# T R A N S C R I P T

# LEGISLATIVE COUNCIL ECONOMY AND INFRASTRUCTURE COMMITTEE

## Inquiry into Expanding Melbourne's Free Tram Zone

Melbourne—Thursday, 9 July 2020

*(via videoconference)*

**MEMBERS**

Mr Enver Erdogan—Chair
Mr Bernie Finn—Deputy Chair
Mr Rodney Barton
Mr Mark Gepp
Mrs Bev McArthur
Mr Tim Quilty
Mr Lee Tarlamis

**PARTICIPATING MEMBERS**

Dr Matthew Bach
Ms Melina Bath
Dr Catherine Cumming
Mr David Davis
Mr David Limbrick
Mr Andy Meddick
Mr Craig Ondarchie
Mr Gordon Rich-Phillips

**WITNESS**

Mr Sven Bluemmel, Information Commissioner, Office of the Victorian Information Commissioner.

**The CHAIR**: Welcome to the Economy and Infrastructure Committee's public hearing for the Inquiry into Expanding Melbourne's Free Tram Zone. We wish to welcome any members of the public watching via the live broadcast.

Before you begin, I would like to just read out a witness statement. All evidence taken at this hearing is protected by parliamentary privilege as provided by the *Constitution Act 1975* and is further subject to the provisions of the Legislative Council standing orders. Therefore the information you provide during this hearing is protected by law. However, any comments you repeat outside the hearing may not be protected. Any deliberately false evidence or misleading of the committee may be considered a contempt of Parliament. All evidence is being recorded. You will be provided with a proof version of the transcript following the hearing. Transcripts will ultimately be made public and be posted on the committee's website.

We welcome any opening comments, but ask that they be kept to a maximum of 5 to 10 minutes to allow time for discussion. Can I please remind members and witnesses to mute their microphones when not speaking, to minimise interference. If you have any technical difficulties, please disconnect and contact committee staff, using the contacts you have been provided. Can you please give your name for the benefit of our Hansard team and then begin your presentation. Thank you, Commissioner.

**Mr BLUEMMEL**: Thank you, Chair. My name is Sven Bluemmel. I am the Victorian Information Commissioner. Thank you, Chair, and thank you to the committee for the opportunity to speak with you today. I will primarily be speaking to item (4) in the terms of reference, which is about the use of technology, and I note that one of your earlier witnesses this morning of course started talking about that as well in terms of capacity optimisation and the like, so that is really the only area I will be speaking to.

For bit of context, as the Victorian Information Commissioner I am the independent Victorian regulator of three jurisdictions: freedom of information, information privacy and what the Act calls 'data protection', which is really information security. From those perspectives clearly anything to do with transport is very data intensive, and I certainly will not be expressing a view in favour or against the free tram zone extension; I do not think that would be appropriate for my role. What I would like to bring to the committee's attention, as I have in my very brief written submission, is the importance of information rights in that term of reference (4) on intelligent transport systems, which is an area that my office has been looking at and commenting on extensively.

Now, in a public transport environment, while technology has the opportunity to provide tremendous benefit in terms of network planning capacity, utilisation, all of those sorts of things, decision-making and the like—and that is certainly something that my office very, very strongly supports as being potentially of great public benefit—the caution we would add is that it is very easy with such an enormous collection of data to not only fall foul of the *Privacy and Data Protection Act* if one is not careful but to genuinely lead to unintended outcomes.

Not long ago—last year—my office published the results of an investigation into the use of Myki data by a datathon, which was intended to be deidentified data. This was done with very, very good intentions to allow Myki touch-on, touch-off data being made available to some very broad research communities with the best of intentions to try and reach better insights into transport planning and the like, again something that conceptually my office supports very much. However, while that data was thought to be deidentified and was attempted to be deidentified, my office found, through investigation, that it was actually possible for substantial amounts of that data to be reidentified.

Now, for many of us we might think, 'Well, what's the big deal if people know what tram I take and at what time?'. But I would say a couple of things in response to that. One is for people in certain scenarios that can be deeply concerning. Imagine a person, for example, fleeing domestic violence or some other form of abuse. Imagine also people who have legitimately assumed identities—undercover operatives for state and federal authorities, for example. If their identities were able to be compromised through the analysis of traffic and transport patterns, you can imagine that the outcomes from that could be potentially catastrophic for them, their

families and indeed others. So really that is all I wanted to say in terms of ensuring that the committee is aware of those risks. I am sure of course that you are.

I would just like to finish my introductory statement by saying that, as I said in my submission, while the public would quite clearly expect their personal information in transport systems to be utilised for certain purposes, such as cracking down on fare evasion and providing the public transport service of course, there are certain things that the public would not expect, such as use for targeted advertising—those sorts of things. Now, I am not suggesting that those are happening here, but that is a very important thing. And why does that matter? Well, as we have seen with the current COVID crisis, trust in government is absolutely crucial to effective response to things like pandemics. If people continue to lose trust in government, both elected and public service, then future efforts in things like pandemic response will be made much, much harder, if not impossible, and that is why that matters. So thank you, Chair, for the opportunity, and I of course welcome any questions.

**The CHAIR**: Thank you, Commissioner, for that concise presentation.

**Mr QUILTY**: Obviously this is an area of concern for me: do you think that the risks of abuse of this data outweigh the benefits of collecting it, first of all?

**Mr BLUEMMEL**: I would say I cannot answer that as an overall. What I would say is it would depend very much on the context. What I would also say is: let us beware any false dichotomies. You are not putting one to me; that is not what I am suggesting. But if we have the argument that is sometimes put as saying, 'Well, you can have an efficient transport system or you can have respect for privacy', or 'You can have a secure law enforcement environment or you can have privacy and human rights', I always caution against those because I think that is, frankly, a little bit lazy. So what I would say is that, well, we can have both. In a case-by-case basis what I would say is: can you have intelligent transport planning without invading privacy? I would say, yes, absolutely you can. So I would say we should not have to choose. I am sure there are certain examples where we may have to choose. There may well be cases—I would imagine this underlines some of your and perhaps your colleagues' thinking—where we can say, 'Well, if we track individuals at an individual level through their journey, can we have some marginal improvement in transport planning?'. Well, perhaps. But I would say, let us first try and find a way of doing that that does not infringe on people's freedoms.

**The CHAIR**: By the way, I also welcome Mr Barton. He has come online as well.

**Mr GEPP**: Thank you, Commissioner, for your presentation. Just in terms of the transport intelligence systems—and I understand your point that if you can collect the data in order to improve the public transport network the requirement there would be anonymity essentially—are you aware of any other systems elsewhere in the world that have those sorts of features, those characteristics, that governments use to drive their public policy, particularly as they gather utilisation data et cetera?

**Mr BLUEMMEL**: Look, it is not something we have looked at in great detail from intelligent transport planning as a whole. The investigation I mentioned that we undertook last year was really, as I said, very well intentioned, but it was really a case of where data was thought to have been de-identified and then made available to researchers. One of the things I would say from that, in answer to your question, is that there is a difference between aggregate data—this many people boarded at Flinders Street station and this many people alighted at Spencer Street station; that is aggregate data. That is not privacy invasive and it is very anonymous, but it is not all that useful because you do not know how many people made which journey.

**A member** interjected.

**Mr BLUEMMEL**: That is right. But what I would say is that I think some years ago with big data, open data, we thought that the way we could do it was to deidentify that unit record-level data, that journey experience, so it is not clear that it was I who took the trip but it is clear that someone took this trip or 28 people took this particular trip, which is very useful for transport planning. We could do that in a de-identified way and then make that available to any researchers broadly without fear of privacy invasion. Unfortunately what we have arrived at is the conclusion that that is impossible, because with data analytics once you just know a little bit of extra data you can then combine that with a dataset and with a fairly high degree of confidence reidentify someone. The silver lining that we can still do is we can do that in house. So rather than making it available to the world, what we can say is: let us create trusted internal labs or data rooms that are controlled by government and invite the researchers in. That can even be virtual; it does not have to be physical. But rather than making

the dataset available, we, government, control the dataset and then the researchers are allowed careful, limited, secure access to it for their queries without being able to take the full dataset away. I think that is where it is heading around the world as well.

**Mr GEPP**: Sorry, Chair, if I might—I would imagine, even in that example that you have just provided, that would only hold true if the management of that data and the research was conducted onshore around very specific laws and guidelines about its treatment.

**Mr BLUEMMEL**: That is exactly right, and of course these days data can be stored offshore without people really turning their mind to it. Under the Victorian *Privacy and Data Protection Act* an agency can only transmit data outside Victoria if they can be confident that that data is protected by a similar or stronger privacy or other law. Now, that is quite tricky these days of course with international data centres that might be a US organisation based in South-East Asia operating an Australian office. It is not impossible to navigate those but it is quite tricky. Of course there is a risk that once it is in those other jurisdictions or indeed if the company operating it is in those other jurisdictions, even if their data centre is onshore, there is the possibility that other governments under their legislation may seek to exert a right of access to that data, and that is something we have to manage very carefully.

**Mr GEPP**: Sorry, Chair, this is an important thread I think.

**The CHAIR**: Yes, very important, please continue.

**Mr GEPP**: As you were just giving that explanation, Commissioner, I was thinking of a financial institution. Many do use offshore or send some of their work offshore, and of course it seems logical to me that if you are sending that work offshore that means that the information of your clients or customers also has to travel offshore. My understanding is that it is the sovereign laws of the country where that data is sitting that apply in an international sense. Is that correct?

**Mr BLUEMMEL**: It is not even that straightforward. It can even be more complicated than that. So, for example, there is a US law that seeks to exert the application of US law to data stored outside the US where that is stored by or under the control of a US company. As far as I know that has not been tested yet, but there is certainly substantial legal scholarship in that area that says, 'That's quite uncertain, that's quite a risk'.

**The CHAIR**: It is a very important topic. I have just got a short question, because one of our previous speakers was from the Department of Transport. How closely do you work with the Department of Transport to ensure that data is collected in accordance with the Act, or do you work completely independently?

**Mr BLUEMMEL**: We work completely independently. We are the regulator and we have the ability to actually take substantial regulatory action against government agencies. So we have to be a little bit careful, but what we do want to do is we do want to be helpful to the extent that that does not erode our ability to do that independently. For example, I mentioned the Myki investigation; we obviously worked very closely with Transport there, but that was in an investigative context, where we were taking regulatory action. Where we have to be a little bit more careful is, for example, when an organisation and government agency is undertaking a project or delivering a system and things like that; we would like them to come to us for some guidance and advice, but we have to be very careful that we cannot be part of, say, the design committee or we cannot be part of any sign-off process to say, 'Yes, this is a privacy compliant', because we may have to take regulatory action down the track, and if we were part of the approvals process then we would be conflicted. So we have to do that fine balance. We do, I think, err on the side of early engagement wherever we possibly can, but we just have to do it carefully and we might point them to, say, some tools or resources or even some good research that is taking place. But we can never say, 'Yes, this is compliant', unless we are actually in that regulatory mode.

**Mr QUILTY**: So when this data is collected—you were talking about collecting personal data but using it only within the organisation, but doesn't that also put it at risk of hacking and data breaches? How do you draw the line about the usefulness versus privacy risk?

**Mr BLUEMMEL**: The answer to your question is certainly yes. Any kind of information that is held—personal information or indeed any information that might be an attractive target—if it is only held within the organisation and onshore, there is of course still a risk. There is the risk of insider threat; there is the risk of hacking, malicious—we see of course state-sponsored and even state-based actors with tremendous not just

incentive but also tremendous capability, and I probably do not need to go too much into that, because I think we are all well aware of that, especially in the last month or so. So, yes, those risks certainly do not go away.

What I would say is that at least when it is within the organisation it is more containable—but it does not go away. So one of the areas that we actually regulate under the *Privacy and Data Protection Act* is that all Victorian government and some local government agencies have to submit to us what is called a protective data security plan every two years. That has to be attested to by the head of the organisation to say, 'Yes, I am confident that this represents our identification of risks and what we do about them'. What we are trying to do with that is we are trying to get away from a security culture that is sort of a check-box culture, where you are, for example, saying, 'Well, our encryption is 256-bit encryption, therefore we are okay', without turning your mind to, 'Well, what's the risk?'. If you have got the best encryption in the world but your decryption key is stored on a USB drive that you leave lying around on a tram, well, then you have got a problem.

So we are trying to get much more towards genuine risk management where you actually say, 'Well, if I am an organisation and I am collecting millions or billions of records of personal information about Victorians and visitors and so on, then I am going to have to be really careful about how I deal with that, whereas if I am an organisation that does much less of that at a much more modest scale, clearly I have a different risk profile'. Both need to manage their risk profile in an appropriate way. So, yes, the short answer is the problem does not go away if you keep it in house, but it is more containable.

**Mr QUILTY**: So what are the penalties for a public organisation that loses data, though, as a data breach?

**Mr BLUEMMEL**: For us in terms of our regulatory action under the privacy Act it is really primarily that we can issue what is called a compliance notice on an organisation and an organisation then has to comply with that. So the Myki investigation that we did, we issued a compliance notice on Public Transport Victoria. I was very pleased to say that that was treated very seriously by Public Transport Victoria and the organisation is actually currently well and truly on its way to complying with all of the things that we put in place there. It is always the issue for a public sector regulator regulating a public sector entity in terms of what is the most useful thing that you can do by way of your regulatory toolkit. For us, what we want is behavioural change. The naming and shaming—yes, look, sometimes it has to be part of the arsenal, but we ultimately do not want people to just be in fear of us, because then there is the moral hazard of organisations closing their books to us and not coming to us when there is an element of risk. What we want instead is organisations to take our recommendations on board and then actually change their behaviour to make sure that in the future the problems do not happen again. We can still get the benefit that we can from data and data analytics but do it in a way that does not have to compromise human rights. It is that behaviour change that we want.

**Mr QUILTY**: You talk about making data collection possibly an opt-out. I guess also having an opt-in would also be an option, but that would presumably create much less official data. Can you expand on that?

**Mr BLUEMMEL**: Yes, the whole opt-in, opt-out is actually quite problematic. A really good example of opt-in, opt-out in the last couple of years was the personally controlled electronic health record, the My Health Record. Now, that is a federal government initiative, so I do not have jurisdiction there, but I think it is a really good illustration, because it was originally an opt-in. Again I think you can argue that there are very good benefits both for the individual and on a public health basis in terms of having people opting in. It then went to an opt-out, but with either of those you have the scenario that, whether it is opt-in or opt-out, you can get a biased dataset. Are the people who are likely to opt out a certain group of individuals? If so, the data you have left is skewed and does not allow you to make the best possible decisions.

One of the things in privacy in any event is that while consent is an important element of privacy and goes with the whole philosophy of choice—I can choose to have a social media account and give up lots of data if I think it is in my interests to do so—the problem with that, especially in a government context, is if you are going to say, 'Well, it's a condition of boarding a train or a tram and tagging on with your Myki that your data can be used for purposes X, Y and Z', that is not real consent, because if you are saying, 'Well, the only way I can use this quasi-government service, or indeed government service, is by consenting, and therefore my other option is to walk 5ks because I can't afford a car', well then that is not really meaningful consent. So we always try and suggest to agencies, 'Don't rely too heavily on consent, because with consent it can be meaningless and it can be ill informed as well'. All of us will have driven into a car park and at the entrance to the car park is a huge board of terms and conditions. Do we read that every time we go into the car park? Probably not, because there

are 20 cars behind us and we just want to get the ticket and park. So that is pretty meaningless as well. What I suggest instead is that agencies should say, 'Design your systems in a way that's inherently more respectful of human lives, more respectful of privacy and individual choice', and then you will be less reliant on those fairly crude opt-in, opt-out or indeed consent mechanisms.

**The CHAIR**: I found that very informative. I will go back to the point that Mr Gepp made just briefly: it sounds like we might need to regulate or further investigate to make sure that this data is not leaving our jurisdiction, because of all the potential capabilities and all the actors involved in this kind of espionage, let us put it that way.

Does anyone else have any more questions? I do not, because it seems that most of the issues that I was concerned about were covered by the questions raised by Mr Gepp and Mr Quilty. If not, I wish to thank you, Commissioner, for that informative session. Like I said, I found it one of the most productive sessions we have had today. It is a very important issue that probably cuts across a number of areas, and I understand the fine balance that you explained between being the regulator and also being informative to all the other bodies that are responsible for data collection and privacy. Thank you very much.

**Mr BLUEMMEL**: Thank you very much, Mr Chair, and all the best with your deliberations.

**Witness withdrew.**