1.1P: Reflection on Data-driven Information Systems around you

In this task, you will reflect on three data-driven information systems (applications or software) that you use in your daily life. For each system, you will explore the followings:

1. What is the system and what sort of data it uses?
2. How do you use the data? What would happen if that data was not available to you?
3. Who/how/where the data is generated, captured, stored, and managed?
4. Do you see any risks/concerns around the security and privacy of the data?

- **System 1: Google Maps**
  - ✓ **System Overview**: With capabilities for route planning, satellite images, real-time traffic updates, and detailed maps, Google Maps is a popular mapping service. The system makes use of a variety of data types, such as business information, user reviews, location data, traffic data, and geographic data.

  - ✓ **Data Usage**: I mostly use Google Maps for navigation, whether I'm trying to figure out how to go to a new place or how long it will take me to get there given the traffic. It would be much harder to navigate unknown regions without access to the data that Google Maps provides. For the purpose of choosing my routes and travel times, I rely on the data's correctness. I would have to use less effective navigational methods, like paper maps or asking for directions, which might not always be accurate or up to date, if this data were unavailable.

  - ✓ **Data Generation and Management**: A variety of sources provide the data that Google Maps uses. Numerous mapping organizations and satellite suppliers give the geographic data and satellite pictures. In addition to collaborating with other data providers and transportation departments, GPS data from users' mobile devices is used to gather traffic statistics. Users that have chosen to participate in location tracking services provide their location data. All of this data is processed and kept on Google's servers, where it is updated and monitored continuously to guarantee relevancy and accuracy.

  - ✓ **Security and Privacy Issues**: Although Google Maps offers useful features, the gathering and use of private location data may carry certain hazards. Users' agreement is required before sharing location data with Google, which presents privacy issues with tracking and storing people's movements. Large-scale storage of sensitive location data also carries security issues, including the possibility of data breaches and illegal access to personal data. Google protects user data with a number of security measures, including encryption and access controls, but security flaws might always be exploited.

- **System 2 : Online Banking App**
  - ✓ **System Overview**: Users can easily access their bank accounts through online banking apps like Chase Mobile, which enable them to check balances, transfer money, pay bills, and handle their finances from a distance. These applications depend on a variety of data types, such as transaction history, account information, and user authentication data.

  - ✓ **Data Usage**: I transfer money between accounts, check recent transactions, and keep an eye on my account balances using the Chase Mobile app. To effectively manage my funds and remain updated about my financial situation, I need access to this data. I wouldn't be able to obtain this data without resorting to more conventional banking techniques, like going to a physical bank branch or using an ATM, which might not provide the same degree of ease or up-to-date information.

  - ✓ **Data Management and Generation**: When consumers make deposits, withdrawals, or transfers from their bank accounts, they generate the data that online banking apps need. The bank's servers receive this data securely in order to process and store it. Strict security protocols, such multi-factor authentication and encryption, are used by banks to guard against fraud and illegal access to their customers' financial information. To further guarantee the security and integrity of their systems and data, banks follow legal mandates like the Payment Card Industry Data Security Standard (PCI DSS).

  - ✓ **Security and Privacy Issues**: Since online banking apps handle private financial information, hackers find them to be appealing targets. The safety of user data is a source of worry because of things like identity theft, phishing scams, and data breaches. To protect consumer financial information, banks invest in cybersecurity solutions like intrusion detection systems, firewalls, and fraud tracking tools. Users must, however, take precautions to safeguard their own data as well. Some of these precautions include utilizing strong passwords, turning on biometric authentication, and refraining from sending private information over unprotected networks. All things considered, even though online banking apps are accessible and convenient, consumers should be aware of security threats and take the necessary safety measures to safeguard their financial information.

- **System 3: Fitness Tracking App**
  - ✓ **Overview of the System**: Users can measure their physical activity, such as riding, jogging, and other workouts, using fitness tracking apps like Strava. These applications gather information on the user's performance and fitness progress, including GPS coordinates, heart rate, distance traveled, and length of workout.

  - ✓ **Data Usage**: I log my runs using Strava and use it to see how I've improved over time. The app provides extensive information, like pace, distance, and elevation gain, by utilizing the data gathered during exercises. Having access to this data helps me stay motivated, track my progress, and create goals. It would be much more difficult to properly track my fitness levels and advancement without this data.

  - ✓ **Data Generation and Management**: Wearable fitness trackers and smartphones with GPS capabilities are the main sources of data used by fitness monitoring apps like Strava. The application gathers data in real-time from users as they interact with it; this data is then uploaded to the app's servers for processing and analysis. Users can decide whether to share or keep their workout data private, and they have control over their data privacy settings. In order to preserve data integrity and safeguard user privacy, app developers are in charge of handling and keeping this data securely.

  - ✓ Fitness tracking apps provide useful information about a user's physical activity and health, but there are worries about the security and privacy of the data they collect. GPS data can provide sensitive details about a user's daily activities and routines, which raises privacy concerns regarding possible tracking or spying. Users' security and privacy may also be jeopardized by the possibility of data breaches or illegal access to their fitness records. It is imperative for fitness app developers to incorporate strong security features, like encryption and secure authentication procedures, to safeguard users' data from unapproved access or misuse.