DAYANANDA SAGAR COLLEGE OF ENGINEERING
An Autonomous Institute Affiliated to VTU, Belagavi Approved by AICTE ; ISO 9001:2015 Certified
Accredited by National Assessment Accreditation Council (NAAC) with 'A' grade
Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078

Department of Artificial Intelligence & Machine Learning

Incident Identification		
Submitted By: Rakshitha PR	**Date & Time:** 25/10/2025	**Report Ref No: 10**
Title: Cambridge Analytica Data Misuse via Facebook	**Company:**Facebook Inc.	**System / Application:** Facebook Data API (Graph API v1)

Type of Incident Detected					
Denial of Service		**Malicious Code**	Yes	**Unauthorized Use**	Yes
Unauthorized Access	Yes	**Unplanned**		**Other**	Yes (Data Privacy Violation)

Description

On March 17, 2018, Facebook Inc. disclosed a major data misuse involving Cambridge Analytica, a political consulting firm. A third-party quiz app, *"This Is Your Digital Life"*, developed by Aleksandr Kogan, exploited Facebook's Graph API to harvest personal data from users and their friends affecting over 87 million profiles without consent.
The data, including names, locations, and psychological traits, was later used for political profiling and targeted advertising.
This breach violated GDPR Article 5 and Section 8 of the DPDP Act 2023, as personal data was processed without consent, shared unlawfully, and transferred to unauthorized foreign entities.

People Involved

- Mark Zuckerberg – CEO, Facebook Inc.
- Aleksandr Kogan – Developer of "This Is Your Digital Life" app
- Alexander Nix – CEO, Cambridge Analytica
- Christopher Wylie – Whistleblower
- Facebook Data Protection and Compliance Team
-

Others Notified

- UK Information Commissioner's Office (ICO)
- European Data Protection Board (EDPB) under GDPR
- US Federal Trade Commission (FTC)
- Data Protection Authorities of Affected EU Nations
- Public Notification via Press Release and Hearings

Actions

Identification / Verification measures:

- Initial media reports and whistleblower statements triggered internal audits.
- Log analysis confirmed excessive API data extraction from the quiz app.
- Third-party app permissions were cross-verified, revealing improper access.
- Facebook's internal security team reconstructed the timeline of data access between 2014–2015.

Containment measures:

- Facebook immediately suspended Cambridge Analytica and Aleksandr Kogan's app access.
- Disabled third-party developer access to friends' data.
- Updated data permission models in Graph API v2.0 to restrict bulk data access.

Evidence collected (system logs etc.):

- API access logs and developer tokens.
- App installation records and consent prompts.
- Legal communication and forensic analysis reports.

Eradication measures:

- Removed all unauthorized apps exploiting API vulnerabilities.
- Conducted complete audits of third-party developer access.
- Enforced stricter review and approval mechanisms for data APIs.

Recovery measures:

- Notified all affected users globally through in-app alerts and emails.
- Enhanced transparency with "Off-Facebook Activity" tools.
- Cooperated with data protection authorities in the UK, EU, and US.

Other mitigation measures:

- Introduced Data Protection Officer (DPO) roles internally for compliance.
- Revised Developer Policy Agreements to mandate consent verification.
- Implemented independent privacy audits and data minimization policies.
- Conducted organization-wide data ethics and GDPR compliance training.

Learning:

1. Third-party integrations can become major privacy risks if not continuously monitored.
2. Data misuse often stems from consent loopholes rather than direct hacking.
3. The case highlighted the importance of DPO oversight and consent traceability under GDPR and DPDP Acts.
4. Transparency and 72-hour breach reporting could have reduced reputational and financial damage.
5. The incident reshaped global awareness of data privacy, leading to stricter data protection regulations worldwide.