Cambridge Analytica's Facebook Scandal - II

Click here for Part-I

\n\n

What is the issue?

\n\n

\n
- A global data analytics company is in spotlight for involving in a data scandal during US election.
\n
- The Facebook data breech involved is a wake-up call for technology companies, policymakers and internet users alike.
\n

\n\n

What is the scam?

\n\n

\n
- Cambridge Analytica, a data analytics company, managed to harvest data from Facebook users.
\n
- This was used to build psychological profiles of more than 50 million individuals.
\n
- A whistle-blower has uncovered it all, highlighting the commercial nexus between Analytica and US politicians.
\n
- This was particularly in relation with predicting and shaping voting preferences.
\n
- A company called Global Science Research (GSR) used a personality App with the permission of Facebook, for supposedly academic research purposes.
\n
- With the help of this, a psychology lecturer at Cambridge University managed to harvest data.

\n
- Data of millions of FB subscribers who used the personality App was sold for presidential campaign.
\n

\n\n

What is Facebook's response?

\n\n

\n
- FB’s stand is that GSR gained access in a legitimate manner.
\n
- But it allegedly violated the rules of agreement by passing on the secured information to a third party, namely, the Republican Party.
\n
- There are no charges on the company as yet that the data in question was obtained through hacking of the Facebook website or by any other unethical technological means.
\n

\n\n

What is the significance?

\n\n

\n
- The scam sends out a worrying warning on the imminent threat in the digital world.
\n
- The impact of the latest data breach could have been limited if users were aware that they could actually turn off permissions to third party applications.
\n
- Unfortunately, it took a data breach incident for Facebook to proactively highlight this security feature.
\n

\n\n

What measures need to be taken?

\n\n

\n
- The entire business model around personalised advertising requires access to more and more user information.
\n

- Some of these activities could be legitimate but it needs to be clearly defined and communicated to the users.
  \n
- The data breach at Facebook is a wake-up call for technology companies, policymakers and consumers of data services.
  \n
- These companies must create awareness about data protection.
  \n
- This should be backed up with strong data protection laws that impose heavy penalties on violators.
  \n

\n\n

  \n
- In all, the scandal calls for tech companies to draw a healthy balance between winning clients and the expenditure involved in nursing privacy and protecting data.
  \n

\n\n

\n\n

Source: Business Line

\n

