Cambridge Analytica and Facebook Data Scandal

Abstract:

This case study discusses the data breaking scandal involving the worlds largest social media network, Facebook , kits impact on the company , and the challenges facing on the social media giant. They was designed with the vision of connecting people with their family and friends to discover what is going on in the world and to share and express what matters to them, Facebook became a popular social media company with about 2.19 billion monthly active users as of the first quarter of 2018. However, the company continuous growth was marred by security concerns. In March 2018, Facebook was caught in a major data breaking scandal in which a political consulting firm – Cambridge Analytica withdraw the personal data of more than 87 million Facebook users without their permissions. The data was illegally used in favor of the US Presidential candidates , Donald Trump , during the 2016 elections. Further , it was found that the data was misused to influence the Brexit referendum results in favor of the vote leave campaign. The tech giant reaction to the scandal was reportedly clumsy, defensive, and confused. When Facebook got to know about the data breach, it allegedly did not do anything and waited for months to send orders to Cambridge Analytica to delete all the data. Further, the company did not follow up to check whether the illegally acquired data been deleted.

Keywords: Data breach , Data privacy , Ethics, Data protection , Cyber Risk Assessments , Cyber Security , Privacy protection , Data leaks.

Introduction:

In march 2018, under a campaign started against the world largest online social networking service Facebook , many of its users vented their anger against the company, as they felt it was making their needs subservient to its financial goals. Through the campaign #delete Facebook people expressed their concern over the data harvesting and manipulation. Anger erupted against the company when the news broke in march 2018 that the personal information of up to 87 million Facebook users had been accessed inappropriately by a British political consulting firm, Cambridge Analytica (CA) to create targeted political advertising with the intention of US President Donald Trump. The movement #Delete Facebook started and it rapidly swept across the internet . The share value of Facebook also declined sharply after the news and the company market value went down by nearly US$50 billion in just two days from 18 March 2018 to 20 March 2018 and the stock biggest two day decline ever.

Excerpts

Cambridge Analytica:

There were many data analytics companies which used social networking sites for academic research purposes. One such firm was a London-based elections consultancy, Cambridge Analytica (CA), founded by a politically active person, Robert Mercer, co-CEO of a hedge fund, Renaissance Technologies. CA was known to be one of the most prominent companies in the data analytics industry and had handled high-profile clients like Republican candidates Ted Cruz (Cruz) and Ben Carson. Explaining the methodology of CA in 2016, its CEO Alexander Nix (Nix), said, we have rolled out a long-form quantitative instrument to probe the underlying traits that inform personality. If you know the personality of the people you are targeting, you can nuance your messaging to resonate more effectively with those key groups.⊙

The Data Scandal:

In 2010, Facebook launched a platform called Open Graph for third-party apps. Through this update, external developers could reach out to Facebook users and request permission to access their personal data and that of their Facebook friends. Once the users agreed, the apps gained access to their information like their name, gender, location, birthday, education, political preferences, relationship status, religious views, online chat status, and even their private messages.

Facebook Under Fire:

While CA was blamed for having harvested the data of millions of other people for political and financial gain without their consent, amid the data-privacy scandal, Facebook also had to face the heat in many countries. Initially, the number of people affected was reported to be 50 million. Facebook later revised this to 87 million. Of the affected people, about 70.5 million were in the US, while the remaining were in several other countries, including the UK, Canada, Australia, and India.

Challenges:

According to analysts, one of the biggest challenges facing Facebook post the scandal was how to regain the trust of its users. Analysts believed that though the company had been offering apologies to fix its reputation among users, advertisers, lawmakers, and investors, there was certainly an erosion of trust. According to a poll conducted online across the US, fewer Americans trusted Facebook than other tech companies...

Critism:

Though NestlÃ© was applauded for its admission of forced labour within its seafood supply chain and its move toward transparency, some analysts felt that this was just an attempt by the company to cover up bigger allegations of child labour in its profitable chocolate making business. They felt that in order to escape the charges of being an unethical company, NestlÃ© had admitted to slavery in seafood suppliers, a low-profit area of the company financial business, in Thailand. Some critics saw NestlÃ© actions as a public relations stunt to alleviate the criticism it had received for abetting child slavery in Ivory Coast.

The Road Ahead:

Zuckerberg publicly apologized for the company has mistake and announced that Facebook would change how it shared data with third-party apps. Further, he promised to investigate all third-party apps having access to data before 2014 and said the company would ban app developers that were not complying with a full audit. .

Solution:

Facebook decided to implement the EU's General Data Protection Regulation in all areas of operation and not just the EU.

What is GDPR ? (General Data Protection Regulation)

The General Data Protection Regulation (GDPR), agreed upon by the European Parliament and Council in April 2016, will replace the Data Protection Directive 95/46/ec in Spring 2018 as the primary law regulating how companies protect EU citizens' personal data. Companies that are already in compliance with the Directive must ensure that they are also compliant with the new requirements of the GDPR before it becomes effective on May 25, 2018. Companies that fail to achieve GDPR compliance before the deadline will be subject to stiff penalties and fines.

GDPR requirements apply to each member state of the European Union, aiming to create more consistent protection of consumer and personal data across EU nations.

Some of the key privacy and data protection requirements of the GDPR include:

- Requiring the consent of subjects for data processing
- collected data to protect privacy

- Providing data breach notifications
- Safely handling the transfer of data across borders
- Requiring certain companies to appoint a data protection officer to oversee GDPR compliance

Simply put, the GDPR mandates a baseline set of standards for companies that handle EU citizens' data to better safeguard the processing and movement of citizens' personal data.

Who within my company will be responsible for compliance ?

GDPR defines the several roles that are responsible for ensuring compliance.

1) Data Controller
2) Data Processor
3) Data Protection officer

How does the GDPR affect third-party and customer contracts

The GDPR places equal liability on data controllers (the organization that owns the data) and data processors (outside organizations that help manage that data). A third-party processor not in compliance means your organization is not in compliance. The new regulation also has strict rules for reporting breaches that everyone in the chain must be able to comply with. Organizations must also inform customers of their rights under GDPR.

What this means is that all existing contracts with processors (e.g., cloud providers, SaaS vendors, or payroll service providers) and customers need to spell out responsibilities. The revised contracts also need to define consistent processes for how data is managed and protected, and how breaches are reported.

"The largest exercise is on the procurement side of the house—your third-party vendors, your sourcing relationships that are processing data on your behalf," says Mathew Lewis, global head of banking and regulatory practice at legal service provider Axiom. "There's a whole grouping of vendors that have access to this personal data and GDPR lays out very clearly that you need to ensure that all of those third parties are adhering to GDPR and processing the data accordingly."

Client contracts also need to reflect the regulatory changes, says Lewis. "Client contracts take a number of different forms, whether they are online click-throughs or formal agreements where you make commitments to how you view, access, and process data."