Justin Bland SIT123: Data Capture Technologies ID: 218478549

Lab Report 7

Question 1:

Firstly, publicly sharing someone data like GPS tracks with identifiable information, in my opinion is a very bad idea and could have potentially dire consequences.

Secondly, the user should be notified that their data was going to be used in this manner, additionally the organization releasing this data should have written permission from the user to use their data in this fashion.

Question 2:

In this scenario, the users who have had their data released, (Names and GPS Traces) have had their daily routines possibly including home and work locations made available to the public, this can leave them to fall victim to any number of malicious actors, anything from stalkers, to even life endearing issues (this could hold true for people who have left domestic violence situations). Additionally, the users could be open to blackmail and ransom situations where someone could imply a user was doing something untoward because of their location and essentially hold the user hostage until their demands are met.

Question 3:

In this scenario, if the company providing the service to John does not have strict policies to ensure his data is protected, like the previous scenario, John could fall victim to any number of malicious actors, Johns data shows where he is in the house, if he is home and whether he is awake or asleep, and likely because of the service the company is providing I would assume they would have at least basic information on any Medical Conditions that John may suffer from.

if anyone with malicious intensions has access to this data they could do anything from stalking through to Life Endangering Actions.

Question 4:

I have mentioned some of these previously however the main effect that sticks in my mind would be with the GPS Tracks, if someone has left a Domestic Violence situation their partner could obtain their home address and any regularly traveled places, this could in some circumstances endanger the life of this person.

Question 5:

For Scenario 1, as a starting point I would remove as much personally identifiable information from the data as possible (e.g. Names, IDs etc.), then if the actual GPS co-ordinates are not required I would remove them. If they are required I would consider using an automatically generated number for each track to offset the latitude and longitude (discarding the offset number so that the co-ordinates can not be reverse engineered), I would also consider hashing the track data to obfuscate it incase of data breach.