**Weekly Assignment 12**

Answer the following questions:

1. Based on the probabilistic rule from the lecture, what are five data examples you can think of that might be considered privacy data? Discuss why you chose them for each example.

Based on the probabilistic rule that data giving a greater than 50% chance of identifying someone should be treated as privacy data, here are five examples:

1. **Browser History**:
   * **Why**: Browser history can reveal a lot about a person's interests, behaviors, and even specific personal details. With enough browsing data, it becomes possible to profile and identify an individual.
   * **Example**: Frequent visits to specific medical websites could hint at particular health conditions.
2. **Geolocation Data**:
   * **Why**: Continuous or frequent location tracking can pinpoint a person's home, workplace, and daily routines. This can be used to identify the individual with a high degree of accuracy.
   * **Example**: GPS data from a mobile device can show a person’s daily commute, favorite places, and even exact home address.
3. **Purchase History**:
   * **Why**: Purchase history can reveal specific preferences, financial status, and patterns. Combining this with other data points increases the likelihood of identifying the person.
   * **Example**: Regular purchases from a specific grocery store, combined with loyalty card usage, can pinpoint an individual’s identity.
4. **Social Media Activity**:
   * **Why**: Posts, likes, shares, and comments can provide detailed insights into a person's life, including their thoughts, relationships, and habits.
   * **Example**: A pattern of social media check-ins at certain locations or events can lead to identification of the person.
5. **Fitness Tracker Data**:
   * **Why**: Data from fitness trackers can include highly personal information like heart rate, sleep patterns, and physical activity levels. When correlated with time and location data, it can identify individuals.
   * **Example**: Data showing frequent runs in a specific park at a specific time can identify an individual when combined with other data sources.
6. List three differences between CCPA and GDPR regulations for privacy.

 **Scope and Applicability**:

* **GDPR**: Applies to all companies processing the personal data of individuals residing in the EU, regardless of the company’s location.
* **CCPA**: Applies to businesses that meet specific criteria (e.g., annual gross revenues above $25 million, or data on more than 50,000 consumers, households, or devices) and do business in California.

 **Consumer Rights**:

* **GDPR**: Provides a broad range of rights including right to access, rectification, erasure, restriction of processing, data portability, and objection to processing.
* **CCPA**: Focuses on the right to know what personal data is being collected, the right to delete personal data, and the right to opt-out of the sale of personal data.

 **Penalties and Enforcement**:

* **GDPR**: Imposes strict fines for non-compliance, up to 4% of annual global turnover or €20 million, whichever is higher.
* **CCPA**: Imposes fines up to $7,500 per intentional violation and $2,500 per unintentional violation, with enforcement by the California Attorney General.

1. If you were to start a new Internet business, what would you need to have in place to satisfy privacy regulations for your new business?

 **Data Protection Policies**:

* Implement clear data protection policies detailing how personal data is collected, used, stored, and shared.
* Ensure compliance with GDPR and CCPA by documenting data processing activities.

 **Consumer Rights Management**:

* Set up processes to handle consumer rights requests, such as access, deletion, and data portability requests.
* Provide easy-to-use tools for consumers to exercise their rights, including opt-out mechanisms for data sales under CCPA.

 **Data Security Measures**:

* Establish robust security measures to protect personal data, including encryption, access controls, and regular security assessments.
* Develop a data breach response plan to notify affected individuals and authorities as required by GDPR and CCPA.

 **Data Protection Officer (DPO)**:

* Appoint a Data Protection Officer if necessary (mandatory under GDPR for certain types of data processing).
* Ensure the DPO is involved in all issues relating to the protection of personal data.

 **Training and Awareness**:

* Conduct regular training for employees on data protection and privacy regulations.
* Promote a culture of privacy awareness within the organization.

 **Third-party Compliance**:

* Ensure that any third parties processing personal data on behalf of your business are compliant with GDPR and CCPA.
* Use data processing agreements to formalize responsibilities and obligations regarding data protection.

When you are finished upload this document into Canvas for your submission.