Seminar Exercise 9: Twitter data

Data Collected by Twitter :

Twitter gathers different types of data. It collects user-provided details like display name, username, email, phone number, date of birth, payment info, location, and even address books. It also tracks usage data, including tweets, likes, reposts, bookmarks, direct messages, ad interactions, and device details such as IP address, browser type, operating system, and installed apps. On top of that, Twitter pulls in data from third parties like advertisers, business partners, and external services. All of this helps personalize the user experience, improve security, and analyze platform activity.

Data Collected by Users from Twitter :

Users can access public data like tweets, profiles, and engagement stats. API access requires approval and comes with restrictions on storage and redistribution. Developers must follow update rules by removing or modifying content if it changes or gets deleted on Twitter. Off-platform data matching is only allowed with explicit user consent or public data. There are also commercial restrictions, Twitter doesn’t allow its data to be used for external ad targeting or paid engagement. Strict policies are in place to balance accessibility and privacy protection.

Pros and Cons of Twitter as a Data Service :

Twitter is a powerful data source, great for tracking trends, analyzing public sentiment, and studying market behavior. Businesses and researchers use its data to understand user engagement and brand perception. The platform follows privacy laws like GDPR and CCPA, ensuring transparency and user control. It also offers structured API access with different tiers, making it flexible for developers. Plus, Twitter enforces strict policies to prevent spam, abuse, and data misuse.

On the downside, Twitter heavily restricts how its data can be used, stored, and shared, which can be frustrating for developers. While it prioritizes privacy, it still collects a lot of user information, including location and interactions, which raises concerns. Compliance with privacy laws can be complex, and API access can get expensive, limiting smaller projects. Developers must also constantly update stored data to reflect changes on the platform, adding extra work.