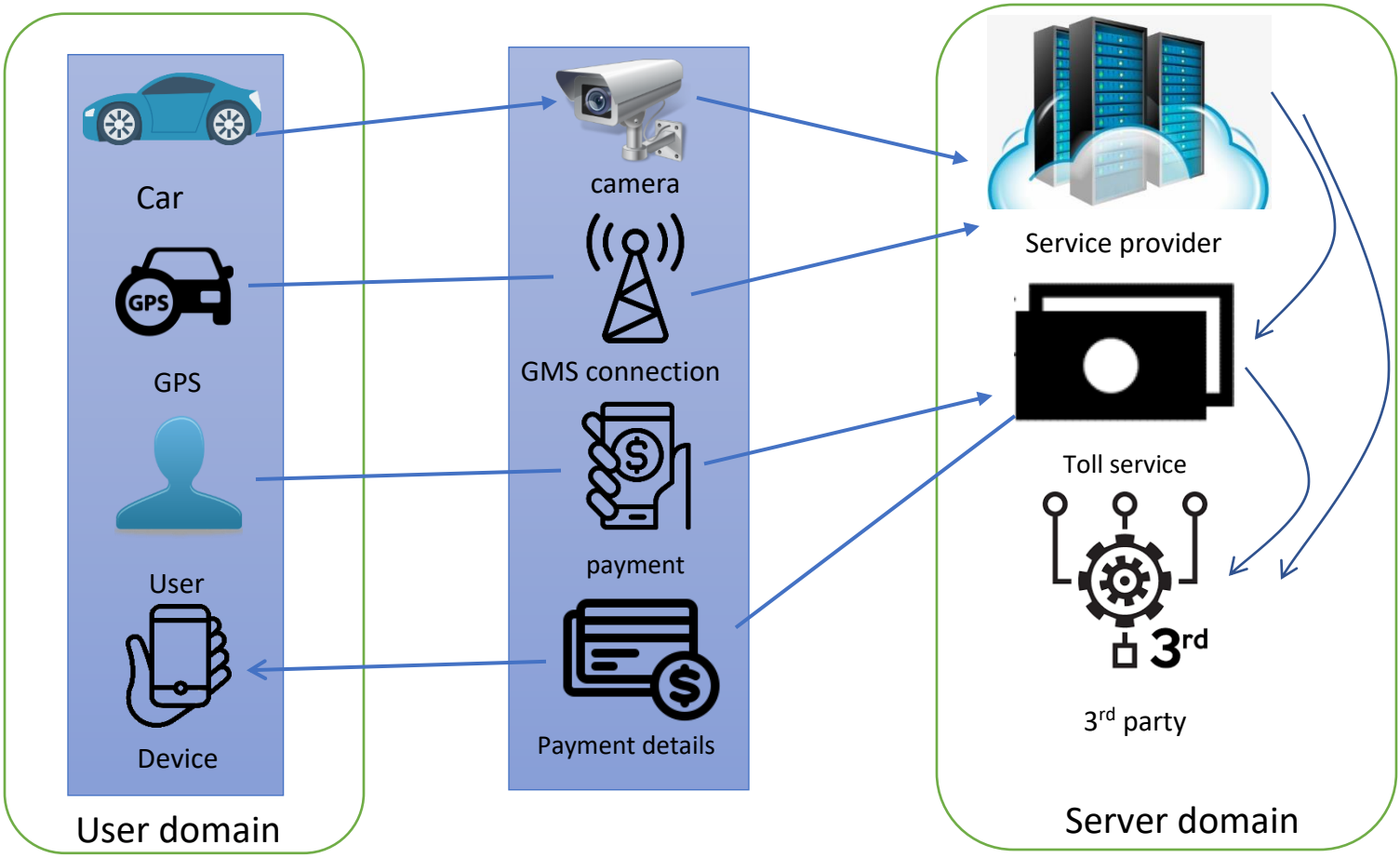
Inaam Kabbara

Case Study2: European Electronic Toll Service

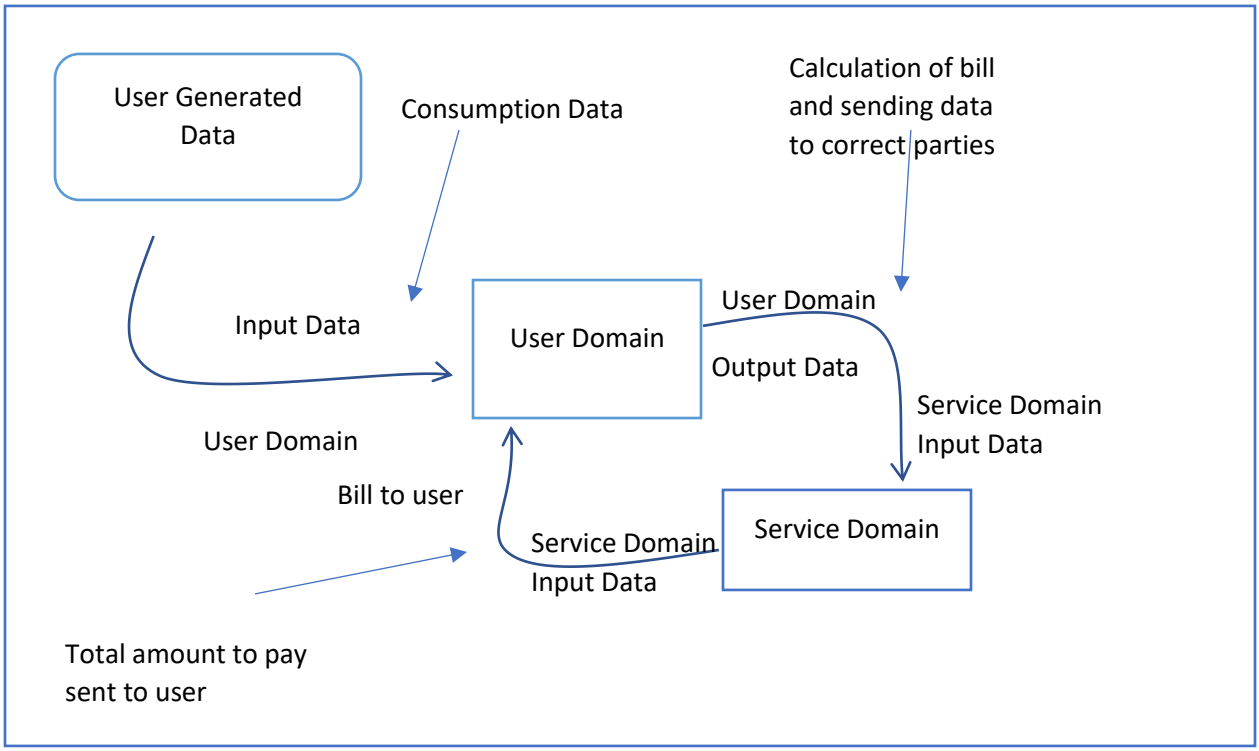
Activity 1:



Activity 2:

User domain	Server domain
A vehicle's identification plate or any other type of scannable card or QR code.	The license plate, the vehicle's specs, the user's position, and other data may be stored on the servers of the service provider.
Location of the vehicle to determine road use fees	Transactions ought to be tracked by toll services. As a result, they will possess transaction logs, billing information, and certain other personal user data.
The user's complete name, phone number, or other device information used to create the transaction.	Third parties should only possess the information necessary for them to function.
Information used by the user to complete the payment	

Activity 3:



1. Client tools not functioning properly (margin of error too high, user misuse, etc)
    a. Tools that are utilized or applied may be prone to mistakes, which could give servers inaccurate data. Effects might include:
        i. The client QR/scannable interface was either not scanned or was scanned for the wrong person.
        ii. Over time, the GPS margin of error results in negative fees for consumers.
        iii. Malicious user behavior to avoid payment

Risk analysis: While points a.i and a.ii are frequent, their influence is minimal. In contrast, the frequency and impact for point a.iii are low and moderate, respectively. Point a.iii, on the other hand, is not under the service provider's control because it is a part of the trusted user domain.

2. Problems with Data Storage
    a. A data retention duration
    b. Data anonymization policy
    c. Do the data show any patterns regarding the users?

Risk assessment: Because of the continuous transmission of data in this case, the frequency of such events may be deemed to be high. Additionally, data breaches will have serious repercussions if data is maintained indefinitely or in an unencrypted, non-anonymized form. having a significant impact

3. Issues with data sharing
    a. Is any private information shared in a situation where it might be prevented?
    b. Was more data transmitted that wasn't necessary?
    c. Can other organizations violate data privacy? (ISPs, man in the middle attacks)

Risk assessment If badly executed, high frequency occurrences with great impact could

4. Server Issues

a. Any or all servers may be unavailable, which could result in:
    i. Data loss
    ii. Unrecorded transactions
    iii. Profit loss

Risk assessment: As was already noted, there is a chance that data and/or financial losses will occur, making this problem a medium impact event. Servers are not anticipated to crash repeatedly, though. As a result, the likelihood of such events is low.

5. Issues with Data Disposal
    b. How long will the data be kept once the user opts out (for travel or relocation, for example)?

Risk assessment: In the event that all data is retained indefinitely, the impact of breaches getting significant amounts of data is high. Since data breaches are not particularly likely to occur, the frequency is minimal.

6. Data processing problems
    a. Are only the necessary pieces of information used, or are there extras that could risk user privacy?
    b. Were there any errors that resulted in overcharging or undercharging the user?

Risk evaluation High frequency, even for the same user, as a result of repeated calculations over time. Impact is negligible since such errors have negligible repercussions.

Activity 4:

We should follow the six principles as much as we can to reduce privacy risks.

The 6 principles are:

1. Minimize collection: Considering that the client is a reputable domain and the service provider should operate on the presumption that the data provided is accurate, the information from the aforementioned section is something we should accept.
2. Minimize Disclosure: Data centralization is the problem. Here, we should set up numerous databases that can handle requests from load balancers and the like in the event that one database fails. In order to reduce the quantity of data that each server possesses and prevent redundant data storage, database sharing may also be employed. The service provider, toll service, and every other entity obtaining the data might all use this system.
3. Minimize Likability: Instead of disclosing the location, it would be preferable if the client handled some of the data processing. This might be achieved by asking the client to determine the distance traveled and submit the necessary data to the service provider. This guarantees that the service provider will only utilize the data required for operations. Furthermore, this processing aids in removing part of the user information that might be kept on the service providers' logs, further enhancing customer privacy.
4. Minimize Centralization: The encryption, distribution, and anonymization of data at rest should be maximized. This protects privacy in the event that a breach occurs by ensuring that potential hackers cannot access any potentially sensitive information. These precautions are crucial not just to prevent breaches but also to protect user privacy on the servers of the service provider.
5. Minimize Replication: In order to guarantee the integrity and confidentiality of the data being shared, the solution to these problems depends on the use of secure methods of data sharing that include encryption and signature. It is crucial to remember that in addition to using effective encryption methods, it is also crucial to make sure that the entire data security process makes it challenging for outsiders to understand the data. For instance, even though AES256 is thought to be a strong symmetric encryption, utilizing it with plaintext HTTP is not regarded as best practice. Instead, employing TLS and encryption strengthens the entire chain.

6. Minimize Retention: It is important to retain data as long as is necessary under the law. All user-related data must be properly disposed of once the legal time period has passed.