Privacy Foundation NZ

Submission on Land Transport Management (Time of Use Charging) Amendment Bill

Introduction

The Privacy Foundation welcomes the opportunity to comment on the Land Transport Management (Time-of-Use Charging) Amendment Bill (the Bill). Our comments are limited to **section 65ZF**, which addresses privacy and transparency.

We are broadly supportive of s 65ZF's intention to clarify that information linked to vehicle registration plates is personal information. However, three areas require further attention including the technical definition of personal information due to the technologies employed, tighter drafting of the purpose-limitation clause to avoid open-ended exceptions, and explicit guidance on retention periods.

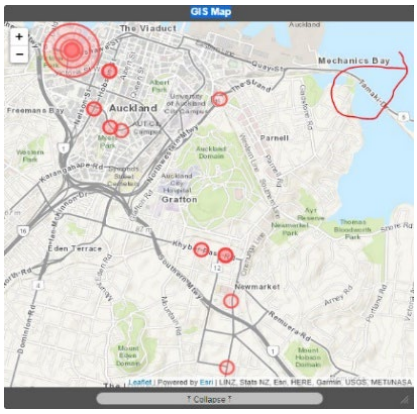

Figure 1: ANPR data collected and disclosed by Auckland Transport.

Automatic number-plate recognition (ANPR) cameras are expected to be the primary mechanism to implement time-of-use charging. Because these cameras operate as an interconnected network, they are aptly described as mass surveillance and create a historically unprecedented erosion of privacy. An example of the surveillance employed by the ANPR system of Auckland Transport is seen in Figure 1.

We emphasise the nature of the aggregate data that ANPR systems allow. It allows comprehensive records of individuals' movements to be ascertained. While privacy interest in isolated surveillance of a public places is low because people expect to be observed in public,[1] it is not absent.[2] Unlike conventional video surveillance, ANPR data is indexable and can be aggregated, forming a mosaic that intrudes upon the protections normally afforded to individuals in public spaces. This is evident within the New Zealand Police's statement that

[1] *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [12] and [162].
[2] *Tamiefuna v R* [2023] NZCA 163, [2023] 3 NZLR 108 at [54] & [57]-[58].

aggregate ANPR data allows future movements of a vehicle to be predicted with "a high degree of accuracy".[3] As one legal commentator relevantly notes:[4]

> "[A]lthough a stranger could easily observe a person's location at any given time, it is highly unlikely that the same stranger could or would observe every movement over a four-week period. Therefore, a subjective expectation of privacy was present in the aggregate of location data over that period."

Because of the erosion of privacy that comes with ANPR, this Bill is a timely opportunity to confront the broader privacy concerns that have emerged in recent years. These concerns include a case study into the ANPR practices of Auckland Transport's existing system, the entity likely to become the scheme's largest enforcement authority. Our findings of alleged unlawfulness are:

1. ANPR data is not treated as personal information, even when direct links to a registration plate are retained. Our view, respectfully, is that false claims are made that ANPR data is "anonymised".
2. ANPR data is indiscriminately collected without a necessary purpose, in breach of the Privacy Act's Information privacy principle 1 (IPP 1).[5]
3. ANPR data is retained 'indefinitely', a period that far exceeds any available lawful purpose, in breach of IPP 9.[6]

These examples are not exclusive to Auckland Transport. They illustrate why the Bill must articulate clear, substantive privacy standards for ANPR and related technologies. In the sections below we address our concerns, discuss relevant legal issues surrounding areas of ANPR, and make six recommendations towards amending the Bill.

---

[3] Police Manual Chapter "Automatic Number Plate Recognition" (14 February 2024) at 8 (Proactive release under the Official Information Act 1982 by the New Zealand Police).
[4] The Privacies of Life: Automatic License Plate Recognition is Unconstitutional Under the Mosaic Theory of Fourth Amendment Privacy Law at 151, applying the "probabilistic model" of Orin S. Kerr, Four Models of Fourth Amendment Protection, 60 STAN. L. REV. 503, 506 (2007) at 509. See also Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311, 320 (2012).
[5] The Office of the Privacy Commissioner (OPC) note that Information Principle 1 states that organisations must only collect personal information if it is for a lawful purpose connected with their functions or activities, and the information is necessary for that purpose. This principle is about data minimisation.
[6] Information Principle 9 states that an agency that holds personal information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.

	Recommendation	Proposed drafting / action
R 1	**Provide greater clarity in the definition of personal information in s 65ZF(6).**	Amend s 65ZF(6) to: "Personal information includes any time-of-use charging data linked, ***directly or indirectly***, to a registration plate, ***including data from similar systems that record a plate at a particular time and location***. ***Data ceases to be personal information only when no reasonable likelihood of direct or indirect re-identification exists for any person, internal or external to the data holder***."
R 2	**Strengthen transparency obligations in s 65ZG.**	Amend s 65ZG(4) to require the privacy policy to set out—at a minimum—(i) the measures adopted to comply with s 65ZF, and (ii) an itemised schedule of retention periods for each type of data.
R 3	**Expand the scope of s 65ZF(1)** to capture all ANPR cameras operated by, or on behalf of, an enforcement authority, even when a camera is being used for collateral purposes.	Replace s 65ZF(1) with: (1) This section applies to every automatic number-plate recognition (ANPR) camera or similar device operated by, or on behalf of, an enforcement authority or the scheme, regardless of its immediate purpose.
R 4	**Exclude the availability of Information Privacy Principle 11 (IPP 11) for disclosure.**	Remove s 65ZF(3) and replace with: (3)(a) Disclosure of personal information to which this section applies may occur only under a production order issued pursuant to s 71 of the Search and Surveillance Act 2012. (b) Real-time detection or alerting may occur only under a tracking-device warrant issued pursuant to s 49, or 48 of the Search and Surveillance Act 2012.
R 5	**Insert a maximum-retention rule in s 65ZF(5).**	Insert a maximum retention period of, at a its highest, six (6) months in line with the expectations of members of the public.
R 6	**Correct a drafting error in the Search and Surveillance Act 2012.**	It is our reading of the Act that the surveillance device warrant regime is intended to capture non-evidential / non-offence-based use of tracking-devices. The Police do not agree.

Definition of Personal Information - s 65ZF(6)

> (1) this section applies to personal information held or stored for the purposes of a time of use charging scheme by or on behalf of the scheme board or enforcement authority.

Section 65ZF(6) rightly recognises that time-of-use charging information linked to registration plates is personal information. We support this explicit confirmation as it will clarify an area that has been subject to misapplication and misinterpretation.

For example, Auckland Transport incorrectly states that ANPR data is information where "no individual, person or otherwise is identifiable".[7] So too has Hamilton City Council, who confidently (and incorrectly) state that "the Privacy Commissioner was not consulted before installing ANPR [cameras] as licence plates are not considered private information".[8] Similarly, some providers of privately aggregated ANPR data who contract to the New Zealand Police – Auror and SaferCities vGRID – have previously suggested that ANPR data is not personal information,[9] at least insofar as their own involvement, while the Police published a contrary position.

We support s 65ZF(6) of the Bill because it partially puts these disputes to rest. However, it is important for this Bill to clarify when personal information ceases to be personal information - what is the point that the information is anonymised?

Anonymisation requires the removal of identifying characteristics from information to ensure there is no reasonable likelihood of re-identification.[10] It differs from data that is merely de-identified or pseudonymised. In this instance, the identifying information is the registration plate number. Certainty is needed that, if information is to be unnecessarily collected or retained (i.e. for statistics), the registration plate number is purged.

For example, in our opinion, Auckland Transport have failed to understand and appreciate the principle of anonymisation. This failure has led to the unprecedented and unlawful collection

---

[7] CAS-630855-V1W9W5 (4 November 2022) (obtained under LGOIMA request to Auckland Transport): https://fyi.org.nz/request/20718/response/79081/attach/3/Auckland%20Transport%20CAS%20630855%20V1W9W5%20ANPR%20follow%20up%20Police%20MOU.pdf.
Also stated in CAS-658036-D0R2K8 on 19 January 2023.

[8] J Rogers 24118 ANPR Cameras (September 15, 2023) (obtained under LGOIMA request to HCC). Available at: https://fyi.org.nz/request/24118-anpr-cameras.

[9] Email from Auror regarding request for personal information (28 July 2022):

> *"Although we may hold licence plate number information on behalf of our retail customers, that does not constitute personal information because we have no abilty to connect the licence plate deals to the registered owner of the vehicle"*

[10] Privacy Commissioner "Care is needed with data anonymisation" (17 September 2024) <https://privacy.org.nz/publications/statements-media-releases/care-is-needed-with-data-anonymisation/>.

and retention of over 914 million individual vehicle-location records at the time of our queries in July 2024.[11] This is because Auckland Transport's public privacy policy confirms that every detected registration plate is logged, and that the "Vehicle Journey time" records are kept "indefinitely to be used [sic] data analysis and reporting purposes". [12] It is stated that only "anonymised" data is kept indefinitely, "mean[ing] no individual, person or otherwise is identifiable".[13] In practice, however. these assurances are unfounded. AT's own CCTV management manual makes clear that ANPR processing merely encrypts or hashes the registration plate numbers – it does not remove them.[14] Encryption (or "hashing") is a form of pseudonymisation, not true anonymisation, because each record remains uniquely associated with the same vehicle identifier. Indeed, the retained identification is illustrated by emails released under the Official Information Act which show that the Police, on request, received several years of historical location data simply by supplying a plate number to AT.[15] For the sake of completeness, the database referred to in this example is known as the CJTI or Comprehensive Journey Time Information database.

We recommend amending s 65ZF(6) to clarify the application of the existing position in law (as per R 1 in our recommendations). Our proposed definition is:

> Personal information includes any time-of-use charging data linked, ***directly or indirectly***, to a registration plate***, including data from similar systems that record a plate at a particular time and location. Information ceases to be personal information only when no reasonable likelihood of direct or indirect re-identification exists for any person, internal or external to the data holder.***

While the examples provided above present as if compartmentalised information is somehow anonymised, we believe that all ANPR data is self-evident personal information, always has been, and is also the case internationally.[16] ANPR data is "information" because it "informs, … tells or makes aware" the location of a particular vehicle and, by extension, the driver at a

---

[11] https://fyi.org.nz/request/27484/response/104623/attach/3/LGOIMA%20response%20Mason%20B.pdf
[12] https://at.govt.nz/about-us/manuals-guidelines/cctv-management-at-auckland-transport
[13] CAS-630855-V1W9W5 (4 November 2022) (obtained under LGOIMA request to Auckland Transport): https://fyi.org.nz/request/20718/response/79081/attach/3/Auckland%20Transport%20CAS%20630855%20V1W9W5%20ANPR%20follow%20up%20Police%20MOU.pdf.
Also stated in CAS-658036-D0R2K8 on 19 January 2023.
[14] https://fyi.org.nz/request/20718-anpr-tracking-memorandum-of-understanding-with-the-police-for-disclosure-of-license-plate-hits?unfold=1#incoming-79265
[15] https://fyi.org.nz/request/22265/response/88563/attach/5/CAS%20735692%20BOM6ZO.pdf
[16] For Canada, see "USE OF AUTOMATED LICENCE PLATE RECOGNITION TECHNOLOGY BY THE VICTORIA POLICE DEPARTMENT" Investigation Report F12-04 (British Columbia Information and Privacy Commissioner, 15 November 2012) at 16-18 & 24. For USA, see *Neal v Fairfax County Police Department* 812 S.E.2d 444 (Virginia 2018) at 8-10 (registration plate alone is not personal information, but it is where it is databased with location because it is the basis of "inferring the presence of the individual who owns the vehicle in a certain location at a certain time").

particular time.[17] The data is also about an identifiable individual, and there is no requirement that the individual is actually identified.[18] Identifiability is established even if only indirectly by third party extrinsic information or knowledge.[19] All reasonable means that are not "prohibited by law or practically impossible" to be used by the controller or any other person must be considered, asking whether the risk of identification in "reality" is "insignificant".[20] Under these principles of identifiability, we can point to at least three immediately available methods to discern identity from ANPR data. One method is by using intrinsic information, such as CCTV to cross reference biometric information already held;[21] another is the use of prior knowledge as to who a vehicle is driven by;[22] and, most relevantly, by using the Motor Vehicle Registry (MVR) and associated legislative tools (as discussed below).

The registered owner of a registration plate linked to ANPR data is in the MVR. If the registered owner is not the driver in question, a legal onus nevertheless rests upon the registered owner to hold that information as per their compellability under the Land Transport Act 1998, s 118. Because of the nexus between the two positions (registered owner vs driver), pointing to either party will be sufficient to establish identifiability.[23] Following *Breyer* v *Bundesrepublik Deutschland*, a case discussed in a NZ Privacy Foundation publication,[24] accessing the MVR is a reasonably likely means of identification through extrinsic information because it is a

---

[17] *Commissioner of Police v Ombudsmen* [1988] 1 NZLR 385 (CA) at 402.
[18] AO 1/2016 [2017] NZPrivCmr 1 at [10] (addresses of fire incidents are personal information).
[19] *Sievwrights v Apostolakis HC Wellington* CIV-2005-485-527, 17 December 2007, at [17].
[20] *Breyer v Bundesrepublik Deutschland* (2016) C-582/14 EJEU at [42] & [46]; M Betkier, N Mazey, R Baptista "Is the current definition of personal information enough to protect individuals from privacy harms?" (22 March 2021, New Zealand Privacy Foundation) at 4.
[21] https://fyi.org.nz/request/22265/response/88563/attach/5/CAS%20735692%20BOM6ZO.pdf At pg. 8: Auckland Transport staff suggest extracting the corresponding CCTV footage to an ANPR data request, which would make available video footage of the driver (identifying information).
[22] *Proceedings Commissioner v Commissioner of Police* [2000] NZAR 277 (CRT) at 7.
[23] It is wrong to argue that ANPR data is not personal simply because the driver might be someone other than the registered owner. The same issue arises with any subscription service: is an SMS about the account holder or the person using the phone? In practice, the law treats them as one and the same, as the cases below show..
For Cell phone data, see *Relying on a report due to language barrier*. NOYB "Location data is personal data - noyb wins appeal against Spanish DPA" (25 January 2023) NYOB.eu where the court expressly rejected that the requestor cannot prove identity of the user at a particular time. See also Case Note 294247 [2019] NZPriv Cmr 1 where call and SMS data received is presumed to be about the requestor.
For IP Addresses, see *Breyer v Bundesrepublik Deutschland* (2016) C-582/14 EJEU at [42] & [46].
For Home Addresses, see AO 1/2016 [2017] NZPrivCmr 1 at [10] (addresses of fire incidents are personal information).

[24] M Betkier, N Mazey, R Baptista "Is the current definition of personal information enough to protect individuals from privacy harms?" (22 March 2021, New Zealand Privacy Foundation) at 4.

lawful process available when certain conditions are met.[25] It is irrelevant that certain legal conditions must be satisfied for it to be executed. In fact, to go one step further, everyone has reasonably likely means to identify ANPR data subjects because the MVR is accessible to everyone with good reason (such as contemplated court proceedings).[26]

Transparency Duties – s 65ZF(4)

The Bill adds a requirement under s 65ZF(4) that enforcement authorities be transparent in their privacy policies by making such policies freely available through the Internet. We support the addition of this requirement. However, we submit that the detail of these policies must go beyond generic statements. Specifically, the privacy policy should describe how the agency complies with s 65ZF. For example, it could state which retention limits apply and the safeguards in place when disclosing data.

We therefore recommend amending s 65ZG(4) (as per R 2 in our recommendations) to require that the policy explicitly set out (at minimum) the measures adopted to implement s 65ZF and include an itemised schedule of retention periods for each class of data (see below). An illustrative example of IPP 9 retention periods is found on page 78 of the recent NZTA Privacy Impact Assessment for Safety Cameras where a "Table of retention periods for spot-speed camera data" is developed and considered the different types of information to be collected, how long it will be retained, how and when the registration plate number will be deleted for anonymisation.[27]

Considering the incomparable privacy erosion that arises from this type of mass surveillance, we consider that this additional requirement is the bare minimum to meet levels of public accountability and confidence. Without it, enforcement agencies could and will claim compliance while retaining or using data far beyond what most New Zealanders would expect. An example is Auckland Transport's current retention of personal information dating back to 2018 when the public are told it will be deleted in 7 days and have a general expectation that all ANPR data will be deleted within 6 months.[28]

---

[25] An analogous identification arose in *Breyer v Bundesrepublik Deutschland* (2016) C-582/14 EJEU at [47]: data logs collected by a website host against a dynamic IP address, akin to licence plates, allowed for the identification of an individual, even though only the Internet Service Provider (ISP) held the linking information. The ISP, akin to NZTA's position, was a reasonably likely means of identification because the website host had access to the ISP's information in certain circumstances such as a criminal cyber-attack.
[26] The Land Transport Act 1998, s 235-237; NZTA "Who can access Motor Vehicle Register information" (2024) <https://nzta.govt.nz/vehicles/how-the-motor-vehicle-register-affects-you/who-can-access-register-information/>.
[27] https://www.nzta.govt.nz/assets/Safety/docs/safety-cameras/safety-camera-privacy-impact-assessment.pdf
[28] I Seow, T Pistorius "Automated Traffic Congestion Charging Systems" (August 2024) Volume 20, Issue 3 Policy Quarterly 69 at 75.

Scope of Application – s 65ZF(1)

Section 65ZF(1) currently applies only to personal information "held or stored for the purposes of a time of use charging scheme by or on behalf of the scheme board or an enforcement authority." We are concerned that this wording unduly narrows the section's reach. Enforcement authorities (and their contractors) will almost certainly operate ANPR cameras beyond the immediate administration of congestion-charging schemes, yet their privacy impact is synonymous. These Cameras may be used "collaterally" for traffic monitoring, stolen-vehicle detection, or other enforcement. If the data captured during those uses is not considered "held… for the purposes of the scheme," then we are concerned that the protections and clarifications of s 65ZF may be given a narrow interpretation.

To prevent circumvention of intended privacy protections, we recommend that s 65ZF(1) be amended to cover every ANPR camera or similar device operated by (or on behalf of) an enforcement authority or the scheme, regardless of its immediate purpose (as per R3 in our recommendations). This expanded scope would ensure that the personal information from any enforcement-authority ANPR camera is protected, whether used for congestion charging or any "auxiliary" law enforcement function.

Purpose Limitation and Disclosure – s 65ZF(2)-(3)

Section 65ZF(2) limits use of time-of-use data to collecting charges and enforcement of the scheme. We fully support this purpose limitation, which helps engender public confidence. In its current form, we cannot support the carve out under s 65ZF(3), which creates a broad exception allowing disclosure under Information Privacy Principle 11 (IPP 11) of the Privacy Act 2020. Critically, we can only support this exception if the bill significantly strengthens the data retention limits under s 65ZF(5) with specific limitations (see below). If not, our recommendation is that a production order requirement is implemented.

We are concerned that extension of the Privacy Act's provisions relating to voluntary disclosures to this new category of time of use charging data allows a further erosion of individual privacy and contravenes a fundamental principle of information privacy that secondary uses ought not to be permitted. Our concerns that the exception provides a convenient back door for police access to vast troves of information is supported by recent evidence.

Discretionary disclosures of information, by agencies, for law enforcement purposes has been a feature of our privacy legislation from its inception with the Privacy Act 1993. It is permitted when an agency believes on reasonable grounds the disclosure of the information is necessary for amongst other reasons the detection, investigation, and prosecution of offences as well as to prevent or lessen serious threats to public health or public safety. The application of these exceptions, however, is challenging in today's big data environment, especially

where automated systems such as ANPR are utilised. Compounding this is what we believe a general disregard for the IPP 11 requirements and a perceived unenforceability of non-compliance by Courts in the Criminal Jurisdiction. We consider the only redress for this situation is to introduce formal external oversight using the legislative toolkit available in the Search and Surveillance Act 2012.

We discuss several of the IPP 11 non-compliance issues below that lead to our reluctance to accept that IPP 11 is sufficiently protective of ANPR data.

Automatic Disclosure

IPP 11 says that where an agency holds personal information, the agency shall not disclose that information unless one of the exceptions applies.

Several audits and assessments have been carried out into the Police's use of ANPR. In one Privacy Impact Assessment (PIA), it noted that:[29]

> Any voluntary request by the Police needs to contain sufficient information to enable the recipient… to form a reasonable view as to whether there is a proper basis for disclosure. If an Organisation is not satisfied that the grounds for release have been satisfied, it will not have a legal basis under the Privacy Act to release the information and the Police request should be declined.

In the ANPR platforms currently used by the Police and discussed in this PIA, the requested information is provided immediately upon request – an automated system. The PIA itself raised that this is yet to be tested by the courts.[30] We consider that there is no case to test. Every disclosure of ANPR data under an automated response breaches IPP 11 because there is no opportunity for the data holders to form a reasonable belief prior to the information being released. As noted in *Geary v Accident Compensation Corporation*, IPP 11 features subjective and objective elements with a positive obligation of inspection:[31]

> the need for reasonable grounds for belief in the necessity of disclosure requires the agency concerned to ***first inspect and assess the material being disclosed. The exception is not engaged where there is a failure to check the contents of the disclosure material before transmission***.

For IPP 11 to be available, the data holder must actually believe that the relevant exception applies (subjective), and that belief must be reasonably held (objective). There must be an

---

[29] New Zealand Police *Privacy Impact Assessment: police use of third party ANPR information* (PIA)17 April 2023 at [6.2.1]. Citing *R* v *Alsford* [2017] NZSC 42, at [33].
[30] PIA at [6.2.1].
[31] *Geary v Accident Compensation Corporation* [2013] NZHRRT 34 at [203], citing *Geary v New Zealand Psychologists Board* [2012] NZHC 384, [2012] 2 NZLR 414 at [63]. See also October-2017-Final-Guidance-on-releasing-personal-information-to-Police-and-law-enforcement-agencies-Principle-11f-and-ei.pdf.

actual belief based on a proper consideration of the relevant circumstances. An explanation devised in hindsight will not suffice.[32] As such, regardless of the material submitted in support of the decision (frequently this too is insufficient or non-existent), no actual belief can be formed because no consideration is given to the facts before disclosure.[33]

We submit that this IPP 11 breach unequivocally applies to several hundred thousand requests for ANPR data made by the Police annually.[34]

Insufficient Information

We have also observed that the rudimentary guidance on IPP 11 set out by the Supreme Court in *R v Alsford* is not consistently actioned by requesting agencies for ANPR data. In *Alsford*, the Court found that the requirement for "reasonable grounds is a meaningful one" and it is for the requestor to provide sufficient information.[35] In *Alsford,* the Court found that a data holder being told only that the Police are investigating an offence is insufficient to form a reasonable belief under IPP 11. But the reasonable belief was met by two information requests to a power company which indicated a cannabis grow was being investigated because the power companies have "general experience" that means they are "well aware" of the link between power consumption and cannabis grows.[36]

By way of example, we have reviewed data received by a defendant in criminal disclosure. We observe 124 individual ANPR queries by the Police pursuant to IPP 11 against one criminal defendant in a single investigation. Nearly all contained no more than a Police file number and the descriptor of "Volume Crime". It is our submission that the provision of a police file number and the non-descriptive term "volume crime" is analogous to the Police's insufficient statement in *Alsford* because no greater meaning is derived by either piece of information. Both inform of the same concept: we are investigating a crime, without further indication. Further examples of more concentrated requests without provision of sufficient information can also be identified in the emails between AT staff and the NZ Police.

Unenforceability

Naturally, the Criminal jurisdiction is where one would expect legal issues related to the privacy breaches of systems which double as surveillance measures will be fleshed out. However, as has been illustrated in several recent evidential objections challenging the

---

[32] *Geary v Accident Compensation Corporation* [2013] NZHRRT 34 at [202].
[33] For instance, in *Elley v Police* [2021] NZHC 2097 at [32], the Court considered that even if the objectively reasonable grounds to believe are available, the officer is still required to "form" the request beliefs themselves. Forming the belief was a distinct consideration.
[34] NZ Police *Follow-up audit of Police staff use of Automated Number Plate Recognition (ANPR) platforms* (December 2024).
[35] R v Alsford [2017] NZSC 42 [2017] 1 NZLR 710 at [41]-[44].
[36] At [41-44] (majority), and also [121] and [139-145] per Elias CJ.

lawfulness of ANPR surveillance, the Courts do not have an appetite for making substantive findings on fundamental Privacy Act breaches due to the unenforceable clause in the Privacy Act 2020, s 31. See for example *R v Kake and others* [2024] NZDC 24739 at [117].

The unenforceability is also a function of core interpretive issues at the heart of criminal prosecutions.[37] Criminal Courts are generally applying the formulation of whether the technology has encroached on a "reasonable expectations of privacy" in public space. Application of this test, as enumerated by higher courts, such as *Hamed v R*[38] in New Zealand and *R v Plant*[39] in Canada largely predates the big data era, arrival of generative artificial intelligence and the potential for automated linkage of myriad datasets to identify and to categorise individuals. *Hamed* concerned one non-facial recognition CCTV camera facing a rural public road, whilst *Plant* involved electricity records.

It is our contention that, unlike courts in these individual instances, the legislature needs to be vigilant as to the *systemic effect* of the *aggregation of such automated systems*, including ANPR and facial recognition (FR), amongst others. The potential exists, for instance, for an individual's power consumption to be matched with their vehicle ownership, locations they travel to and individuals they associate with.

The Bill contains the potential for a significant erosion of the fundamental rights of New Zealanders such as those protected by the New Zealand Bill of Rights Act 1990 - such as but not restricted to the freedom of movement, of association and expression. There is a very real possibility for a chilling effect on these freedoms through potential uses of the technology. To give one very recent example, protest movements associated with Destiny Church members have received considerable publicity: the registration plates of some of these individuals is easily accessible and it would be easy to track or retrace their movements to ascertain intentions as well as the association between individuals even prior to any offences taking place. It is not beyond the bounds of credibility to imagine future applications of such technology to disrupt the activities of individuals pre-emptively, in a manner not dissimilar to that depicted in the celebrated film *Minority Report*.

Use of IPP 11(1)(f) for Real-Time Surveillance

The Police currently recognize IPP 11(1)(f) as legislative authority for using real-time ANPR alerts in situations where there is "insufficient information to suspect an offence" but a serious risk to the life or safety of any person.[40]. We submit that this authority is

---

[37] The Search and Surveillance Act 2012 and the New Zealand Bill of Rights Act 1990.
[38] *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305.
[39] *R v Plant* [1993] 3 SCR 281.
[40] https://www.police.govt.nz/sites/default/files/publications/automatic-number-plate-recognition-140224.pdf at 11.

irreconcilable with the mandatory language of the tracking warrant mandate pursuant to the Search and Surveillance Act 2012 (SSA), s 46. The Police's adoption of this interpretation is an attempt to avoid judicial oversight and reporting obligations, which are intended to cover exactly such scenarios as described.

Under the SSA, the use of a tracking device by enforcement officers is unlawful unless authorised either by a tracking warrant or by a specific statutory exception. Section 46(1)(b) of the SSA clearly mandates the need for a tracking warrant for any investigative use of such a device, with only two relevant exceptions. The first is an "authorisation under any other enactment" (s 47(1)(d)), and the second is the urgent or emergency use provision in s 48.

IPP 11 cannot satisfy the first exception (s 47), because the Privacy Act is not an empowering statute for law enforcement purposes. It is merely permissive given that it outlines the circumstances under which an agency may voluntarily disclose information without incurring liabilities —it does not confer authority upon Police to utilise a tracking device or engage in surveillance activities.[41] However, the language of IPP 11(1)(f) - referring to a "serious threat to life, health or safety" - closely resembles that of section 48(2)(b) of the SSA. S 48(2)(b) provides for the warrantless use of a surveillance device in emergencies where no offence is suspected, and an officer has reasonable grounds:[42]

i. To suspect that any 1 or more of the circumstances set out in section 14(2) exist [including a "risk to the life or safety of any person that requires an emergency response"]; and

ii. to believe that use of the surveillance device is necessary to … avert the emergency.

Unlike subsections in s 48(2), this emergency power does not require the suspicion of an offence. However, its application is limited by s 48(1), which stipulates that the officer must be "entitled to apply for a tracking warrant". That entitlement is defined in s 51, which, on its face, does not appear to provide a pathway to apply for a warrant where no offence is suspected.

We consider this to be a legislative drafting error by failing to provide for a corresponding non-offence-based ground in s 48(1), or a non-evidential category of tracking warrant under s 51. Section 48(2)(b) expressly cross-references the warrantless emergency situations outlined in s 14(2), which include a "risk to the life or safety of any person that requires an emergency response". Section 14(2) was enacted on the recommendation of the NZLC R97 report,[43]

---

[41] R v Alsford [2017] NZSC 42 [2017] 1 NZLR 710 at [64].

[42] Search and Surveillance Act 2012, s 48(2)(b).

[43] L*aw Commission Search and Surveillance Powers* (NZLC R97, June 2007) , at [5.43]-[5.61], discussing the issue posed by New Zealand Law Commission Preliminary Paper 50 Entry, Search and Seizure (April 2002) at [21].

which proposed codifying two types of warrantless powers: "one for crime prevention, and one for emergency assistance to people."[44]

The Law Commission recommended that "the circumstances in which surveillance devices may be used by enforcement officers pursuant to emergency powers should reflect those situations when a warrantless search power may be exercised," including "where there is an emergency that may endanger the life or safety of any person."[45]

Accordingly, the legislative intent behind s 48(2)(b) is to permit tracking devices to be used in non-offence emergencies, mirroring s 14(2)'s provisions for emergency search powers. The SSA, s 60 further supports this notion. Section 60 requires a judicial report after the use of a tracking device under emergency powers, including whether its use "resulted in … averting the emergency (in the case of use of a device in a situation set out in section 48(2)(b))." If s 48(2)(b) were limited to offence-based-use, this express inclusion of a reporting requirement would be rendered meaningless.

We therefore submit that s 48(2)(b) was intended to authorise non-evidential emergency use of a tracking device in precisely the circumstances which the Police currently authorise under IPP 11. By relying on a permissive Privacy Act exception rather than the legislative intent of the SSA's emergency provisions, the Police are circumventing Parliament's strict judicial safeguards found in s 60.

One example of IPP 11(1)(f) being used in this manner instead of under SSA, s 48 is "Operation Hiking", a high-profile case that resulted in the Northland's Covid-19 lockdown. There, that Police falsely recorded two target vehicles as stolen in the NIA to trigger real-time live alerts from Auror and vGRID (a tracking device).[46]

The above example prompted the 2022 audit of Police ANPR use. However, that methodology of the "misuse" inquiry appears to have avoided a review of the legal authority for those very requests. Furthermore, although this may be speculative, we nonetheless raise the concern that 2,732 live ANPR tracking functions were used in 2022,[47] but only 300 total tracking devices were legally authorised for that period.[48] Without more (we have been

---

[44] NZLC R97, at [5.50].
[45] NZLC R97 at [11.109].
[46] https://fyi.org.nz/request/20978/response/80582/attach/8/Helm%20Mason%20IR%2001%2022%2034038%20Response.pdf . In this instance, not only did the Police circumvent reporting obligations, but they also used the tracking device for longer than the 48-hour maximum permitted by s 48.
[47] https://fyi.org.nz/request/21129/response/80603/attach/4/Walter%20John%20IR%2001%2022%2035618%20Response.pdf ; https://www.police.govt.nz/sites/default/files/publications/police-use-anpr-platforms-audit-report.pdf
[48] NZ Police *Annual Report 2021/2022* (November 2022) at 122.

unsuccessful in further OIA requests), we submit that there is a very real possibility that this statistical disparity is due to unlawful reliance on IPP 11(1)(f) instead of the SSA, s 48.

The Amendment

We argue that, should the carve out from the purpose limitations set out in subsection (3) be retained, much greater clarity is needed in the rules set out in subsection (5) for length of retention. We accept that a very short retention period would mitigate some privacy concerns.

However, considering past performance indicators, we do not consider IPP 11 is sufficiently protective of ANPR data. Our formal recommendation is for the inclusion of a production order requirement for all ANPR data under the SSA, s 70. We also consider the SSA, surveillance device warrant regime as the exclusive authority for real-time ANPR alerts which will invariably be implemented in the future, if not already. Benefit would be derived from express clarification to that effect, ensuring that judicial oversight is enforced where originally intended.

If our recommendation to incorporate SSA requirements into the bill is not adopted, we consider the IPP 11(1)(f) and SSA, s 48 conflict would nevertheless benefit from statutory clarification given the apparent drafting error.

Length of Retention – s 65ZF(5)

We support subsection (5) which contains requirements as to length of retention of personal information collected in connection with the time of use charging scheme. Sub paragraphs (a) and (b) state that personal information may only be retained for as long as it is reasonably necessary for the purposes of collection and enforcement of the scheme. However, we think the words "reasonably necessary" are superfluous and ought to be removed, as they add a layer of discretion which may allow agencies to retain information longer than necessary. It should be self-evident how long the information should be retained for collection and enforcement purposes, and that period should be consistency across enforcement authorities.

It is our recommendation that the maximum retention period is prescribed by statute or delegated to the scheme board for consultation. That retention period should be graduated based on the different types of information that are sought to be collected and their resulting necessity, drawing a minimum standard from the schedule presented in NZTA's safety camera PIA.[49] Ultimately, we consider that the public's expectation of privacy to their aggregate location data should also inform the determination of this period. A recent survey conducted

[49] https://www.nzta.govt.nz/assets/Safety/docs/safety-cameras/safety-camera-privacy-impact-assessment.pdf at pg. 78-79.

by University of Auckland researchers into the congestion charging scheme determined this to be six months.[50]

In addition, we do not support sub paragraph (c) as it currently stands. It is unreasonable for members of the public to be aware of information retention requirements in other enactments. Again, the provision risks allowing agencies discretion by pointing to unspecified reasons for retaining the information. Should this sub paragraph be retained, then we believe it needs to be supplemented with examples or further elucidation as is nowadays common in other legislation. See for example the guidance notes contained in the Customer and Product Data Bill,[51] or the use of examples in the Plain Language Act 2022.[52]

Summary

To conclude, the Foundation is supportive of the sections in the Bill addressing privacy and transparency. We are concerned about the proliferation of automated surveillance throughout the private and public sectors in New Zealand, especially its potential use by law enforcement authorities as a back door mechanism to avoid strict ex ante legislative requirements as well as for ex post accountability. We also believe clear legislative guidance is needed in relation to technologies such as ANPR, to supplement and, where necessary, correct outdated case law as to what the reasonable expectations of privacy are in the big data environment. The provisions we have referred to in the bill go some way towards this but still leave room for improvement.

Specifically, we believe the exceptions contained in the Bill's purpose limitation rules are too wide and ought also to be linked more closely to the Bill's retention limits. Furthermore, the wording of the requirements as to length of retention of personal information collected in connection with the time of use charging scheme ought to be more specific and contain time limits (if necessary, through appropriate regulations). Lastly, the legislation should include specific examples of the matters it covers, in addition to listing any legislation that operates to override, for instance, its retention limits.

This submission was compiled by the Convenor of the Surveillance Working Group, Associate Professor Gehan Gunasekara, with input from other members of the Working Group and the Privacy Foundation NZ Committee.

---

[50] I Seow, T Pistorius "Automated Traffic Congestion Charging Systems" (August 2024) Volume 20, Issue 3 Policy Quarterly 69 at 75.
[51] Customer and Product Data Bill 2025, s 80.
[52] Plain Language Act 2022, s 6.