Facebook: Privacy Controversy II

Why in news?

The documents released by a British MPthat contains Facebook internal emails shows that Facebook compromised user privacy to help its partners and hurt its rivals.

Who released the document of internal emails?

- The 250 pages of documents was published online by the Digital, Culture, Media and Sport (DCMS) Select Committee of the UK House of Commons.
- Itincludes internal Facebook emails from 2012-15, which were part of sealed evidence in a lawsuit filed in the US against Facebook by app developer Six4Three.
- The documents are part of the DCMS Committee's investigation into Facebook's practices, which started after the Cambridge Analytica scandal earlier this year.

What do the Facebook emails reveal?

- **Whitelist**: Facebook had **whitelisting agreements** with certain companies that got full access to the data of users' friends.
- Whitelisting is the practice of identifying entities that are provided a particular privilege, service, mobility, access or recognition.
- In 2014-15, Facebook barred app developers from accessing the data of friends.
- However, it created a special application programming interface (API) to let some firms like the online dating-focussed Badoo, HotorNot, and Bumble, and OTT giant Netflix, continue to have access to friends' data.
- Facebook argued that whitelisting was common in the industry at the time of testing new features.
- **User data and revenue:** The emails show Facebook leveraged user data to drive its own revenues.
- Apps that spent more on advertising on Facebook got more access to the data.
- Developers either bought Facebook's ad products or paid for access to data.
- **Data reciprocity:** App developers had to ensure that users could share back their experiences to the social network from their apps in exchange for

access.

1. If you access a certain type of data (e.g. music listens), you must allow the user to publish back that same kind of data.
2. Developers also had to allow users to post their activity from the app back to Facebook, which would mean more social sharing on Facebook.

- **Android users' call, SMS data:** The emails show Facebook knew that the Messenger app update on Android that collected call log data and texts sent by the user, would be controversial and a PR challenge.
- The company found a way so that the updated Android app would ask for access only to users' call logs and not to other types of data.
- Facebook got the data once the app was updated.
- **Tracking usage of other apps:** Facebook used Onavo, a VPN service app that it acquired in 2013, to "conduct global surveys of the usage of mobile apps by customers" without their knowledge, including what apps they downloaded and used.
- This helped Facebook track rising competitors and potential targets for purchase in the future.
- The data showed, for example, that WhatsApp was rising fast with 8.2 billion messages sent in 2013.
- **Killing off the competition:** Facebook restricted access for Vine, a six-second video sharing service effectively killing the product because users would not be able to find their friends on the service.
- Facebook then launched its own short video format on Instagram.

What is the response of Facebook to these revelations?

- In case of whitelist agreements, Facebook justified it's decision as it was to restrict apps built on top of their platform that replicated their core functionality.
- Facebook is now removing this out-of-date policy.

- Data reciprocity: People had the choice about whether to share their app experience (game score, photo, etc.) back to their Facebook friends.
- With respect to collecting the users call log data Facebook said that the information collected was to make better suggestions for people to call in Messenger and rank contact lists in Messenger and Facebook Lite.
- The usage of Onavo creates a safer connection as it collects information about app usage to gain insights into the products and services people value, so that Facebook can build better experiences.

Source: The Indian Expres