the application of social networking. In this paper, a new model is proposed on the basis of social network analysis and a new security metrics is suggested that helps in the security improvement and also reduces the risks that are associated with the users. According to this paper the issue of social networking security become a crucial parameter to business as well for the common users. The paper concludes that the attack consideration that exists in the social networks, there are always some sort of security measures and metrics that helps in the

improvement of safety and reduce the risks that makes environment suitable and safe for the user. The proposed model has some minimum needs to addressing the attacks.

**Brett Hawkins January 2015** - The key take away from this paper is that the Home Depot breach could have been prevented by taking a proactive approach. Learning how Target was breached in December of 2013 should have immediately prompted Home Depot to assess their environment and address the gaps that existed before becoming compromised. Taking the preventive measures that I have outlined could have prevented the Home Depot breach and will be able to prevent other retail data breaches in the future. These types of retail breaches are becoming more common. I hope that retailers will learn lessons from previous breaches to safeguard their environment and prevent it from happening to them

**Kuppuswamy and Rekha 2015** studied on the social network media effects on the quality and changes in the life style. The social media has led to the shifts in ways in which the people work and do some kind of business for the purpose of interaction and socialization. In Arab countries, the Social media has been included in gatherings of people around the social causes and movements which are political, community participation, interaction between the society and the government.

**Xiaokui Shu, 18 Jan 2017** - There is no silver bullet in cyber space against data breaches. With the increasing amount of data leak incidents in recent years, it is important to analyze the weak points in our systems, techniques and legislations and to seek solutions to the issue. In this paper, we presented a comprehensive analysis of the Target data breach and related incidents, such as the TJX breach. We 10 described several security guidelines to enhance security in merchants' systems. We presented the state-of-the art credit card security techniques, and gave customers best practices to hide card information during purchase transactions.

### Key Findings

Stuxnet 2010 but origins date to 2005 – Malware from the Stuxnet worm designed to target only Siemens SCADA system which damage the Iran's nuclear program by destroying 984 uranium enrichment centrifuges.

Impact- SCADA system vulnerable

RSA Security March 2011 – RSA which is a security division of EMC reveal two hackers groups who work in collaboration with foreign government to launch

phishing attacks against RSA employees trusted so as to penetrate company network.

Impact- 40 Million employee records stolen

Adobe October 2013 – Company claimed that the hackers had stolen nearly 3 million encrypted customer credit card records, login data of an undetermined number of user accounts. Later it was revealed this result in exposing customer names, IDs, Passwords and debit and credit card information

Impact- 38 Million user record

Home Depot September 2014 – they were infected with what the company called a “unique custom-built” malware which posed anti-virus software. The company estimated around \$161 million of pre-tax expenses for the breach which also include customer settlement and expected insurance proceeds

Impact- 56 Million customer

JP Morgan Chase July 2014 – the nation largest bank was the victim that compromised data of more than half of U.S. households, according to an SEC filing. Hackers got the root privileges on more than 90 bank's servers which help them in transfer funds and close accounts.

Impact- 76 Million households and 7 million small businesses

eBay May 2014 – The online auction giant reported a cyber-attack which exposed names, address, date of birth and encrypted passwords of users. The hackers by using the network credential of three employees made their way to user database.

Impact – 145 million users compromised

Yahoo 2013-2014 – In 2016 while in negotiation to sell itself to Verizon, Yahoo announced that 2 years back it had been the biggest victim of data breaches. The attack compromised data for 500 million users. Later Yahoo disclosed an earlier breach that had compromised 1 billion accounts.

Impact – 1.5 billion user accounts.

Anthem – February 2015 – The second largest health insurer in U.S reveal that the cyber-attack had exposed the names of addresses, security numbers, dates of birth and employment histories of current and former customers.

Impact- Personal data of upto 78.8 million customer.

Uber 2016 – Two hackers were able to get names, email addresses and mobile phone number of 57 users of Uber app. They also gained driver license number

of 600,000 Uber drivers. The hackers were able to access Uber's GitHub account where they found the passwords and username credentials of Uber's AWS account.

Impact - Personal information of 57 million Uber users and 600,000 drivers exposed.

Equifax July 2017 – considered as one of the largest bureaus in U.S. that an application vulnerable by one of its website led to data breach.

Impact- 143 million consumers

## Conclusion

Social Networking sites can be the sales of the valuable sources and the tools related to the markets as well as diversion that connects to the fun. With the applications, there are some inherent security risks that can put the user or any company in trouble or at serious risk or in a compromising situation. The major precaution taken is the least usage of these sites but along with this all policies and procedures should be made and are documented which is the most existing fundamental principle. A user who is well informed will have to maintain security issues and also educate other people on these concerns and the best practices were established that are standardized or optimized with the new applications..

## References:

Acquisti. Privacy and security of personal information: Economic incentives and technological solutions. In Jean Camp and Stephen Lewis, editors, *The Economics of Information Security*, 2004

Alessandro Acquisti Carnegie Mellon University [acquisti@andrew.cmu.edu](mailto:acquisti@andrew.cmu.edu) Allan Friedman Harvard University [allan\\_friedman@ksgphd.harvard.edu](mailto:allan_friedman@ksgphd.harvard.edu) Rahul Telang Carnegie Mellon University [rtelang@andrew.cmu.edu](mailto:rtelang@andrew.cmu.edu), Is there a cost to privacy breaches? An event study.

Anderson, K.B., E. Durbin, and M.A. Salinger, 2008. "Identity Theft," *Journal of Economic Perspectives* 22, 171-192.

Biscoe, Chloe. "Six Steps to Help Prevent a Data Breach." *IT Governance Blog*, 2 Nov. 2017, [www.itgovernance.co.uk/blog/six-steps-to-help-prevent-a-data-breach/](http://www.itgovernance.co.uk/blog/six-steps-to-help-prevent-a-data-breach/).

Breaking the Target: An Analysis of Target Data Breach and Lessons Learned Xiaokui Shu, Ke Tian\*, Andrew Ciambrone\* and Danfeng (Daphne) Yao, Member, IEEE

Bygrave, Lee a. *Legal and privacy challenges of social networking sites*. University of Oslo, 2012, [www.duo.uio.no/bitstream/handle/10852/22928/CvetankaxTrichkovskaxThesis.pdf?sequence=1](http://www.duo.uio.no/bitstream/handle/10852/22928/CvetankaxTrichkovskaxThesis.pdf?sequence=1).

Hiatt, David, and Young B Choi. "Role of Security in Social Networking." (*IJACSA*) *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 2, 2016, pp. 12–15.

ITRC breach report, [http://www.idtheftcenter.org/images/breach/ITRC Breach Report 2014.pdf](http://www.idtheftcenter.org/images/breach/ITRC%20Breach%20Report%202014.pdf).

Spinelli, Christopher F. "Social Media: No 'Friend' of Personal Privacy." *The Elon Journal of Undergraduate Research in Communications*, vol. 1, ser. 2, 59AD, pp. 59–69. 2.

Vadisala, Jyothi, and Valli Kumari Vatsavayi. "Challenges in Social Network Data Privacy." *International Journal of Computational Intelligence Research*, vol. 13, ser. 5, 2017, pp. 965–979. 5.

William Roberds Stacey L. Schreft Federal Reserve Bank of Atlanta the Mutual Fund Research Centre, LLC This revision: April 8, 2009 Data Breaches and Identity Theft

Wuest , Candid. "The Risks of Social Networking." *Symantec*. pp. 1–32.