1. **Sensitive and Personal Data Collected During a Digital Forensics Investigation**

As per the scenario provided, for digital forensics investigation, the sensitive and personal data may be collected;

- ✓ **Social Media Activities.** Posts, likes, shares, and other interactions on social media platforms.
- ✓ **Location Data.** GPS coordinates, IP addresses, and other location-based information.
- ✓ **Financial Information.**Credit card numbers, bank account details, and transaction histories.
- ✓ **Communication Data.** Emails, text messages, chat logs, and social media interactions.
- ✓ **Behavioral Data:** Browsing history, search queries, and online activity logs.
- ✓ **Biometric Data.** Fingerprints, facial recognition data, and other biometric identifiers.
- ✓ **Health Information.** Medical records, health insurance details, and other health-related data.
- ✓ **Personal Identity Information.** This includes names, addresses, phone numbers, email addresses, and social security numbers.
- ✓ **Employment Information.** Job titles, work history, and salary details.

2. **Uganda's Data Privacy Law and Individual Rights.**

Uganda's data privacy law is primarily governed by the **Data Protection and Privacy Act, 2019**.

This laws aims to protect the privacy of individuals and regulate the collection, storage, and processing of personal data. In the context with the Cambridge Analytica case, the following rights would be relebvant.

- ➢ **Right to Consent.** Individuals have the right to be informed and give consent before their personal data is collected or processed. In the Cambridge Analytica scenario, users would have had to explicitly consent to their data being accessed by third parties.
- ➢ **Right to Access.** Individuals have the right to access their personal data held by data collectors or processors. This means that Facebook users in Uganda could request to see what data was collected and how it was used.
- ➢ **Right to Rectificatio.** Individuals can request the correction of inaccurate or incomplete personal data. If users found that their data was misrepresented, they could demand corrections.

- **Right to Erasure (Right to be Forgotten).** Individuals can request the deletion of their personal data when it is no longer necessary for the purpose it was collected. Users could have asked Facebook to delete their data to prevent further misuse.

16. Correction of personal data.

(1) A data subject may request a data controller to—

(a) correct or delete personal data about the data subject held by or under the control of the data controller that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

(b) destroy or delete a record of personal data about the data subject held by the data controller which the controller no longer has the authority to retain.

Figure 1. Showing right No. 16 Correction of personal data.

- **Right to Restrict Processing.** Individuals can request the restriction of processing their personal data under certain conditions. This would allow users to limit how their data is used by third parties like Cambridge Analytica.
- **Right to Data Portability.** Individuals can request their data in a commonly used format and transfer it to another data controller. This would enable users to move their data to a more secure platform if they wished.
- **Right to Object.** Individuals can object to the processing of their personal data, especially for direct marketing purposes. Users could have objected to their data being used for political advertising.
- **Right to Compensation.** Individuals have the right to seek compensation for damages suffered due to unlawful processing of their personal data. Affected users could potentially sue for damages resulting from the data breach.

26. Right to prevent processing of personal data for direct marketing.

(1) A data subject may by notice in writing to a data controller, require the data controller to stop processing his or her personal data for purposes of direct marketing.

(2) A data controller shall within fourteen days after receipt of the notice inform the data subject in writing that the data controller has complied or intends to comply with the notice of the data subject, or of the reasons for non-compliance.

Figure 2. Showing right No. 26 to prevent processing of personal data for direct marketting

3. Role of the General Data Protection Regulation (GDPR)

The **General Data Protection Regulation (GDPR)** is a comprehensive data protection law enacted by the European Union (EU) that came into effect in May 2018.

This is how it might have influenced the Cambridge Analytica case.

- **Heavy Penalties.** GDPR imposes significant fines for non-compliance, up to 4% of global annual turnover or €20 million, whichever is higher. This would have been a strong deterrent against Facebook's lax data-sharing practices.
- **Right to Erasure.** Under GDPR, individuals have the right to have their data deleted. This would have allowed users to request the removal of their data from both Facebook and Cambridge Analytica's databases.
- **Strict Consent Requirements.** GDPR requires explicit and informed consent for data collection and processing. This means that Facebook would have needed clear, unambiguous consent from users before sharing their data with Cambridge Analytica.
- **Data Minimization.** GDPR mandates that only the minimum amount of data necessary for a specific purpose should be collected. This would have limited the extent of data that Cambridge Analytica could access.
- **Transparency and Accountability.** GDPR requires organizations to be transparent about how they use personal data and to implement measures to ensure accountability. Facebook would have had to disclose its data-sharing practices and demonstrate compliance with data protection principles.
- **Data Protection Impact Assessments (DPIAs).** GDPR requires organizations to conduct DPIAs for high-risk processing activities. Facebook would have had to assess the risks associated with sharing data with third parties like Cambridge Analytica.

If GDPR had been in effect at the time of the Cambridge Analytica scandal, the outcome might have been significantly different.

- **Increased Transparency.** Facebook would have been required to be more transparent about its data-sharing practices, potentially preventing the scandal from occurring in the first place.
- **Prevention of Data Misuse.** The strict consent requirements and data minimization principles would likely have prevented the unauthorized access and misuse of user data by Cambridge Analytica.
- **Legal Consequences.** Facebook could have faced substantial fines and legal actions under GDPR, which would have served as a strong deterrent against future data breaches.
- **User Empowerment.** Users would have had more control over their data, including the right to access, rectify, and erase their information, thereby reducing the impact of the data breach.