ARCADIS Design & Consultancy for natural and built assets

Mobility as a Service: Navigating the challenges of a MaaS data sharing future

Expanding city populations pose many challenges, especially when it comes to mass transit. The demands placed on infrastructure are increasing, along with concerns about pollution, precisely at a time when societies wish to reduce public health risks. Arcadis's Tim Strong and Dr Danny Steed from ReSolve Cyber explore what this means from the perspective of data privacy and security issues.

There is a growing belief that Mobility as a Service (MaaS) has the potential to alleviate these problems, if implemented in line with clear public policy. MaaS could reduce the need for car ownership and contribute to reducing congestion, improving air quality, enabling economic growth and improving quality of life for all citizens.

As we move towards a driverless future in which Connected and Autonomous Vehicles become ubiquitous, the potential for MaaS adoption grows. With this comes the opportunity for a city to improve services to meet known and predicted customer needs. The more people that participate and share their data, the better the service can become.

But what might be the result of this mass data-sharing future? Is sufficient consideration being given to potential unintended consequences, particularly how MaaS customers might feel about how much the system knows about them? This is especially relevant if MaaS achieves significant levels of penetration. Perhaps then we'll reach a tipping point when being a MaaS customer moves from being a choice to a dependency, when no other attractive or viable travel options are available.

DATA TRAILS

The beating heart of the MaaS system will be the data and the system that processes and communicates it. This will rely on users accessing the service through devices like smartphones. But a data-centric service inherently carries cyber security concerns, such as who owns the data, you or the service? What constitutes appropriate use? Should user data be automatically shared with law enforcement and emergency services?

With the impact of GDPR in Europe, as well as the furore over the conduct of organisations like Facebook, how data is used sits at the forefront of awareness. If you live in a large city, it would be near impossible not to use a MaaS system once operational. But how much data must a user volunteer? And what uses are not only permissible, but acceptable and even desirable?

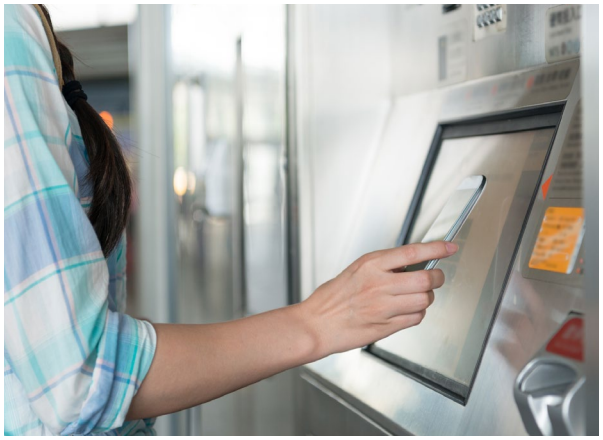
A DAY IN THE LIFE

This data dynamic is best illustrated through a fictional scenario from the perspective of a commuter living 20 miles out of the city where she works. Sarah's journey is typical: she uses the mainline train to reach the city centre, where she finishes her journey by cycling. During the day Sarah uses a variety of services to travel around the city, including the underground, bus services and taxi.

Under a MaaS system Sarah would use a smart device as her primary point of access. There would be no need for separate rail passes, bus tickets, bike fobs and taxi payments; one account would allow access to all. This ease of use alone is a huge incentive, highlighting one of the many advantages of a MaaS system.

But consider the data trail; Sarah taps into her home railway station with her phone, having paid for her coffee through her phone by credit card, as well as registering loyalty points through her phone at the coffee store. Already Sarah has voluntarily registered three data points that reveal her commuting habits and breakfast preferences.

While travelling, Sarah sees an advertising board with an offer from a major credit card provider; she 'Googles' the offer and visits the web page for more information. The credit provider, via tracking on Google AdWords combined with the location services on Sarah's phone, adds Sarah to the list of people in close proximity to the poster for follow-up targeted advertising.



Once Sarah leaves the train, she takes out a registered bike for her journey. The bike immediately logs itself out to the relevant transport authority, while the handlebar camera takes a photo of Sarah's face for verification purposes. While cycling, Sarah passes numerous shops, coming within reach of the data beacons that register pings from Sarah's mobile device. Those shops begin pushing tailored ads towards Sarah's device in the hope of getting her custom the next time she checks her phone.

Finally, Sarah docks her bike close to work. The bike registers itself as locked, with the inbuilt GPS chip having recorded Sarah's journey for the MaaS provider to gather cyclist's journey routes, times, and behavioural patterns for further analysis.

For Sarah, this is merely one example of passive data collection. MaaS provides ample opportunity not only for a simpler and more user-responsive journey experience, it also creates a unified system of data collection that would be extremely attractive for everyone from transport authorities and law enforcement to advertisers and retailers. Major cities represent one of the most efficient means of accessing millions of potential clients and customers.

USER BEWARE – TOO HIGH A PRICE TO PAY?

This raises numerous questions about how comfortable - and even aware – users need to be of the data price that comes with accessing a MaaS network. Let's consider some examples:

Advertising

Advertising will be significantly disrupted by MaaS. Cities offer a large pool of customers, meaning the cost of advertising would hit a premium. But what code of conduct would a MaaS provider subscribe to in judging the appropriate level of access to customer data? Would they permit push advertisements based on user interaction with QR codes and data beacons? Would they enable a push notification system for preferred vendors such as coffee shops and outlets in their stations, or in proximity to bike racks and car pick-up points?

The risk is that users opting in to a MaaS system won't be aware of this advertising environment. The future of marketing could lie in targeted advertising based on MaaS providers allowing advertisers access to data points. This raises the question of informed consent, in which people need to know how their data is used as a result of their custom.

Data tracking

In a world of big data and artificial intelligence, service providers will be analysing the stream of data from users for many reasons. This might include predicting commuter bottle necks; anticipating probable accident points; or analysing the most frequented cyclist routes for lane and signal improvements.

Once again, the question is around informed consent. When do these analytic practices cross an ethical line? Any user buying into a MaaS system should be aware that even if they are not being targeted by advertisers, then their data is certainly contributing to a big data set serving numerous analytic purposes. MaaS providers need to develop a transparent system of practice, whereby users are afforded the opportunity to act as trustees of how such practices take place, and for what purpose.

Sharing with law enforcement/ emergency services

The partnership with law enforcement and emergency services is a double-edged sword. Access to a constant and ever-increasing big data set - in real time – could allow for a more efficient response to any incident. For example, if criminals try to escape using a self-driving fleet car, real time facial recognition could identify perpetrators and remotely disable the car and lock the doors, helping law enforcement apprehend the suspects.

Conversely, police forces in London have already courted controversy and even threatened legal action over the use of facial recognition technology. In a liberal society, it is a core argument and position that people should not be subject to mass surveillance without probable cause, and that the police should not automatically have a record of people's movements through a MaaS system without there being a legal requirement to.

A delicate balance would need to be reached; how much data should law enforcement and emergency services have access to? What access is appropriate to optimise responses that potentially save lives, when balanced against reasonable civil liberties?

Whatever MaaS system comes to the fore, law enforcement and emergency services will need to build a close relationship with the provider. Users must be in an informed position to offer a view on how close that relationship should be.

RESPONSIBLE USE

MaaS has the potential to deliver huge advantages and help solve some of our cities' most challenging problems around pollution, mass transit, congestion, and ease of use. Yet there is also a significant cyber security concern around the application of such a data-driven service.

What is important is to begin preparing for the cyber security questions that MaaS will present, lest users and providers find themselves committed to a system that is not prepared for and informed about these challenges. If the system appears to know more about you, your travel habits and your preferences than you are comfortable with, how will you feel about using the system, and what if MaaS becomes a necessity rather than a choice? MaaS must be designed with these data and user perceptions firmly in mind.

With big data comes big responsibility.

CONTACT US

Tim Strong

Transport Innovation Director
E tim.strong@arcadis.com