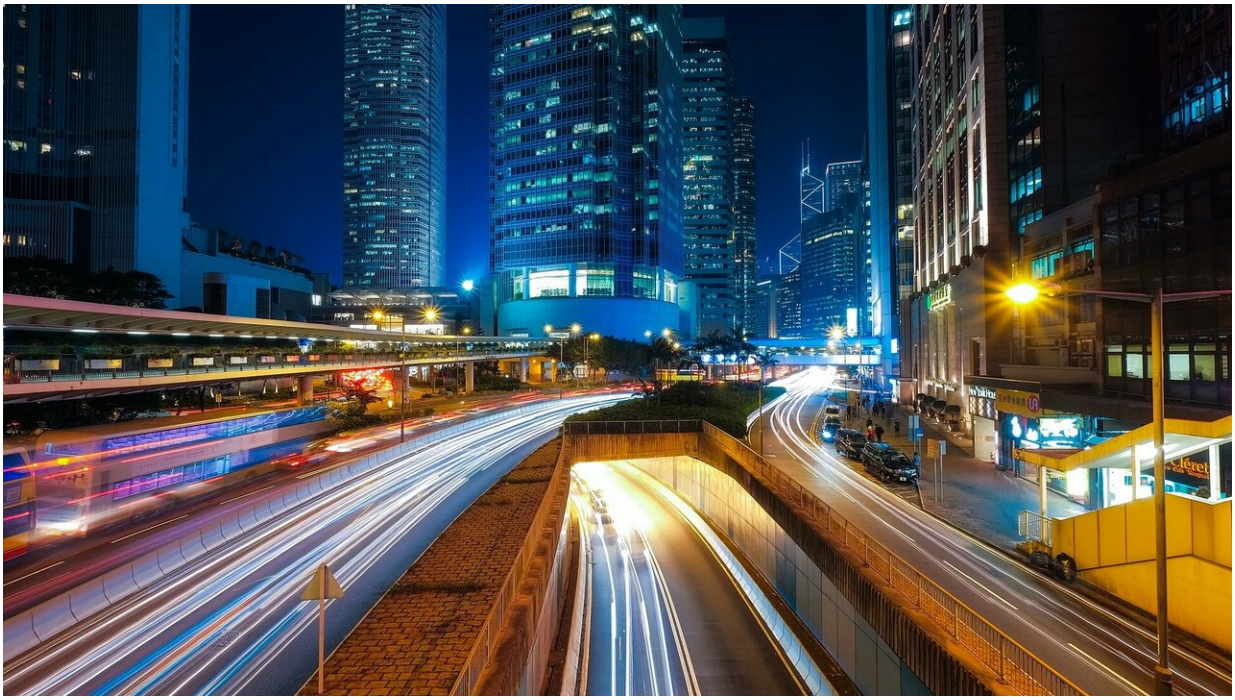
Will congestion charging come with a privacy toll?

August 28 2024



Credit: CC0 Public Domain

As New Zealand edges closer to adopting congestion charging in its busiest cities, University of Auckland researchers are highlighting a critical but often overlooked issue: privacy.

In a new paper published in *Policy Quarterly*, Professor Tana Pistorius (Business School) and Isa Seow (Research Fellow, School of Computer

Science) discuss the technology that could be utilized in the rollout of congestion charging systems such as satellite tracking, number plate identification cameras and short-range communication systems.

Each of these technologies carries inherent risks to individual privacy and pose significant challenges within the framework of the Privacy Act, according to the researchers.

Number plate recognition cameras capture images of vehicles and their license plates but can record additional information, such as the vehicles' drivers and passengers. And with the increasing resolutions of cameras, the researchers say there's a heightened risk of capturing sensitive biometric information, raising concerns about the recording and storage duration of high-resolution facial data.

Aotearoa's biometric regulations are still evolving, says Professor Pistorius, and the widespread use of new automatic number plate recognition technology and software, which could be required if congestion charging systems are introduced, can accentuate the risks associated with the processing of biometric data.

Seow points out that there are further challenges regarding what such data could be used for, with significant concerns around analytics, crime tracking and prediction, all of which could potentially infringe on individual privacy.

Meanwhile, navigation satellite technology can pinpoint a vehicle's location with remarkable accuracy, raising concerns about daily and repeated surveillance.

Another potential option, dedicated short-range communication systems, which facilitate communication between vehicles and roadside equipment, are particularly risky if they store data related to payments

and vehicle location history on card systems.

Seow says congestion charging systems are exposed to data risk and have been targeted by cybercriminals overseas.

The researchers stress that no matter what technology is used, any data collected must be limited to what's strictly necessary for the intended purpose.

"A privacy impact assessment, namely a review of the privacy implications and the mitigation of risks, should be undertaken by the government before anything is put in place to curb congestion to ensure that we have adequate safeguards," says Pistorius.

The researchers also sought public opinion through four focus groups, which saw Aucklanders and Wellingtonians express concerns about the implications of congestion charging systems on privacy. Questions were raised regarding the duration of data retention by the systems, potential security breaches, and the over-collection of data.

Respondents suggested that all data should be deleted after six months to mitigate privacy risks. They also advocated for clear regulations to protect against unwarranted police access to congestion charging data.

Other suggestions to help address privacy risks included anonymizing license plate information during transit or storage, implementing platforms for individuals to monitor their data across all government services, and establishing geolocation fences to confine data collection and viewing within city limits.

The researchers say these "fences," which are virtual boundaries that limit data collection and viewing to specific areas, would ensure people's data would not be collected while at home or outside congestion

charging zones.

More information: Isa Seow and Tana Pistorius. Automated Traffic Congestion Charging Systems: Privacy Considerations for New Zealand, *Policy Quarterly* (2024). ojs.victoria.ac.nz/pq/issue/view/1013/95

Provided by University of Auckland