Name: SOHAIB ZAHID

Reg No: FA20-BSE-027

Section: FA20-BSE-B

Submitted to: DR. TARIQ OMER

NATIONAL LEVEL CASES:

Case No. 1 - WhatsApp Group Admin Arrests in India (2020)

Multiple WhatsApp group administrators in India were detained on various times in 2020 for their participation in the platform's distribution of false material. Such content was spread, which resulted in social turmoil and violent incidents. The arrests were made in accordance with several provisions of the Indian Penal Code and the Information Technology Act, underscoring the difficulties in policing and controlling the information shared on messaging apps.

Prosecuted Under:

The arrested WhatsApp group administrators were charged under relevant sections of the Indian Penal Code and the Information Technology Act, which encompass provisions related to spreading offensive content, inciting violence, and creating public nuisance.

Court Decision:

The court proceedings following the arrests varied depending on the specific cases and charges brought against the accused group administrators. Detailed information about specific court decisions or outcomes for individual cases was not provided in the available reference.

Reference:

https://www.bbc.com/news/world-asia-india-53698627

Case No. 2 - Snapchat Data Breach in India (2017)

In 2017, Many users in India were impacted by a data breach involving the well-known social media network Snapchat. Hackers accessed user accounts without authorization and exposed private data,

including usernames, email addresses, and phone numbers. The security and privacy of user data on social media sites have come under scrutiny because of this hack.

Prosecuted Under:

Legal actions were initiated based on applicable sections of the Indian Penal Code and the Information Technology Act, which cover offenses related to unauthorized access, data breaches, and the compromise of personal information.

Court Decision:

Specific court decisions and outcomes resulting from the Snapchat data breach case in India were not explicitly mentioned in the available reference.

Reference:

https://indianexpress.com/article/technology/social/snapchat-data-breach-india-4640824/

INTERNATIONAL LEVEL CASES:

Case No. 1 - Cambridge Analytica and Facebook Data Scandal (2018)

In 2018, the Cambridge Analytica scandal emerged as a major international privacy issue. It was revealed that the political consulting firm, Cambridge Analytica, had obtained and improperly used personal data from millions of Facebook users without their consent. This data was utilized for political advertising and manipulation purposes, raising concerns about privacy, data protection, and the influence of social media on elections.

Prosecuted Under:

The investigation into the Cambridge Analytica scandal resulted in legal actions against the company and its involved individuals under various data protection and privacy laws, including the General Data Protection Regulation (GDPR) in the European Union.

Court Decision:

The specific court decisions and outcomes resulting from the Cambridge Analytica scandal varied across different countries, with regulatory bodies imposing fines and penalties on Facebook for its role in the data breach.

Reference:

https://www.theguardian.com/news/series/cambridge-analytica-files

Case No. 2 - Twitter Hack Targeting High-Profile Accounts (2020)

In 2020, a significant security breach occurred on Twitter, targeting high-profile accounts. Hackers gained unauthorized access to prominent accounts, including those belonging to politicians, celebrities, and business figures. The breach was used to perpetrate a cryptocurrency scam, with fake tweets requesting

followers to send Bitcoin payments. This incident highlighted vulnerabilities in social media platforms and the potential for large-scale security breaches.

Prosecuted Under:

Legal actions were pursued against the individuals involved in the Twitter hack under relevant computer hacking and fraud laws.

Court Decision:

Specific court decisions and outcomes resulting from the Twitter hack case were not explicitly mentioned in the available reference.

Reference:

https://www.nytimes.com/2020/07/16/technology/twitter-hack-bill-gates-elon-musk.html

IMPLEMENTED PRIVACY LAWS

SWEDEN

- **Personal Data Act:** This act governs the processing and protection of personal data in Sweden. It sets out the rights and obligations of data controllers and data subjects, ensuring the privacy and security of personal information.
- **Electronic Communications Act:** This law regulates electronic communications, including the processing and protection of personal data in electronic communication services. It ensures the confidentiality and security of communications and imposes obligations on service providers regarding data protection.
- **General Data Protection Regulation (GDPR):** The GDPR is an EU regulation that directly applies to Sweden. It governs the processing of personal data, emphasizing individuals' rights and imposing obligations on data controllers and processors. The GDPR strengthens data protection standards and grants individuals' greater control over their personal information.

ZIMBABWE

- **Data Protection Act (2019):** Zimbabwe implemented the Data Cortana Protection Act to regulate the processing of personal data and protect individuals' privacy rights. This law provides guidelines on the collection, storage, use, and disclosure of personal information, promoting responsible data handling practices.
- **Postal and Telecommunications Act (Chapter 12:05):** The Postal and Telecommunications Act in Zimbabwe addresses various aspects of communication services, including privacy. It outlines provisions related to the protection of personal data, confidentiality of communications, and the rights and obligations of communication service providers and users.
- **Interception of Communications Act:** This act regulates the lawful interception of communications in Zimbabwe. It establishes procedures and safeguards for authorized entities, balancing national security needs with the protection of privacy rights.

CONCLUSION:

In conclusion, Sweden has implemented the Personal Data Act, Electronic Communications Act, and complies with the General Data Protection Regulation (GDPR) to safeguard personal data and ensure privacy protection. Zimbabwe has enacted the Data Protection Act (2019), Postal and Telecommunications Act, and Interception of Communications Act to regulate the processing of personal data, protect privacy rights, and establish procedures for lawful interception. These laws reflect the commitment of both countries to uphold privacy standards and promote responsible handling of personal information.