**CAMBRIDGE ANALYTICA CASE STUDY**

**A PROJECT REPORT**

Submitted by Vanshika Bansal

Group 52

*in partial fulfilment for the award of the degree of*

**BACHELOR OF TECHNOLOGY**

*in*

**COMPUTER SCIENCE AND ENGINEERING WITH SPECIALIZATION IN**

**CYBER SECURITY AND DIGITAL FORENSICS**



**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING**

**VIT BHOPAL UNIVERSITY**

**KOTHRI KALAN, SEHORE**

**MADHYAPRADESH - 466114**

APRIL 2022

1

**VIT BHOPAL UNIVERSITY, KOTHRIKALAN, SEHORE MADHYA PRADESH – 466114**

**BONAFIDE CERTIFICATE**

Certified that this project report titled **Cambridge Analytica Scandal Case Study** is the bonafide work of **Vanshika Bansal (20BCY10053)** who carried out the projectwork under my supervision. Certified further that to the best of my knowledge the work reported at this time does not form part of any other project/research work based on which a degree or award was conferred on an earlier occasion.

**Dr. R. Rakesh**

Programme Chair - B.Tech School of Cyber Security division

VIT BHOPAL UNIVERSITY

**Dr Suryakanta Panda**

Project guide

VIT BHOPAL UNIVERSITY

2

**A C K N O W LED G EM EN T**

First and foremost, I would like to thank the Lord Almighty for His presence and immense blessings throughout the project work.

I wish to express my heartfelt gratitude to **Dr R Rakesh,** Program Chair, School of Computer Science Engineering (Cyber security) for much of his valuable support and encouragement in carrying out this work.

I would like to thank my internal guide **Dr Suryakanta Panda**, for continually guiding and actively participating in my project, giving valuable suggestions to complete the project work.

I would like to thank all the technical and teaching staff of the School of Computer Science Engineering, who extended directly or indirectly all support.

Last, but not least, I am deeply indebted to my parents who have been the greatest support while I worked day and night for the project to make it a success.

**ABSTRACT**

The case discusses the data breach scandal involving the world’s largest social media network, Facebook, its impact on the company and the challenges the

social media giants faced. It further discusses how India itself got involved with

Cambridge Analytica, and the assumed influence on the political scene. How the individuals, companies and nations reacted to this. Lastly, it elaborates on the initiatives Facebook took to overcome this huge scandal, the resulting changes in the field of data security and some preventive measures to secure personal data.

6

**TABLE OF CONTENTS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **C H A PTER** |  | **TITLE** | **PA G E N O.** |  |
| **NO.** |  |  |  |  |
|  |  | |  |  |
|  |  | |  |  |
|  |  | |  |  |
|  | Abstract |  | 6 |  |
|  |  | |  |  |
| 1 | **C H A PTER -1:** | |  |  |
|  | **PROJECT DESCRIPTION AND OUTLIN E** | | 9 |  |
|  | 1.1 | Introduction and Motivation for the work | 9 |  |
|  | 1.2 | Objective of the work | 9 |  |
|  |  |  |  |
|  |  | |  |  |
| 2 | **C H A PTER -2:** | |  |  |
|  | **CAMBRIDGE ANALYTICA CASE** | | 11 |  |
|  | 2.1 | Data Breach Scandal | 11 |  |
|  | 2.2 | India’s encounter | 11 |  |
|  |  | |  |  |
| 3 | **CHAPTER -3:** | |  |  |
|  | **AFTERMATH OF THE SCANDAL** | | 12 |  |
|  | 3.1 | Effects on individuals, organisations, and nations and their reactions | 12 |  |
|  | 3.2 | Effect on Facebook | 12 |  |
|  |  |  | 12 |  |
|  |  | |  |  |
| 4 | **C H A PTER -5:** | |  |  |
|  | **DATA SECURITY MEASURES** | | 13 |  |
|  | 4.1 Facebook’s initiatives  4.2 Facebook’s new privacy policy | | 13 |  |
|  | 4.3 | Technology and algorithms behind key security features | 26 |  |
|  |  |  |  |  |

7

|  |  |  |  |
| --- | --- | --- | --- |
| 5 | **C H A PTER -6:** | |  |
|  | **CONCLUSION** | | 27 |
|  | 5.1 | Conclusion | 27 |
|  | 5.2 | Project applicability on Real-world applica | 28 |
|  |  |  |  |
|  |  | References | 37 |
|  |  |  |  |

**PROJECT DESCRIPTION AND OUTLINE**

**INTRODUCTION :** Attackers are drawn to social media channels because they are cost effective and cybercriminals can easily create fraudulent accounts that spread malicious content efficiently and at an unprecedented scale. Scams on social media skyrocketed by 150 percent across Facebook, Twitter, Instagram, and LinkedIn in 2016, and that number is likely to continue to climb.

In the 21st century, information has become a new currency. People are constantly giving away their privacy rights on social media sites, at time without even being aware. Following the Cambridge Analytica scandal, people should be paying more attention to what they are agreeing to share when they sign up or log into an account. For example, according to Facebook's Statement of Rights and Responsibilities, any photos and videos shared by other users remain on the site after you deactivate the account most individuals are likely unaware of that.

***“The total number of records compromised in 2020 exceeded 37 billion, a 141% increase compared to 2019 and by far the most records exposed in a single year since we have been reporting on data breach activity.” –***[***Risk Based Security 2020 Year End Report***](https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf)

**OBJECTIVE:**

* To study how social media platforms risk the leak of private and sensitive information nowadays,
* How data security is becoming a necessity
* The post- Cambridge Analytica effects
* Different Data Security technologies in use and how they function

# HOW DATA COLLECTION OCCURRED AND GOT USED

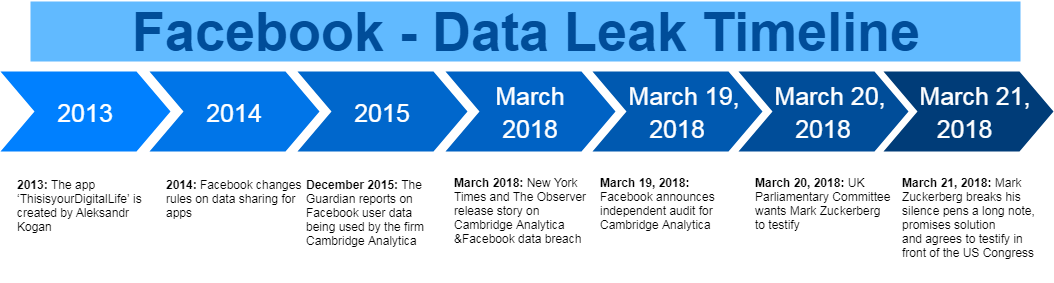
➢ Aleksandr Kogan, a data scientist at the University of Cambridge, was hired by Cambridge Analytica, an offshoot of SCL Group, to develop an app "This Is Your Digital Life" .

➢ Cambridge Analytica then arranged an informed consent process for research in which several hundred thousand Facebook users would agree to complete a survey for paymentthat was only for academic use.

➢ However, Facebook allowed this app not only to collect personal information from survey respondents but also from respondents’ Facebook friends.[14] In this way, Cambridge Analytica acquired data from millions of Facebook users.

➢ Ted Cruz Campaign- Cambridge Analytica started to create individual psychographic profiles and used this data to create tailored advertisements for each person to sway them into voting for Cruz.

➢ Donald Trump campaign-Donald Trump’s 2016 presidential campaign used the harvested data to build psychographic profiles, determining users' personality traits based on their Facebook activity. The campaign team used this information as a micro-targeting technique, displaying customized messages about Trump to different US on different digital platforms.

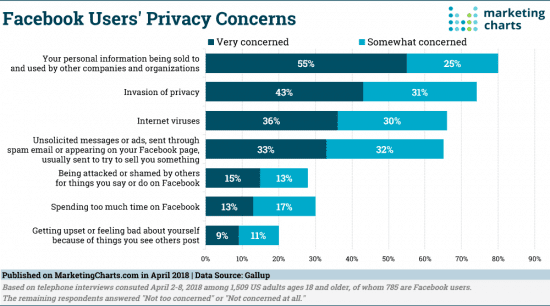


POST CAMBRIDGE ANALYTICA EFFECTS

# Effects on individuals, organisations and nations

Effect of Data Leak on Individuals and Organizations:

1. **Individuals:**  
   Personal details of individuals and details on their personality, political inclination, food habit preferences and allied was shared to various companies looking out for it hungrily. This becomes more dangerous if details on debit/credit cards or identity proof details get leaked which can be misused by people and also anti-national outfits to gain access to various services.
2. **Organizations:**  
   At a time like this, organizations take the biggest hit of losing consumer trust. [**Facebook lost nearly $50 billion**](https://www.recode.net/2018/3/20/17144130/facebook-stock-wall-street-billion-market-cap) in market capitalization since the leak news surfaced. It has not been long since Unilever in very clear terms instructed that they would pull out of advertisements off Facebook and Google if they didn’t do anything about the extremist content being published on their platforms.
3. **Nation:**  
   With data of around 50 million American users being accessed by one single organization, it is a threat to national security and its democracy. Elections can be manipulated, policies can be made populous to favour a specific outfit. God forbid if the data goes in the hand of anti-national elements the results could be more dangerous. Nations need to pull up their socks to fight this new calamity.



DATA SECURITY MEASURES

# BASIC MEASURES AT YOUR WORKPLACE

1. **Read the terms:**  
   While it seems to be a herculean task, people in compliance will strongly recommend you take five more minutes to read the terms and conditions before you click on ‘I Agree’. I personally remember an app asking for my credit card details including its pin before I could access it. Scary, isn’t it?
2. **Is it a necessity? :**  
   While the world seems to be in a rat race, let’s be happy being a tortoise! Just because your friends have downloaded an app and going gaga over it, doesn’t mean you need it too! Ask yourself if you really need that app! If not, let it pass.
3. **Be the investigator:**  
   Once in a month, try to become an auditor. Review the apps you are using, what are the permissions you have already given to the
4. app. In the wake of the Facebook scandal, we have come to know that we can know where all has our data been transported through Facebook.
5. **Be a whistleblower:**  
   If you find certain malpractices going on in your organization or any other internet platform, take a step forward to blow the lid off.
6. **Privacy policy:**  
   Every organization and nation need to have a reasonably stringent policy at the earliest if they don’t have one. The Facebook leak clearly brings into the open the loopholes in the privacy policy of the world’s largest social media platform.

# PROPOSED INTIATIVES TO PREVENT ANOTHER DATA LEAK BY Facebook

The initiatives include:

— Reviewing all apps that have had access to large amounts of data on its platform and apps with suspicious activity,  
  
— Alerting people who have had their information misused through apps,

— Turning off an app’s access to users’ data if the person hasn’t used the app in the last three months

— Changing Facebook Login data so apps can only see a user’s name, profile photo and email address unless the app goes through a further review process,  
  
— Helping people manage the apps they use on Facebook and what information the apps can see about them, and,  
  
— Increasing [bug bounty program](https://www.facebook.com/whitehat) for people to report and get rewarded if they find instances of app developers incorrectly using people’s data.

# FACEBOOK’S NEW PRIVACY POLICY

**At its F8 2019 keynote, Zuckerberg detailed six core pillars of what the new, privacy-focused Facebook will look like:**

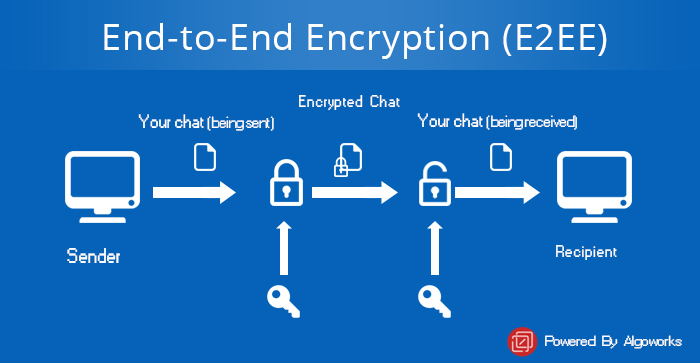
**PRIVACY:** Private interactions users should have control over being able to share something with one or a few people, privately, and without prying eyes. And private interactions bleed over a little into encryption — after all, encryption is partly how user interactions will remain private.

**ENCRYPTION:** end-to-end encryption will essentially ensure that no one can see activity you want to keep private, except for you, and that should include Facebook.

**REDUCED PERMANENCE**: implement ephemeral messaging i.e. the data text gets deleted as soon as its viewed.

**SAFETY:** the company could aim to reduce online bullying, by doing things like adding tools for users to prevent people from targeting them online or being able to continue targeting them online. Part of making Facebook a little safer could tie into the reduced permanence of content.

**UNTEROPERABILITY:** Facebook wants to tie all of its products together, and a big part of that is ensuring that its messaging services work well together.



**WHAT IS END-TO-END ENCRYPTION?**

**E2E2EE** or **End to End Encryption** refers to the process in which encryption of data are being done at the end host. It is an implementation of Asymmetric encryption and hence ensures a secure way of data communication. It is the most secure way to communicate privately and securely as data can be read-only by the sender and the receiver. No one else can encrypt the data including government or even by the server through which data is passing.Th

e s

**Working of End to End Encryption/ ALGORITHM**

* It uses asymmetric encryption technique for data communication between sender and receiver
* Sender pulls down receiver’s public key from the server
* Sender then encrypts the messages to be sent using the public key of receiver
* Sender then send the encrypted messages to the server
* Receiver then receives the encrypted messages from the server
* Receiver then using its private key decrypt the messages
* Receiver the reads the messages.

# REDUCED PERMANENCE

EPHEMERAL MESSAGING:

A message is sent from one device to another.

Once the message is received and viewed, it automatically deletes thus resulting in temporary permanence.

**Algorithm:**

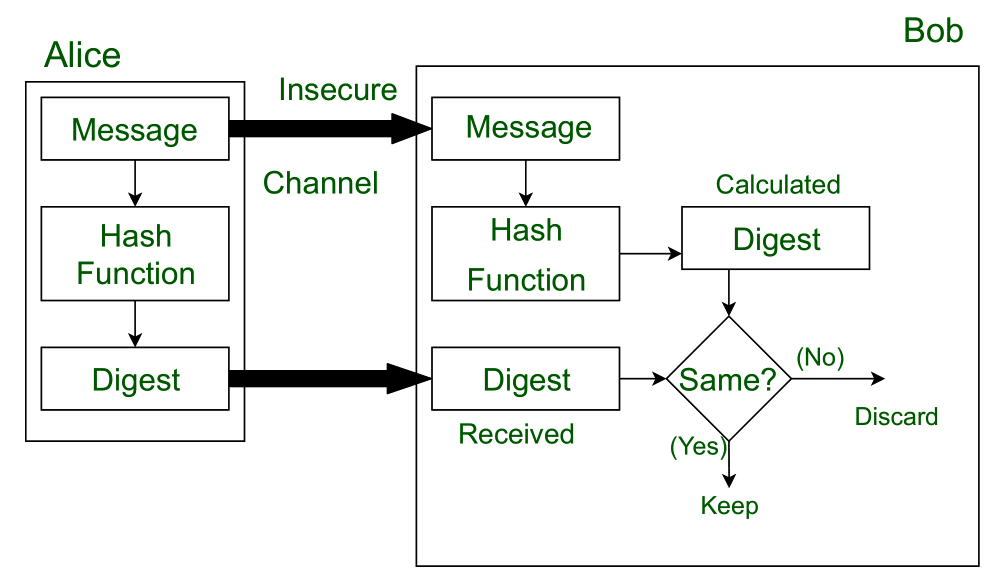
A function **view** that check whether the given string is viewed or not, and returns true or false.

If(view(str)==true) then delete str;

Else break;

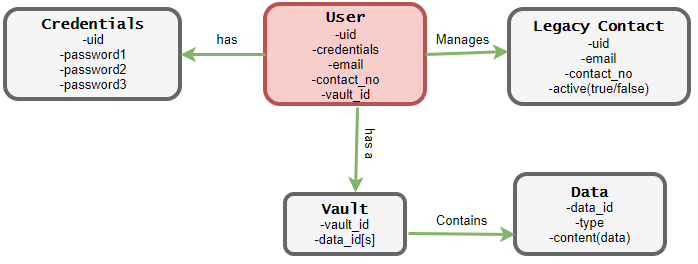
## Message Digest in Information security

* **Message Digest** is used to ensure the integrity of a message transmitted over an insecure channel (where the content of the message can be changed). The message is passed through a [Cryptographic hash function](https://www.geeksforgeeks.org/passwords-and-cryptographic-hash-function/). This function creates a compressed image of the message called **Digest**.



LYV – Liberate Yourself Vault

LYV aims to provide a robust, secure and customisable data storage platform where the user can store his/her most private data like email credentials, mobile’s password, social media account’s credentials, images, videos, audios, wills, private journals and any other type of data imaginable.  
A user will be allowed to choose legacy contacts(emails, mobile numbers, contact address) and the conditions to meet before the release of information. Upon meeting these conditions, the user’s data will be made available to the legacy contacts.



CONCLUSION

This scandal served as a huge wake-up call to everyone regarding data security , despite there being an increase in the number of cases of data breach and the consequent losses suffered.

This has further promoted the use of data security measures such as encryption, and their need in the current times has been finally highlighted.

REFERENCES

<https://en.wikipedia.org/wiki/Cambridge_Analytica>

<https://www.digitaltrends.com/social-media/facebook-says-the-future-is-private-but-what-does-that-mean/>

<https://www.icmrindia.org/casestudies/catalogue/Business%20Ethics/Cambridge%20Analytica-Case.htm>

<https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/>

<https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>

<https://www.virtusa.com/perspectives/article/the-importance-of-cyber-security-in-a-post-cambridge-analytica-scandal-era>

<https://repositorio.ucp.pt/bitstream/10400.14/29693/1/152118129_RaquelDuarte_DPFA.pdf>

<https://legaldesire.com/case-study-on-cambridge-analytica-embezzling-on-facebook-users-data/>

<https://indjst.org/download-article.php?Article_Unique_Id=INDJST3194&Full_Text_Pdf_Download=True>

<https://www.researchgate.net/publication/330032180_Cambridge_Analytica_Ethics_And_Online_Manipulation_With_Decision-Making_Process>

<https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/>

<https://fotislaw.com/lawtify/case-study-on-facebooks-data-breach/>

<https://thecomputerjoker.com/case-study-facebook-cambridge-analytica-data-breach>

<https://www.geeksforgeeks.org/project-idea-liberate-yourself-vault-lyv/>