



18 March 2014

To whom it may concern

**Letter of Introduction for Mr Bruce E M Flett**

Auckland Transport is currently looking to expand the use of closed Circuit TV (CCTV) and associated analytics to a broad range of traffic and public safety initiatives, including potential to provide access to other agencies such as Police.

As the use of CCTV expands issues of Privacy, enforcement opportunities and purpose for collection of information become more meaningful. In order to gain clarity on a number of these issues Auckland Transport is engaging with relevant parties to ensure that its own operations and proposed useage of this emerging technology conforms to all the relevant regulations and guidelines.

Auckland Transport has recently engaged the services of Mr Bruce Flett, a Director of Ridgehill Ltd to assist it with determining strategies, polices, procedures and identify initiatives to make better use of Closed Circuit TV (CCTV) and associated analytical technology to enhance public safety and better manage our transport network.

This work by Ridgehill will cover assessments of:

- Technical implementations, results and developments (such as reading number plates, using CCTV to control Traffic lights, monitor misuse of clearways, and provide a potential to measure traffic flows)
- Current legislation, Regulations & By laws controlling the collection, use and storage of both the video information and any derived analytical information
- Personal Privacy implications regarding the use of the use of the information gathered and processes to manage this
- Codes of Conduct for Auckland Transport staff
- Public Communications over the reasons that we need to use such technology

I would appreciate it if you would give Bruce every assistance with his research to help us develop appropriate strategies for the use of CCTV technology. We will of course keep the information made available confidential. We will make any available to other government and local bodies the outcomes of our work upon request.

Yours sincerely

A handwritten signature in black ink, appearing to read 'R Jones', with a large loop at the end of the line.

Roger Jones

GM Business Technology  
Auckland Transport

6 Henderson Valley Rd, Henderson, Waitakere 0612  
Private Bag 92250, Auckland 1142



---

**From:** Russell Derecourt (AT) [REDACTED] >  
**Sent:** Thursday, 1 May 2014 3:05 p.m.  
**To:** Sarah Thompson  
**Subject:** RE: Check in

Sarah

On behalf of Auckland Transport I would be very keen to talk through specifics with you and have tried the number in your signature to no avail unfortunately.

Whats the best way to get hold of you.

Thanks

Russell Derecourt  
6 Henderson Valley Rd, Henderson, Auckland 0612  
Private Bag 92255, Auckland 1142

[REDACTED]  
[www.aucklandtransport.govt.nz](http://www.aucklandtransport.govt.nz)  
[REDACTED]

**Auckland  
Transport**   
*An Auckland Council Organisation*



---

**From:** Sarah Thompson [mailto:[REDACTED]]  
**Sent:** Wednesday, 30 April 2014 4:57 p.m.  
**To:** Gillian Stewart  
**Cc:** Bruce Flett <[REDACTED]> ([REDACTED]); Bram Van Melle; Russell Derecourt (AT)  
**Subject:** RE: Check in

Hi Gilly

Thanks for your email. I apologise for the delay in getting back to you – things have been especially hectic here for the last couple of weeks!

I've now had a chance to look the issues you've raised and my initial thought is that multipurposing isn't an issue so long as, to the extent which it can be anticipated, reasonable steps are taken to make it clear what the purposes are.

What is 'reasonable' will depend largely on how likely it is that people could or will expect that the info will be used this way. So, for example, if you had a cameras operating next to big "safer communities" type sign with logos for AC, Auckland Transport and Police, it's pretty likely people would expect that the information would be used for things like investigating crime or managing traffic during a big event or after an accident. But if you then wanted to give the info to another unrelated third party – or even part of AC which doesn't seem connected (for the sake of argument let's say the zoo), or if you wanted to use the information for another purpose that seems completely unrelated (say using the information to help developing marketing strategies for businesses in that area) then you would need to take additional steps to make this clear.

Then if something new comes up – an unanticipated use – then the policy would just need to set out a clear process to follow for testing whether any exception applies allowing the information to be used that way. If not, then the information shouldn't be used for that purpose.

So looking at the suggested policy purposes of i) public and staff safety, ii) asset security and protection and iii) business and operational efficiencies – my concern would be that these are so broad that people aren't being given effective notice of how the information may actual be used. We generally advise that principle 3 statements (including things like posters and signs) need to work on a 'no surprises' basis - that the statement provides enough detail that people aren't surprised with how their information is used down the track.

So possibly a better way to approach it would be to try and identify all the different purposes you may want to use camera information for (whether this is something that is done council wide or broken down to different types or categories of cameras) and then work back from there to make sure the purposes captured in the policy clearly reflect the purposes the information is being collected for.

In terms of your query about the impact of the ownership or control of various parts of the overall system (including the cameras themselves, the network over which the information is shared, and the storage/access of information) that is a really interesting question, and it largely depends on the nature of the agreements established between the various parties involved. Generally speaking, usually the agency operating the actual cameras would be held responsible for the initial collection of the information, and then for any subsequent disclosure or use of that information. Once the information is passed on to another agency (so that agency has some measure of control over the information) that next agency would then be responsible for how the information is stored/used/disclosed etc.

However, if one agency is operating the cameras on behalf of another agency, for instance under contract, then the second agency is the one which would be liable in the first instance if there was a breach of privacy (you may want to have a quick look at section 3 of the Privacy Act which defines what information is "held" by an agency). Obviously the more agencies there are that are involved in the network the more complicated these arrangement may be – in which case it needs to be very clear exactly who is responsible for what. It would be important to establish, for instance, when an information request is received, which agency is responsible for responding to that request .



Hopefully this is of some assistance, but if you'd like to discuss this further, or maybe meet up to have a bit of a chat about this, just let me know.

On another note, I recall that shortly after the stakeholder workshop in Feb, there were a couple of emails circulated where people had raised concerns about difficulties in accessing statistical crime information from Police for the purpose of establishing camera surveillance systems (both in terms of working out if cameras were needed and where they should be placed). I just wanted to see if there had been any further discussions on this within the work done on Auckland Council project, as this is issue has also been raised with our office in a more general way in other parts of the country. If you could let me know what, if any, outcome was reached from these discussions, or if there is someone in particular who is dealing with this, that would be much appreciated.

Cheers  
Sarah

Sarah Thompson | Investigating Officer (Auckland)

Office of the Privacy Commissioner Te Mana Matapono Matatapu  
PO Box 10094 | Wellington 6143 | New Zealand [REDACTED]  
[REDACTED] | [www.privacy.org.nz](http://www.privacy.org.nz)

*Privacy is about protecting personal information, yours and others. To find out how to do that, and to stay informed, [subscribe](#) to our quarterly Privacy Newsletter or follow us online  *

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments. Please treat the contents of this message as private and

confidential. Thank you.

**From:** Gillian Stewart [mailto: [REDACTED]]  
**Sent:** Wednesday, 9 April 2010 11:07 a.m.  
**To:** Sarah Thompson  
**Cc:** Bruce Flett - [REDACTED] ([REDACTED]); Bram Van Melle; Russell Derecourt (AT)  
**Subject:** Check in

Hi Sarah.

I hope this finds you well. It's been a while since you joined us in Feb, and I have meant to come back to you on numerous occasions!!

I'd like to try a couple of scenarios out with your advice on the Privacy Act please. We are in the process of drawing up a draft strategic action plan, but thinking particularly at the moment of council's policy position and what approach would flow from that. In the first instance, a goal would be to enable multipurposing and interoperability of cameras/ systems to enhance coordination between stakeholders – something that is encouraged by sharing/ linking on a data network. Our Auckland Transport colleagues (I have cc'd in) are also dealing with this issue but at a different level/ range of uses, and might be interested in your thoughts.

- Multipurposing concept. Where CCTV cameras are owned by Auckland Council and we aim to utilise the efficiency of the cameras by enabling different business units to view and use the data for other uses.  
E.G. a camera or system of cameras in a town centre used to enhance safety of locations and identify antisocial behaviour of youth is primary purpose, but
  - a) may also be sitting on major/ key thoroughfares that would be utilised and needed to be viewed by Civil Defence team to direct emergency services of people or traffic in case of a civil emergency.
  - b) Those same cameras or systems may also offer information (live feeds or stored data) that might assist staff in liquor licencing or resource consents to identify a problem or breach of a licence.
  - c) The same cameras might also be located near a facility like Eden Park or museum/ gallery and access to live feeds might assist the facility to make improved decisions about event management, crowds entering/ leaving the facility.
  - d) Those cameras might have value if linked to a local monitoring station of a business association who have their own system, but the council camera offers an additional view of the high street that they can't get, but shouldn't want to install another camera in the same location.

I guess the issue is about third parties uses (other than Police for lawful purposes, etc) within and without council accessing and using the data captured by the cameras for additional council business. Is it simply about addressing the multipurposing issue when deciding the purpose and designing the system?

- Lastly, if Council policy stated that every camera owned by Council is to be established for the following generic purposes i) public and staff safety, ii) asset security and protection iii) business and operational efficiencies
- would this be a good starting point, and what level of further detail would be required to enable scenarios such as above?
- Would this multipurposing have to apply to each camera or the system and where the images are viewed/ stored?
- Would the ownership of the network on which the data is shared have any impact, or is it simply about the ownership of the CCTV asset and where/ how data is stored and accessed, where the Privacy Act applies?

I recognise you will be busy, but I'd really appreciate your thoughts.

Thanks very much and kindest regards  
gilly

# File Note

**By** : Sarah Thompson  
**Date** : 6 May 2014  
**Subject** : **Meeting with AT and Rep**

---

File note of a meeting with AT and reps from today, 6 May 2014.

Present at the meeting were Bruce Flett, Ridgehill Limited (who are consulting with Auckland Transport regarding some upcoming work they are doing). Also present were Ginny Nalar (not sure of spelling) and Russell Derecourt from Auckland Transport.

So the purpose of today's meeting was to have a brief chat about some of the upcoming work AT is looking to implement or at least trial in order to provide more efficient or better services.

The meeting began with Bruce talking through some of the main areas of work they were looking at. Firstly, in terms of enforcement, looking at parking for instance and the use of ANPR and data matching both with internal information, for example AT's database of permit passes, and externally with MVR.

Bruce also talked about moving vehicle enforcement including, for instance, red light cameras. He noted that there are questions around who does what in terms of managing or paying for the system and sharing this burden between AT and Police. He also noted questions around what technology is used, for instance APNR.

He also referred to enforcement regarding bus and transit lanes and mentioned that currently this is done by having an individual stand on the side of the road recording the lanes.

Another area of work related to traffic lights management and the potential to use camera or radar to more effectively manage traffic lights. He mentioned for instance technologies to detect the pedestrians and referred to the 'Puffin' crossings being trialled elsewhere in NZ. He also noted the potential use of this technology to make traffic lights better at sensing other users like cyclists.

He noted that with all the methods described above this would involve a fairly instantaneous collection of information and it would less likely to capture personal identifiable information.

He also noted the potential for using the same cameras for looking at traffic flow statistics, for instance traffic time management, so how long it takes to get from A to B or for statistical information on sourcing destination, e.g. 10% of cars leaving from point A travel to point B; 30% travelled to point C etc.

Given these areas of work Bruce raised three key areas. The first was regarding multi-purposing, the second was around communication and the third was in terms of data matching.

With regards to multi-purposing he noted there is a possibility of using one camera to do multiple jobs. He noted they would cost approximately \$10,000 per camera per lane and so they would want to make the best use of this money. He noted, for instance, they could be collecting red light information through ANPR when information would be recorded and matched. It could also be recording length of queue in which case this information would not be kept or identifiable. Or the information could be used for traffic flow management in which case it maybe that the information would be identifiable, because they need to be able to recognise the same car in one point was in other points but said that there are technologies which allow them to encrypt this information so people outside the system could not make it identifiable.

I discussed some of the general points I have already raised in correspondence with AC (which AT et al have been copied into) about multi-purpose use of cameras. Again I acknowledged that the more purposes they have for collecting information the stronger argument they have in terms of why the collection is necessary under principle 1 and then it is really just a case of how to deal with a 'no surprises' approach to principle 3.

We spend a bit of time discussing the situation of meeting legal requirements as opposed to dealing with issues of perception or communication so that people aren't surprised with how it is being used and are therefore less likely to want to complain about it.

At around this point Russell raised a couple of questions regarding setting up systems if they want to be able to disclose information or if they are receiving requests for information under LGOIMA. For instance, he referred to the fact they get requests from insurance companies wanting camera recordings from intersections after crashes occur.

I spend a bit of time talking about the LGOIMA provisions but noted that this was something outside of our area. Again I noted that legally if they released in response to a request then they were protected in terms of the Privacy Act. However, I acknowledged that they may still be in the gun public perception wise if they have done this.

I discussed the fact that this is where it is particularly important to be very clear on what their purpose is for collecting the information are initially because having that information available will inform the decisions about whether any withholding grounds apply for preventing release of the information further. However, I did note this is something they may want to raise with the Office of the Ombudsman for further guidance.

We also spend a bit of time talking about what is reasonable in terms of communicating. Again, we discussed legal requirements versus perceptions or potential communication plans they may want to put in place. I talked about the fact this has not really been tested through the Office or Tribunal or terms of what is reasonable when it does come to cameras of this nature but that the general approach being taken is that there does need to be some ability to recognise that the camera is there and who is responsible for it which would then allow the person to go and look for further information about exactly what is being collected

and what it is being used for etc. Russell noted that they have already made information available through their website and this is probably a good communication tool for them.

We also discussed the possibility that if they go forward with trials on some of the different projects they are looking at, for instance looking at cameras on intersections which have been problematic for cyclists, then they would likely publicise this as well and get comments at that time. We have also agreed that before they put in place any of these trials or put in place policy they will run it past our office to give us a chance to provide some feedback.

We then spent a bit of time talking about potential access or use of the information collected by AT by other bodies and in particular Police. They noted the situation at the moment is that they getting a number of requests from Police to have access to footage and of particular concern is requests for access to real time footage or direct access.

I noted that the legal position is likely to be that in terms of use or disclosure, if it is for maintenance of the law purposes it will not be breach of the Act. However, I again noted perception concerns and acknowledged that because AT holds the information they have still got obligations around security and retention and providing access.

This led to a bit of discussion about retention times and the current lack of guidance within AT about how long they want to retain the information for. I noted that the Privacy Act places no minimums only maximums and that it is really up to each agency to decide what it's purpose for having the information are and how long it needs the information to meet these. I noted we have seen other areas, for instance in the telecommunications information area, where there has been some pressure on agencies to retain information because of the potential usefulness to law enforcement agencies. I noted that while we certainly would not want to discourage engagement or cooperation with Police, that ultimately it should be a case that if they need to make sure that if they are facilitating access it is to the information at AT has a purpose for holding, rather than AT is holding information for the purpose of providing access to Police.

I understand that there will be some further internal discussions about exactly how they want to manage this and in particular whether there is going to be a separate MOU put in place between Police and AT.

Bruce also raised concerns concerns about data matching referred to earlier in the parking context. I explained that internally using data matching within their own databases does not really raise too many issues but just cautioned them in terms of making sure they had appropriate processes for testing the information before using it in terms of principal 8.

In terms of external data matching I noted this was not my area of expertise and said I would want to refer to a colleague in Wellington who deals with this more generally so I didn't steer them wrong. Bruce noted that he is generally based out of Wellington and so said he would be happy to meet with someone in the Wellington office if that was more appropriate. I said I would look into this and get back to him.

We also talked a little bit around public communications and public perception and I referred to the introduction of cameras in taxis as being something they may want to have a look at



as an example of how a system can be suggested, there may be a bit of fight back about the appropriate way for the system to be implemented, and eventually a position is reached which most parties seemed comfortable. I did acknowledge that in that case it was slightly different as there was some regulation around it and as a result this would have overridden the generally provisions of the Privacy Act.

Another issue Russell raised was the question around balancing security and utilities. He mentioned that Parking Wardens for example would need to retain some quite detailed specific information in terms of infringement notices and for that purpose had access to MVR. He noted that there had been requests to have some sort of mobile access to this which they have been resisting for the moment due to concerns about potential security breaches or the potential this information could be lost or misused.

I acknowledged his concerns and discussed that it is a bit of a balancing act between how sensitive the information is and potential consequences of loss/misuse and taking reasonable steps and what would be reasonable in the circumstances. I acknowledged that even with the best security system in place mistakes still to happen so it is really a question of seeing what they could do to mitigate it and whether that outweighs the potential risks. I also noted that although principle 5 is rather general, I could specifically say that staff training is key because if they haven't trained staff it would be very difficult to ever argue they have taken reasonable steps to secure the information.

I think that is about everything so there is quite a lot going on but it is all still early stages at the moment. However, we have agreed that they will keep in touch and let me know how things are proceeding. I explained that we can't make any going commitments in terms of involvement but said that if they want to keep us in the loop that would be much appreciated even if it only so we are aware of things they are about to go public on before they do so we can answer the inevitable enquires we will receive.

---

**From:** Bruce Flett <[REDACTED]>  
**Sent:** Monday, 12 May 2014 3:32 p.m.  
**To:** Sarah Thompson  
**Cc:** Tim Henwood  
**Subject:** RE: Auckland Transport - Early considerations of Privacy Implications from Collecting Transport Information via various technologies

Hi Sarah,

Many thanks for the information and your time last week.

I checked up on the previous correspondence that I was referring to with NZTA and you were quite right it was to and from Sarah [Adams-Linton](#).

I have also made contact with Superintendent Griffiths of traffic Police in Wellington and have booked a meeting in three weeks about rules, regulations and issues around using standard cameras and a data centre analytic engine to monitor red light runners. This option would make use of cameras already there for other purposes as we discussed. However there are many legal, procedural and political issues to work through, all of which would need to be communicated to the public once we have a possible course of action. I suspect from a brief discussion with Superintendent Griffiths that these issue will take some time.

What I hope to come up with, during May and June is an outline programme for AT to follow once we have decided on some technical systems. The initial uses will probably not involve any issues of privacy (e.g. detecting bicycles at lights to activate them, or detecting the length of queues of cars to alter traffic light settings, but as we work through other potential uses there will inevitably be areas that we will need to work through and discuss with the Office of the Privacy Commissioner.

Regards  
Bruce Flett

---

**From:** Sarah Thompson [mailto:[REDACTED]]  
**Sent:** Monday, 12 May 2014 2:20 p.m.  
**To:** Bruce Flett  
**Cc:** Tim Henwood  
**Subject:** RE: Auckland Transport - Early considerations of Privacy Implications from Collecting Transport Information via various technologies

Hi Bruce

It was nice meeting with you, Ginny and Russell last week to discuss some of the projects coming up for Auckland Transport.

Just following on from our meeting, I've now had a chance to check with the policy team in our Wellington Office to see who would be the best person for you to liaise with regarding a discussion about potential data matching arrangements, particularly with respect to the MVR. I've been advised that Tim Henwood, Policy Adviser (Technology), would be the best person for you to get in touch with in the first instance.



I've also had a chance to look to see what information I could find with respect to the process which occurred when steps were taken to introduce CCTV in taxis. The only information we appear to have on our website is the guidance

we published on the subject – which can be found at: <http://privacy.org.nz/news-and-publications/guidance-notes/information-sheet-for-taxi-organisations/>.

I hope this is of assistance to you and I look forward to hearing from you and/or Auckland Transport as these projects progress.

Kind Regards  
Sarah

Sarah Thompson | Investigating Officer (Auckland)  
Office of the Privacy Commissioner Te Mana Matapono Matatapu  
PO Box 10094 | Wellington 6143 | New Zealand  
[REDACTED] 4 9 302 2305 | [www.privacy.org.nz](http://www.privacy.org.nz)

Privacy is about protecting personal information, yours and others. To find out how, and to stay informed, [subscribe](#) to our quarterly Privacy Newsletter or follow us online  

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments. Please treat the contents of this message as private and confidential. Thank you.

---

**From:** Bruce Flett [mailto:[REDACTED]]  
**Sent:** Tuesday, 22 April 2014 2:39 p.m.  
**To:** Sarah Thompson  
**Cc:** 'Russell Derecourt (AT)'; [REDACTED]; Gillian.Stewart@[REDACTED]  
**Subject:** Auckland Transport - Early considerations of privacy implications from Collecting Transport Information via various technologies

Hi Sarah,

Thank you for the chat today.

I am working for Roger Jones and Russell Derecourt of Auckland Transport (AT) as a consultant researching a wide range of areas around collecting information from technological sources. Our intention is to develop a programme of work to make use of those technologies to provide the public with better traffic flows, assist with some types of traffic enforcement, improve AT's efficiencies and provide public safety enhancements.

I am very much aware that Auckland Council are in the process of consolidating their various CCTV systems and establishing rules for their use and deployment. I have just started attending those meetings run by Gillian Stewart. What I am seeking here, is a parallel stream of engagement with the Office of the Privacy Commissioner to help us determine the issues we should be considering around a large range of possible methods of capturing video, pictures, data, analytics such as number plates or times that vehicles are parked etc.

We recognise that internally we need to be very clear about the business reasons that we are going to want to collect certain types of information; be very focused on ensuring that data is not then used for other purposes; that data is kept for the minimum time needed; that where we are seeking statistical information individuals cannot be identified; but where enforcement is concerned we do need specific information.

There are possibly 10 to 15 areas that we will be looking at but to give you some examples that AT may focus on first:

- Use of cameras to detect cyclists waiting at traffic lights to trigger light changes (at the moment cyclists are not detected by traffic light sensors)
- Use of cameras to detect the length of queues at traffic lights to phase the lights better to favour the peak routes
- Use of camera and number plate recognition to ensure that non-residents do not park in residents car parks

We believe that if these can be made to work they can immediately be seen by the public to be of benefit to them. But we know that we need to be very careful about handling the communications with the public, and as such need to anticipate the concerns that might be raised and address them up front.

I would appreciate setting up a meeting with you and whoever else you think might be appropriate within the Office of the Privacy Commissioner. I fully realise that you are not in a position to offer legal advice, and that is not the purpose of this request. It is to ensure that AT does everything possible to anticipate concerns around privacy and internally takes the appropriate steps to ensure that those concerns are addressed as part of our programme development.

I will be in Auckland on the 28<sup>th</sup> April, and free either between 10:00 and 13:00, or between 15:00 and 17:30. I will then be in Auckland from the 5<sup>th</sup> to the 8<sup>th</sup> May.

Would it be possible to meet you on either the 28<sup>th</sup>, or on say the 6<sup>th</sup> May?

Regards  
Bruce Flett

Bruce Flett | Director  
Ridgehill Ltd. | PO Box 520 | Wellington | New Zealand  
Telephone: [REDACTED] Facsimile: [REDACTED] Mobile: [REDACTED] Email: [REDACTED]

No virus found in this message.  
Checked by AVG - [www.avg.com](http://www.avg.com)  
Version: 2014.0.4570 / Virus Database: 3931/7477 - Release Date: 05/11/14

15/5/14

Brice Flett → contracted AT  
program of work for AT technology impt.  
already in progress: CCTV. → public safety.

AT interest is in Traffic  
how can tech be used? ↙ ↘

no surprises.

Looking at detecting vehicles  
cyclists  
people ] numbers in order  
to trigger lights  
length of queues

Also: Residents parking zones  
using pictures or ANPR

Need Journeytime information.

main roads + arterial

low tech cameras with back end [ANPR]?

Timeline: September + before things happen  
Trials leading up.

email PIA handbook.

Notes of meeting  
15/5/14

written by Tim

New road

## Katrine Evans

---

**From:** Bruce Flett <[REDACTED]>  
**Sent:** Thursday, 22 May 2014 10:25 a.m.  
**To:** Tim Henwood  
**Cc:** Sarah Adams-Linton  
**Subject:** RE: Auckland Transport - Early considerations of Privacy Implications from Collecting Transport Information via various technologies

Hi Tim,

I must apologise to you. I thought I had replied to this email, but now realise that I didn't.

Thank you both for your time, for the discussions and for the links to the various pertinent reports.

I have now set up meetings with people in NZTA, and with the Police for two weeks' time to discuss Traffic Systems in general, and Red Light running.

Regards  
Bruce Flett

Bruce Flett | Director  
Ridgehill Ltd. | PO Box 520 | Wellington | New Zealand  
Telephone: [REDACTED] Facsimile: [REDACTED] Mobile: [REDACTED] :mail: [REDACTED]

---

**From:** Tim Henwood [mailto:[REDACTED]]  
**Sent:** Thursday, 15 May 2014 12:35 p.m.  
**To:** 'Bruce Flett'  
**Cc:** Sarah Adams-Linton  
**Subject:** RE: Auckland Transport - Early considerations of Privacy Implications from Collecting Transport Information via various technologies

Hi Bruce,

Good to meet you today. As discussed, here's a link to our privacy impact assessment handbook:  
<http://www.privacy.org.nz/news-and-publications/books-and-articles/privacy-impact-assessment-handbook/>

Also, here are links to NZTA and MOT's transport technology positions/position development:  
<http://www.nzta.govt.nz/resources/intelligent-transport-systems/position-statement.html>  
<http://www.transport.govt.nz/ourwork/intelligenttransportsystems/draft-its-action-plan-consultation/>

And the position paper on red light cameras from MOT is here:  
<http://www.transport.govt.nz/news/motivate/land/redlightcamerapositionpaperreleased/>  
This paper was released in July last year, so Sarah's still following up to see if there is anything more recent.

Cheers

Tim

---

**From:** Bruce Flett [mailto:[REDACTED]]  
**Sent:** Tuesday, 13 May 2014 9:35 a.m.  
**To:** Tim Henwood  
**Cc:** Sarah Adams-Linton

**Subject:** RE: Auckland Transport - Early considerations of Privacy Implications from Collecting Transport Information via various technologies

Hi Tim,

That suits fine, thank you. See you at 11:00.

Regards  
Bruce

---

**From:** Tim Henwood [mailto: [REDACTED]]  
**Sent:** Tuesday, 13 May 2014 9:15 a.m.  
**To:** 'Bruce Flett'  
**Cc:** Sarah Adams-Linton  
**Subject:** RE: Auckland Transport - Early considerations of Privacy Implications from Collecting Transport Information via various technologies

Hi Bruce

How does 11am Thursday suit?

Cheers

Tim

---

**From:** Bruce Flett [mailto: [REDACTED]]  
**Sent:** Monday, 12 May 2014 6:22 p.m.  
**To:** Tim Henwood  
**Cc:** Sarah Adams-Linton  
**Subject:** RE: Auckland Transport - Early considerations of Privacy Implications from Collecting Transport Information via various technologies

Hi Tim,

Unfortunately I have just arranged a meeting at 2:00 with NZTA for Thursday. I can do any other time on Thursday though. So either 15:00 or morning through to 13:00? Please let me know.

I have noted Sarah's name on other OIA correspondence with NZTA about Automatic Number Plate Recognition, which is also extremely relevant.

I enclose a letter of introduction from Auckland Transport.

Regards  
Bruce

Bruce Flett | Director  
Ridgehill Ltd. | PO Box 520 | Wellington | New Zealand  
Telephone: [REDACTED] | Facsimile: [REDACTED] | Mobile: [REDACTED] | Email: [REDACTED]

---

**From:** Tim Henwood [mailto: [REDACTED]]  
**Sent:** Monday, 12 May 2014 5:15 p.m.  
**To:** 'Bruce Flett'  
**Cc:** Sarah Adams-Linton  
**Subject:** RE: Auckland Transport - Early considerations of Privacy Implications from Collecting Transport Information via various technologies

Bruce

Thursday works fine for me. I'll also bring along my colleague Sarah Adams-Linton as the your work sounds like it falls across both our desks.

How does the afternoon work for you? Say, 2pm?

Cheers

Tim

**Tim Henwood** | Policy Adviser (Technology)

Office of the Privacy Commissioner Te Mana Matapono Matatapu

PO Box 10094 | Wellington 6143 | New Zealand

Level 4 | 109-111 Featherston St | Wellington 6011

F +64 4 474 7595 | [www.privacy.org.nz](http://www.privacy.org.nz)

*Privacy is about protecting personal information, yours and others. To find out how, and to stay informed, [subscribe](#) to our quarterly Privacy Newsletter or follow us online [Facebook](#) [Twitter](#)*

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments. Please treat the contents of this message as private and confidential. Thank you.

---

**From:** Bruce Flett [mailto: [REDACTED]]

**Sent:** Monday, 12 May 2014 3:56 p.m.

**To:** Tim Henwood

**Subject:** Auckland Transport - Early considerations of Privacy Implications from Collecting Transport Information via various technologies

Hi Tim,

As per the email from Sarah Thompson, would it be possible to find a slot this week for me to come in and see you?

My best days would be Thursday or Friday.

Regards

Bruce Flett

**Bruce Flett** | Director

Ridgehill Ltd. | PO Box 520 | Wellington | New Zealand

Telephone: [REDACTED] | Facsimile: [REDACTED] | Mobile: [REDACTED] | Email: [REDACTED]

---

**From:** Bruce Flett [mailto: [REDACTED]]

**Sent:** Monday, 12 May 2014 3:32 p.m.

**To:** 'Sarah Thompson'

**Cc:** 'Tim Henwood'

**Subject:** RE: Auckland Transport - Early considerations of Privacy Implications from Collecting Transport Information via various technologies

Hi Sarah,

Many thanks for the information and your time last week.