Isa Seow and Tana Pistorius

Automated Traffic Congestion Charging Systems

privacy considerations for New Zealand

Abstract

New Zealand is considering implementing congestion-charging technologies to improve traffic flows and reduce emissions in city centres. This article reviews current congestion-charging technologies against New Zealand's Privacy Act 2020 and identifies varying privacy risks with these technologies. In particular, using global navigation satellite (GNS) systems and an on-board unit can pose a risk of collecting data that exceeds congestion management requirements. Additional issues arise from data processing for purposes other than congestion charging. Overall, the findings indicate the need for stricter control over who can process what type of personal data and the use and retention of such data.

Keywords privacy, technology, congestion charging, location tracking, surveillance, New Zealand

Isa Seow is a research fellow in the Department of Computer Science at the University of Auckland; email: isa_seow@post.harvard.edu. **Tana Pistorius** is a professor in the Department of Commercial Law at the University of Auckland.

Congestion charging, which involves a fee for driving into city centres to reduce traffic, is recognised as a solution to urban inefficiencies affecting businesses (Asian Development Bank, 2015, p.5). The New Zealand Institute of Economic Research estimates decongestion benefits in Auckland to be of the value of $0.9–1.3 billion annually (Ministry of Transport, 2020a). Additionally, congestion charging promises to improve New Zealand's environment and quality of life. The current government acknowledges challenges for low-income groups, but sees congestion charges as part of a broader plan to shift from road user charges and petrol taxes to manage traffic demand. The minister of transport, Simeon Brown, anticipates a two- to three-year timeline for implementation (Orsman, 2023).

Congestion-charging schemes can be categorised in several ways (de Palma and Lindsey, 2009). These dimensions include: the type of scheme, encompassing facility-based, area-based or distance-based variations; the extent to which tolls vary

over time, often referred to as time-based differentiation; additional factors for toll differentiation, such as the type of vehicle; and the utilisation of various technologies, depending on the enforcement model. The potential charging models encompass corridor (applicable to highways), cordon, area, network and lane-based systems. Additionally, newer charging models, such as distance travelled-based schemes, are undergoing experimentation (Cheng et al., 2019). The essential functionalities of congestion charging systems include data collection about vehicles, vehicles' measurement or location, communicating with in-car devices, and providing payment methods and evidence for enforcement. These functionalities are crucial for effectively operating and implementing congestion-charging systems.

Three primary technologies track vehicles. First, automatic number plate recognition (ANPR), also known as automated licence plate recognition (ALPR), employs cameras to identify vehicles and their licence plates without needing embedded vehicle technology. These systems utilise optical character recognition (OCR) to extract licence plate numbers from vehicle registration plates captured through video recording (de Palma and Lindsey, 2009). Second, the global navigation satellite (GNS) system encompasses satellite technologies that provide positioning, navigation and timing services (GPS.gov, 2022), offering precise vehicle identification with accuracy ranging from 1 to 2.5 metres (Li et al., 2022). Typically, GNS systems utilise an on-board unit attached to the vehicle, similar to mobile phone technology. Finally, dedicated short-range communication (DSRC) functions, like radio frequency identification (RFID), facilitate communication between vehicles and nearby receivers. In DSRC systems, electronic tags on on-board devices are recognised as they pass specific beacons (toll points) installed along the road. DSRC, a subset of RFID, offers higher data rates and longer ranges compared to traditional RFID toll applications, with data rates of up to 25 megabits per second and a range of up to one kilometre (Ukkusuri et al., 2008).

Since 2009 the New Zealand Transport Agency (NZTA) has used ANPR for electronic toll collection on three toll roads: Takitimu Drive toll road in Tauranga, Tauranga Eastern Link toll road, and the Northern Gateway toll road north of Auckland.

New Zealand's current congestion review and toll charging

The investigation into congestion pricing outlined in the consultation technical report *The Congestion Question*, produced by the central government and Auckland Council (Ministry of Transport, 2020a), proposed implementing congestion charges in Auckland city. This proposal was supported by various agencies and ministries and aimed to address rising costs for transport infrastructure and to increase revenues. The report suggested initially implementing a congestion fee for users entering the Auckland central business district, with potential expansion to include surrounding strategic highways (corridors). The *Congestion Question* report and related investigations indicated that congestion reduction could be between 8% and 12% (Transport and Infrastructure Committee, 2021). Phil Harrison, from a professional consulting firm, highlighted significant economic benefits for Auckland from easing congestion (de Silva, 2023). Other cities, such as Tauranga and Wellington, also studied these proposals' potential benefits and impacts (Orsman, 2023).

Implementing a congestion-charging system would involve several key components and considerations. The fee structure proposed in the *Congestion Question* technical report (Ministry of Transport, 2020b) is $3.50 upon entering or exiting the business district during peak periods, with charges applying only once within a two-hour window, regardless of the distance travelled. Moreover, individuals could only incur a charge of twice the amount per day. To enforce payment, roadside cameras equipped with OCR technology, similar to those used in automatic toll roads, would capture vehicle information, with ANPR as the preferred vehicle detection technology. However, implementing this policy would entail upgrading the existing camera network and constructing additional stand-alone infrastructure. The *Congestion Question* report also proposes using apps and websites for manual or automatic payments and adding number plates to the user's account.

A current charging standard is already in place. Since 2009 the New Zealand Transport Agency (NZTA) has used ANPR for electronic toll collection on three toll roads: Takitimu Drive toll road in Tauranga, Tauranga Eastern Link toll road, and the Northern Gateway toll road north of Auckland. The current ANPR technology NZTA uses is ten years old and lacks support for crucial elements such as location-based charging, time-of-day charging and vehicle trip aggregation, which are fundamental for an expanded congestion-charging scheme. The existing toll road system implements a simple mapping of single-trip detection to a fixed single-vehicle charge and does not support new features (Ministry of Transport, 2019). A recent attempt to access the toll collection system's online payment portal found it inaccessible, indicating the need for system upgrades and technical improvements. The current tracking system leans heavily on ANPR technology to capture licence plates for road tolls. While ANPR enjoys widespread support for future adoption, authorities have not definitively dismissed GNS technology for future congestion charging.

New Zealand has implemented road user charging for non-petrol vehicles, and

individuals can make payments through various outlets, such as post shops, online platforms and Automobile Association offices (AA, n.d.). Road user charging bases charges on the distance travelled by these vehicles. While for smaller cars diesel tax is derived from the mileage device of the vehicle, larger vehicles are required to have a trackable device equipped known as the Hubodometer, which monitors the distance travelled. These devices can come in digital or manual variants, with the digital version featuring location tracking capabilities such as global positioning system (GPS) and GNS technologies. Given the current uses of ANPR and GNS technologies in New Zealand's transportation systems, it is reasonable to expect both technologies to be considered for congestion charging. Electric vehicles have been subject to road user charges since April 2024. EV drivers pay via a website by entering the vehicle's licence plate number and current odometer reading; the odometer reading is verified and tracked using vehicle registration databases and regular warrant of fitness certifications.

In addition to road toll technologies, New Zealand employs a camera detection system for 'T2' lanes, whereby vehicles with two or more occupants are allowed to use, aiming to promote car-sharing. Cameras in these T2 lanes distinguish single and multiple occupants and monitor vehicle occupancy. Both human and computer monitoring of these T2 cameras can pose privacy risks, particularly in distinguishing between actual occupants and dummies or mannequins. In short, video surveillance is already used on highway toll roads and T2 roads. However, these technologies present various levels of privacy exposure. The *Congestion Question* report acknowledges the necessity for a comprehensive examination of privacy risks. This article advocates reviewing these technologies and developments against general privacy concerns and the privacy principles entrenched in the Privacy Act 2020.

Privacy risks and implications of ANPR, GNS and DSRC technologies

In an article published by the American Bar Association, David Horrigan rightly asks if ANPR technology is a godsend for safety or an Orwellian nightmare. He then remarks, 'Perhaps it's both.' ANPR can draw an intimate portrait of a driver's life and may be used to target drivers who visit sensitive places such as health centres or places of worship (Horrigan, 2021). Other academics have written about the privacy concerns of ANPR technologies (Ziegler, 2023; Brayne, 2020). Some may argue that there is no reasonable expectation of privacy in a vehicle's number plate as it is there for the world to see. However, not only does the government oblige vehicles to have a licence plate, but it can also track your every move with that number plate. The impact of tracking extends to using data for surveillance, data analytics, and applications that can lead to unconsented uses or biases.

Although widely deployed, traffic monitoring technologies such as ANPR cameras pose other significant privacy risks. Such technology has the potential to inadvertently capture facial information or other sensitive details, which could then be exposed to human reviewers. There are instances where road camera systems have unintentionally captured private body parts instead of the intended traffic offences (News.com.au, 2023). With increasing resolutions of cameras, there is a heightened risk of capturing biometric information, raising concerns about the recording and storage duration of high-resolution facial data. New Zealand's biometric regulations are still evolving, and new camera technology and software accentuate the risks associated with such data. Furthermore, visual data captured by ANPR systems may inadvertently include details of children and vulnerable groups, potentially infringing on their privacy rights.

ANPR technology is primarily designed for traffic law enforcement. Still, governments have been known to use it for other investigations (Brayne, 2020), raising concerns about the transparency of the underlying algorithms for police surveillance. In New Zealand, for example, police flagged a car as stolen to trigger camera tracking in a homicide investigation (Pennington, 2022), leading to questions about the scope and oversight of such practices. The New Zealand Police maintain their own standards and privacy practices under the police manual (New Zealand Police, 2022). Moreover, ANPR systems may capture secondary infringements, complicating legal processes and leading to individual infringement data potentially being retained for extended periods. Human verification of infringements further introduces privacy risks, as drivers may not expect others to view their images. Concerns arise regarding forgery or theft of licence plates, which could result in privacy breaches if charges are incorrectly levied against innocent individuals. Systems have also been reported to have misread licence plate numbers in the United Kingdom, leading to wrongful penalties (BBC, 2018; Dron, 2022).

> In theory, DSRC – dedicated short-range communication – poses fewer threats to individual privacy than GNS technology due to its limited capabilities to track a vehicle's location.

GNS devices can track individuals' locations, travel times and distances, potentially revealing daily routines. For instance, the current road user charge tracking for large diesel vehicles, as indicated by official sources (NZTA, 2014), turns on and off at ignition. While such data collection is typical in law enforcement, explicit consent for extended application is not always obtained or transparent. Additionally, GNS technology may gather more enforcement data than required, posing risks from unauthorised access. In the event of vehicle theft, location

information stored by GNS devices may be accessed by unauthorised third parties or cyber criminals. Combining vehicle data with other sources such as social media could further heighten privacy risks.

In theory, DSRC – dedicated short-range communication – poses fewer threats to individual privacy than GNS technology due to its limited capabilities to track a vehicle's location. However, there is an elevated risk when DSRC systems store data related to payments and vehicle location history on card systems. This stored information, including data accumulated over time, may be susceptible to privacy breaches. Moreover, integrating DSRC with video surveillance for enforcement purposes introduces additional risks. Using technologies in tandem increases the risks to privacy.

A significant data breach in Sheffield, England, where 8.6 million images were accessed due to deficient online security, demonstrates that all data technologies are susceptible to cybersecurity threats (Griffiths, 2020). The ANPR server network was left unprotected and accessible simply by entering its IP address into an internet browser (Security, 2020). While deploying ANPR and other traffic systems serves practical purposes, the storing of data and payment information introduces cybersecurity risks, especially if devices store data locally. Law enforcement agencies are known to intercept personal data from traffic systems for various purposes, including criminal or terrorism analytics. Nations like Singapore openly declare the dual use of their road congestion charging systems for law enforcement purposes; governments such as China's utilise their camera systems for other forms of citizen surveillance (Drinhausen et al., 2021).

The New Zealand Privacy Act 2020

General privacy implications

The concerns highlighted above over the potential infringement on individuals' privacy due to the use of cameras and devices for locating and monitoring the movement of vehicles are valid, as privacy is a fundamental human right. Important international instruments such as the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (adopted on 23 September 1980) (OECD, 2021) and the United Nations Universal Declaration of Human Rights emphasise the right to privacy, the lawful processing of personal data and the protection of individuals against arbitrary interference (articles 2 and 12 respectively). Internationally, privacy protection is also upheld through statutes such as those in the United States and the general data protection regulations of the European Union. These legal frameworks provide mechanisms to safeguard individuals' personal information and ensure compliance with privacy standards.

While privacy is not explicitly mentioned in the New Zealand Bill of Rights Act, various legal statutes and the common law recognise the right to privacy in New Zealand, as evident by case law and precedent ...

While privacy is not explicitly mentioned in the New Zealand Bill of Rights Act, various legal statutes and the common law recognise the right to privacy in New Zealand, as evident by case law and precedent (Butler, 2013). The Privacy Act 2020 (replacing the Privacy Act 1993) aims to promote and protect personal privacy. The Privacy Act 2020 imposes rights and obligations for collecting, protecting and processing personal information.

ANPR, GNS and DSRC technologies pose significant challenges within the framework of the Privacy Act. Several principles are relevant, especially concerning congestion-charging systems and ensuing privacy concerns. We address only a few of those concerns below.

The first question is whether a photograph or video of a licence plate number constitutes personal information, as the Privacy Act only relates to the lawful processing of personal information. The answer to this question depends on a number of circumstances.

All traffic monitoring systems are based on the identification of vehicles. However, in the end, this also requires identifying persons rather than vehicles, as charging for the distance travelled or the presence of a vehicle within a location within a specific time requires billing a person (Custers, 2008, p.90). This is usually done by linking a vehicle to a person using the information in the number plate registration database to locate the vehicle's owner.

In the United States there is a growing public awareness of the threats to privacy and civil rights posed by tools of mass surveillance (Pedersen, 2019). In Virginia, for instance, it is no longer a moot question whether licence plate numbers constitute personal information. In 2015, in *Harrison Neal v. Fairfax County Police Department*,[1] the American Civil Liberties Union (ACLU) sought an injunction against the Police Department's 'passive collection' of licence plate data beyond an immediate need or existing criminal investigation. The ACLU brought this case to clarify that licence plate numbers could constitute personal information. The case is also of importance as it affects how long – if at all – Virginia police can keep licence plate data (Jackman, 2019).

In 2016 the Fairfax Circuit Court granted the Fairfax Police Department's motion to dismiss the case, saying that a 'license plate number' does not fall within the Government Data Collection and Dissemination Practices Act's definition of 'personal information'. The judge ruled that a licence plate number 'does not tell the researcher where the person is, what the person is doing, or anything else about the person'. On appeal to the Virginia Supreme Court, it was held in 2020 that ANPR images and associated data (the time when and location where the photographs of the number plates were taken) do meet the statutory definition of personal information under the Act, as the licence plate database

may be used to cross-reference ANPR data with the identity of an individual. The court held that the Police Department's 'passive use' of the ANPR system, therefore, violates the Government Data Collection and Dissemination Practices Act.

The United Kingdom's Information Commissioner's Office has confirmed that a car registration number and/or VIN can indirectly identify an individual and constitute personal data (Information Commissioner's Office, n.d.). The position is similar in New Zealand, where the registration number plate of a vehicle is matched with an individual registered owner or where the captured biometric data can be liked to an identifiable individual. Section 7(1) of the Privacy Act defines personal information as 'information about an identifiable individual'. It is important to note that the individual need not be identifiable from the information alone and that it is sufficient if identification can be made by a link to other information. So, where a photograph of a licence plate number can be linked to an identifiable individual (the motor vehicle owner), it will constitute personal information. Where the photograph includes biometric information about the driver and the number plate of the vehicle, it may involve the personal information of more than one person.

In the case of a company car the number plate of the vehicle will often not identify a person. So, where the photograph is of a vehicle's number plate only and that vehicle is owned by an incorporated company, it would not constitute personal information as it will not be linked to an identifiable individual. The situation differs for privately owned vehicles. As noted above, one may argue that this could be identifiable information and, therefore, personal information for privately owned vehicles and vehicles owned by sole traders. The Australian Privacy Foundation has noted that only a proportion of vehicles are driven by the registered owner, so the assumptions about the driver's identity are frequently wrong (Australian Privacy Foundation, n.d.). This may be so, but it is a moot point as the purpose of congestion charging is to collect payment from the registered owner of a vehicle because a vehicle was driven in a designated area during a designated time. Ultimately, the ANPR and related datasets will contain mixed personal and non-personal information.

The application of information privacy principles

The Privacy Act applies in relation to any action with respect to personal information (s4). The Privacy Act is applicable once a surveillance system is operational provided there is an element of intention or premeditation in collecting personal information about a particular person. This would apply where the personal information is 'sought to identify an as of yet unidentified individual caught in *flagrante* by surveillance' (Roth and Stewart, 2021, PA7.5(b)(ii)). This means the Privacy Act applies once any system to record vehicle movement to curb traffic congestion is in use.

Part 3 of the Privacy Act contains provisions related to information privacy principles. Information privacy principle 1 requires that personal information must be collected for a purpose, which then, in turn, determines, inter alia, to what uses it can be put and to whom it can be disclosed (s22). The concept of 'purpose' is a key concept in connection with the application of the information privacy principles (Roth, 2011).

Information privacy principle 1 underscores the importance of data minimisation, meaning that organisations should only collect the minimum amount of personal information required for their intended purpose. Principle 1 implements part of paragraph 7 of the OECD guidelines, the 'Collection Limitation Principle', which states that 'There should be limits to the collection of personal data'. Also called the 'minimality principle', this is expressed in information privacy principle 1(1) of the Privacy Act, which prohibits the collection of personal information unless it 'is collected for a lawful purpose connected with a function or an activity of the agency', and 'the collection of the information is necessary for that purpose' (ibid., p.3). While collecting data on vehicles and their movements is essential for congestion-charging systems, potential expansions of this purpose, such as data analytics and law enforcement activities, may thus raise privacy concerns under the Act. Additionally, technologies like GNS systems may collect location data beyond the congestion charging zone, and, as we have seen, cameras may capture personal information, such as facial data or other biometrics, beyond the licence plate numbers, leading to unnecessary data collection.

Woods (2017) notes that the data store in the National ANPR Data Centre in the United Kingdom can be used for data mining in a number of ways and could be used to create a detailed profile of a person ...

The various systems that are used to monitor traffic and vehicle movement imply data mining and risk profiling. Woods (2017) notes that the data store in the National ANPR Data Centre in the United Kingdom can be used for data mining in a number of ways and could be used to create a detailed profile of a person:

> real time and retrospective vehicle tracking; identifying all vehicles that have taken a particular route during a particular time frame (vehicle matching); identifying all vehicles present in a particular place at a particular time (geographical matching); verifying alibis, locating offenders or identifying potential witnesses; linking individuals to identify vehicles travelling in convoy (network analysis); and subject analysis when ANPR data is integrated with other sources of data (CCTV,

communications analysis, financial analysis) to create an in-depth profile of an individual (Woods, 2017, p.2).

Woods notes that these diverse types of analysis mean that the data generated by ANPR could be used predictively and generally. She submits that the storage of ANPR reads, as well as the subsequent analysis in a variety of ways, constitute intrusions into privacy that must be justified. She notes that the argument on location privacy is strong, raising wider questions about the impact of the use of other interconnected surveillance and tracking devices in public spaces, and that this increase in cameras affects our autonomy as we lose the ability to be free from surveillance, and our choices are limited by the invisible choices of the state.

Other possible consequences include selection discrimination and the stigmatisation of particular groups. Function or scope creep may also have significant consequences (Custers, 2008, pp.85, 88). The Australian Privacy Foundation notes that an ANPR database can become 'a "honeypot" that attracts attention from many organisations for many purposes, resulting in "scope creep"'. This is in violation of the purpose specification for the processing of personal information.

It then follows that congestion charging poses additional risks to privacy as opposed to the risks of, for example, road user charging systems. These risks can be significantly reduced where the minimality principle is adhered to and a system only determines the distance travelled, without monitoring vehicle location (Custers, 2008, pp.88–9).

Information privacy principle 4 of the Privacy Act highlights the necessity of collecting personal information in a lawful, fair and reasonable manner. Transparent communication about surveillance methods, such as camera monitoring, is crucial, particularly in areas where individuals' movements are recorded for congestion-charging purposes. While public consultations and website disclosures typically communicate the purpose of technologies like ANPR and GNS, there may be insufficient communication regarding additional uses, especially those related to law enforcement.

Although some GNS systems have incorporated privacy-enhancing measures, including pseudonymous identifiers, widespread deployment often lacks a comprehensive privacy review.

Information privacy principle 5 emphasises the importance of storing and securing personal information to prevent loss, misuse or unauthorised disclosure. The systemic retention of ANPR data is problematic. Issues include the bulk nature of the data retained, the lack of safeguards against abuse and the disproportionate extent of the retention. In short, Woods notes, the regime is fundamentally defective. The retention of copious amounts of data, especially sensitive data, can increase the privacy risks inherent in data mining and risk profiling (Custers, 2008, pp.88–9). The Australian Privacy Foundation notes that ANPR could represent a gross privacy intrusion as it generates a very large database of personal data, containing registration data and multiple sets of the date and time of sighting of a vehicle, as well as the location and direction of movement. The database 'is impossible to protect against unauthorised access, resulting in leakage of content'. This breaches the minimality principle as well as the requirement to deploy adequate safety measures.

Protection measures should be implemented in technologies like on-board devices and gantry towers to safeguard personal data. The proposed measures are discussed below.

Mitigation of risks

ANPR is big business: the value of the global market for ANPR technology was US$794.1 million in 2019 and is expected to increase to over $1.2 billion by 2025 (Horrigan, 2021). ANPR technology is not only very lucrative, but also here to stay. It is thus imperative that steps be taken to mitigate risks. The current position is undesirable from the perspective of the road user. A broad review of the privacy implications should be undertaken prior to the introduction of technological means to curb congestion charges to ensure that adequate safeguards are in place.

Although some GNS systems have incorporated privacy-enhancing measures, including pseudonymous identifiers, widespread deployment often lacks a comprehensive privacy review. Furthermore, while various privacy-protecting measures exist, their adoption remains a topic of ongoing discussion. Measures such as data encryption, obfuscation, blockchain technology, and settings for information deletion are being considered to enhance the protection of privacy.

Approximately 10% of licence plate numbers were reported as being misread by software systems in the United States in 2019, leading to wrongful law enforcement actions (Klawans, 2023). To address such scenarios, it is recommended that congestion-charging systems provide drivers with a user-friendly platform to check their data easily. Evidence should be provided in case of disputes, ensuring compliance with privacy laws and protecting individuals' rights.

In Hong Kong, the Office of the Privacy Commissioner for Personal Data suggested that a privacy impact assessment be conducted to identify the potential risks involved in the Central District's electronic road pricing pilot scheme. It suggested that privacy issues such as what data should be collected, notification before the collection of data, retention of data, use of data and security of data should be considered.

A privacy impact assessment is essential as it thoroughly examines the business

model, technology infrastructure and operational processes involved, identifying potential privacy risks and proposing solutions to mitigate them. Its primary objective is to assess the likelihood of personal data exposure and ensure compliance with legal data collection and usage requirements.

New Zealand's privacy commissioner has released a privacy impact assessment toolkit. It lists privacy risks and examples of risk mitigation measures that could be adopted (Privacy Commissioner, n.d.). A privacy impact assessment will be helpful in identifying and addressing some of the privacy issues related to congestion charging. Two examples will suffice. A common risk, as far as information privacy principle 1 is concerned, is the collection of excessive personal information. To mitigate this risk, a need for the collection of personal data should be established and be used to limit the information to be collected to what is truly necessary for road charging purposes.

Furthermore, in line with information privacy principle 4, consideration should be given to collecting information for the purpose of congestion charging that does not identify individuals. In this regard, it will be important to ensure that the biometric data of drivers and passengers of vehicles is not captured, and/or when using CCTV pixelation technologies should be used. This technique will also address a common risk associated with information privacy principle 4, namely that the collection method may be unjustifiably intrusive. The Office of the Privacy Commissioner also adopted CCTV guidelines in 2009. Although technological advances have rendered some of the recommendations obsolete, the guidelines are overall still largely applicable and useful (Privacy Commissioner, 2009).

Summary from focus groups

In this section, we delve into the perspectives of typical New Zealanders regarding congestion charging and its implications for privacy. We advertised on social media platforms to attract respondents. Subsequently, focus groups comprising 20 individuals from Auckland and Wellington, distributed across four sessions, were convened to uncover public views surrounding the proposed congestion-charging system. Participants from both cities were selected to represent diverse ethnicities, industries and age demographics. Each participant received a small token of appreciation for their time and contribution. The focus group discussions were conducted anonymously, with participants' names withheld from their feedback and formal consent obtained. Although open-ended, the discussions were guided by a set of four basic questions prepared to steer the conversation. Following the sessions, a thematic analysis was conducted to identify key themes and concerns voiced by the participants.

There is a growing risk of excessive data collection and prolonged data retention periods, which raises questions about compliance with New Zealand's Privacy Act 2020.

Awareness

Many participants expressed a lack of awareness regarding the congestion-charging proposals. Some respondents indicated that the research they were participating in was their first exposure to these proposals. They desired more information, particularly concerning any potential impact on their privacy. Some participants perceived decisions being made without their knowledge or input, leading to resentment and frustration.

Privacy concerns

Participants in the focus groups expressed the understanding that there is a balance between efficiency gains and privacy risks associated with a congestion-charging system in New Zealand. While road cameras are generally accepted and familiar to respondents, there was significant apprehension towards using GPS technology for location tracking. Concerns 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. Participants distinguished traffic congestion surveillance from providing location data to private companies like Google, noting that the latter typically involves (perceived) transparent consents and disclosures. In contrast, there was a perception that communication and consent had not been adequately managed for congestion-charging systems.

Data collection and use

The respondents agreed that traffic data collected by these systems should be strictly limited to specific purposes. There was a widespread belief that if the systems detect an infringement beyond traffic congestion, such as other forms of law-breaking, police intervention should not be based solely on that information. Participants argued that law enforcement agencies already possess means to access data for criminal identification and investigations through other channels. Therefore, they advocated for clear regulations to protect against unwarranted police access to traffic data. They suggested that police should be required to obtain a court order or other official permission to access the data for investigation purposes. Respondents underscored the importance of individual rights and emphasised that the New Zealand government should not infringe upon their privacy rights.

Respondents highlighted the need for enhanced government communication regarding data collection purposes and the focus on traffic management. They called for tighter restrictions on collecting and accessing traffic-specific data to ensure privacy protection. Participants emphasised the necessity for more robust controls and measures to safeguard personal data obtained from traffic systems. Ultimately,

respondents urged improved communication and transparency to understand the nature of collected data and to feel assured about its security. There was a consensus among participants regarding exploring new technologies to address privacy risks associated with data collection. Suggestions included anonymising licence plate information during transit or storage, implementing platforms for individuals to monitor their data across government services, and establishing geolocation fences to confine data collection and viewing within city limits. Participants demonstrated support for innovative solutions aimed at enhancing privacy protection in the context of traffic management.

As noted above, a privacy impact assessment could be instrumental in reviewing technologies and privacy concerns relating to implementing the congestion charging technical design in New Zealand. This would go a long way towards addressing the issues canvassed in this article and the valid concerns raised by the respondents.

Conclusion

This article has highlighted the privacy concerns arising from the emerging technologies in congestion charging. There is a growing risk of excessive data collection and prolonged data retention periods, which raises questions about compliance with New Zealand's Privacy Act 2020. It is imperative that any data collected is strictly necessary for its intended purpose, and limitations on data collection are advocated for by New Zealanders. Using GNS technology may encounter challenges in aligning with privacy objectives, prompting specific concerns. While the government's consultation report did not provide clear guidance on using GNS technology, its implementation for road user charging raises concerns about potential future applications. Similarly, issues surrounding ANPR technology, such as the potential for intrusive data collection and unauthorised use beyond its intended purpose, highlight the need for stringent regulation and oversight.

From our interaction with the focus groups it is clear that New Zealanders demand transparency in law enforcement activities and advocate for stricter controls on data access. The recommendation to enforce the Police code of conduct under the oversight of the privacy commissioner aims to address this concern and ensure accountability. An important consideration is if the Police code of conduct should come under the jurisdiction of the privacy commissioner. Furthermore, respondents suggested a data retention period of six months for traffic data and technical solutions to protect personal data. These suggestions include anonymisation techniques and platforms for individuals to access and review their data, aligning with the evolving landscape of privacy protection. In summary, this article emphasises the importance of communication and balancing technological advancements with privacy rights.

1 Harrison Neal v. Fairfax County Police Department, et al. [2018] 812 S.E.2d 444 , 295 Va. 334.

References

AA (n.d.) 'Paying road user charges (RUC)', https://www.aa.co.nz/cars/owning-a-car/licensing-safety-fees/road-user-charges/paying-road-user-charges-ruc/

Asian Development Bank (2015) *Introduction to Congestion Charging: a guide for practitioners in developing cities*, https://www.adb.org/sites/default/files/publication/159940/introduction-congestion-charging.pdf

Australian Privacy Foundation (n.d.) 'Automated number plate recognition (ANPR)', https://privacy.org.au/policies/anpr/

BBC (2018) 'Number plate cloning: fake plates are ready in 10 minutes', BBC News, 10 September, https://www.bbc.com/news/uk-england-birmingham-45397087

Brayne, S. (2020) *Predict and Surveil: data, discretion, and the future of policing*, Oxford University Press

Butler, P. (2013) 'The case for a right to privacy in the New Zealand Bill of Rights Act', *New Zealand Journal of Public and International Law*, 11 (1), pp.213–56, https://ssrn.com/abstract=2718756

Cheng, Q., J. Xing, W. Yi, Z. Liu and X. Fu (2019) 'Distance-based congestion pricing with day-to-day dynamic traffic flow evolution process', *Discrete Dynamics in Nature and Society*, 1 September, https://downloads.hindawi.com/journals/ddns/2019/7438147.pdf

Custers, B.H.M. (2008) 'Privacy issues of traffic monitoring', in H.M. Ali and A. Bidin (eds), *Abstracts and Proceedings of the 3rd Conference on Law and Technology*, Kuala Lumpur, pp.85–94

de Palma, A. and R. Lindsey (2009) *Traffic Congestion Pricing Methods and Technologies*, Hal-Open Science, https://hal.archives-ouvertes.fr/hal-00414526/document

de Silva, T. (2023) 'Would you pay $7 to drive into Auckland's CBD? Congestion charging explained', *Spinoff*, 28 April, https://thespinoff.co.nz/politics/28-04-2023/would-you-pay-7-to-drive-in-and-out-of-aucklands-cbd-congestion-charging-explained

Drinhausen, K. (2021) *China's Social Credit System in 2021*, Mercator Institute for China Studies, https://merics.org/sites/default/files/2022-05/MERICS-China-Monitor67-Social-Credit-System-final-4.pdf

Dron, W. (2022) 'Lamborghini driver baffled after being charged 15 times', *Sunday Times*, 18 February, https://twitter.com/ST_Driving/status/1494694974134362114?lang=en

GPS.Gov (2022) 'Other global navigation satellite systems (GNSS)', US Government, https://www.gps.gov/systems/gnss/

Griffiths, H. (2020) 'Massive ANPR camera data breach reveals millions of private journeys', *Auto Express*, 29 April, https://www.autoexpress.co.uk/news/106295/massive-anpr-camera-data-breach-reveals-millions-private-journeys

Horrigan, D. (2021) 'Data privacy vs. crime prevention: the automated license plate recognition debate', American Bar Association, https://www.americanbar.org/groups/tort_trial_insurance_practice/committees/automobile-litigation/data-privacy-vs-crime-prevention/

Information Commissioner's Office (n.d.) 'Can we identify an individual indirectly from the information we have (together with other available information)?', https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/can-we-identify-an-individual-indirectly/

Jackman, T. (2019) 'Judge orders Fairfax police to stop collecting data from license plate readers victory for privacy advocates could force police statewide to erase license databases', *Washington Post*, 2 April, https://www.washingtonpost.com/crime-law/2019/04/02/

judge-orders-fairfax-police-stop-collecting-data-license-plate-readers/

Klawans, J. (2023) 'The pros and cons of license-plate reader technology', *The Week*, 17 December, https://theweek.com/tech/automatic-license-plate-readers

Li, Z., L. Wang, N. Wang, R. Li and A, Liu (2022) 'Real-time GNSS precise point positioning with smartphones for vehicle navigation', *Satellite Navigation*, 3, https://doi.org/10.1186/s43020-022-00079-x

Ministry of Transport (2019) 'The Congestion Question: workstream 2: technical assessment', New Zealand Government, https://www.transport.govt.nz/assets/Uploads/Paper/TechnologyAssesment.pdf

Ministry of Transport (2020a) *The Congestion Question: main findings*, New Zealand Government, https://www.knowledgeauckland.org.nz/media/1979/congestion-question-auckland-main-findings-min-transport-et-al-july-2020.pdf

Ministry of Transport (2020b) *The Congestion Question: technical report*, New Zealand Government, https://knowledgeauckland.org.nz/media/1980/congestion-question-auckland-technical-report-min-transport-et-al-july-2020.pdf

New Zealand Police (2022) 'Automatic number plate recognition – Police Manual chapter', https://www.police.govt.nz/about-us/publication/automatic-number-plate-recognition-police-manual-chapter-0

News.com.au (2023) 'Couple demand apology after traffic camera takes photo up wife's skirt', 24 January, https://www.news.com.au/technology/motoring/on-the-road/couple-demand-apology-after-traffic-camera-takes-photo-up-wifes-skirt/news-story/4c812442f8b23fe0300c97548591ebc2

NZTA (2014) *Code of Practice for Electronic Road User Charges Management Systems* (updated 2021), Wellington: Waka Kotahi NZ Transport Agency

OECD (2021) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris: OECD

Orsman, B. (2023) 'Congestion charging: everything you need to know', *New Zealand Herald*, 7 November, https://www.nzherald.co.nz/nz/congestion-charging-everything-you-need-to-know-including-when-the-latest-plans-could-hit-motorists-in-the-pocket/7AIPZTAXYBDGZGERDGYVWL66R4/

Pedersen, H. (2019) 'Communities across the country reject automated license plate readers', Electronic Frontier Foundation, 21 August, https://www.eff.org/deeplinks/2019/08/communities-across-country-reject-automated-license-plate-readers

Pennington, P. (2022) 'Police admit misuse of number plate-reading technology as surveillance powers increase', RNZ, 29 September, https://www.rnz.co.nz/news/national/475725/police-admit-misuse-of-number-plate-reading-technology-as-surveillance-powers-increase

Privacy Commissioner (2009) *Privacy and CCTV: a guide to the Privacy Act for businesses, agencies and organisations*, Wellington: Office of the Privacy Commissioner, https://privacy.org.nz/assets/New-order/Resources-/Privacy-and-CCTV/Privacy-and-CCTV-A-guide-October-2009.pdf

Privacy Commissioner (n.d.) 'The privacy principles and examples of risks and mitigations', https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/PIA/2023-PIA-toolkit-files/PIA-Toolkit-The-privacy-principles-and-examples-of-risks-and-mitigations.pdf

Privacy Commissioner for Personal Data (2016) 'PCPD's submission in response to the public engagement for electronic road pricing pilot scheme in central and its adjacent areas', https://www.pcpd.org.hk/english/enforcement/response/files/ERP.pdf

Roth, P. (2011) 'Report on aspects of privacy compliance and practice of NZ Post Lifestyle Survey 2009: part 2: Privacy Act perspective', https://privacy.org.nz/assets/Files/Surveys/Report-NZPost-Survey-Part-2-Privacy-Perspective-by-Paul-Roth.doc

Roth, P. and B. Stewart (2021) *Roth's Companion to the Privacy Act 2020*, Wellington: LexisNexis NZ

Security (2020) 'Automatic number plate system exposes 9 million records', *Security*, 1 May, https://www.securitymagazine.com/articles/92287-automatic-number-plate-recognition-system-exposes-9-million-records

Transport and Infrastructure Committee (2021) 'Inquiry into congestion pricing in Auckland', final report, New Zealand House of Representatives, https://selectcommittees.parliament.nz/v/6/34853fc9-cb0a-479f-b9a8-0f6261fb18dc

Ukkusuri, S., A. Karoonsoontawong, S. Waller and K. Kockelman (2008) 'Congestion pricing technologies: a comparative evaluation', in F. Gustavsson (ed.), *New Transportation Research Progress*, New York: Nova Science Publishers, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.636.3245andrep=rep1andtype=pdf

Woods, L. (2017) 'Automated number plate recognition data retention and the protection of privacy in public places', *Journal of Information Rights Policy and Practice*, 2 (1), http://dx.doi.org/10.21039/irpandp.v2i1.35

Ziegler, A. (2023) 'ALPR expansion programmes and data privacy', master's thesis, Naval Postgraduate School